The Back Cover Photos

This actually is far from the first speedometer picture we've gotten, but it's one of the coolest looking ones. It comes from a 2010 Ford Fusion belong to **timi2shoes** who set an alarm on his phone to keep from missing the magical event. He had to pull off of a busy street and drive into an alleyway for a while in order to capture the 2600 moment. Now that's dedication.

This is one of the better looking "2600 lairs" that we've seen lately. Spotted in Vancouver, Washington by **MotoFox**, this building has since had their huge red numbers removed. Apparently, too many readers were showing up to get autographs.

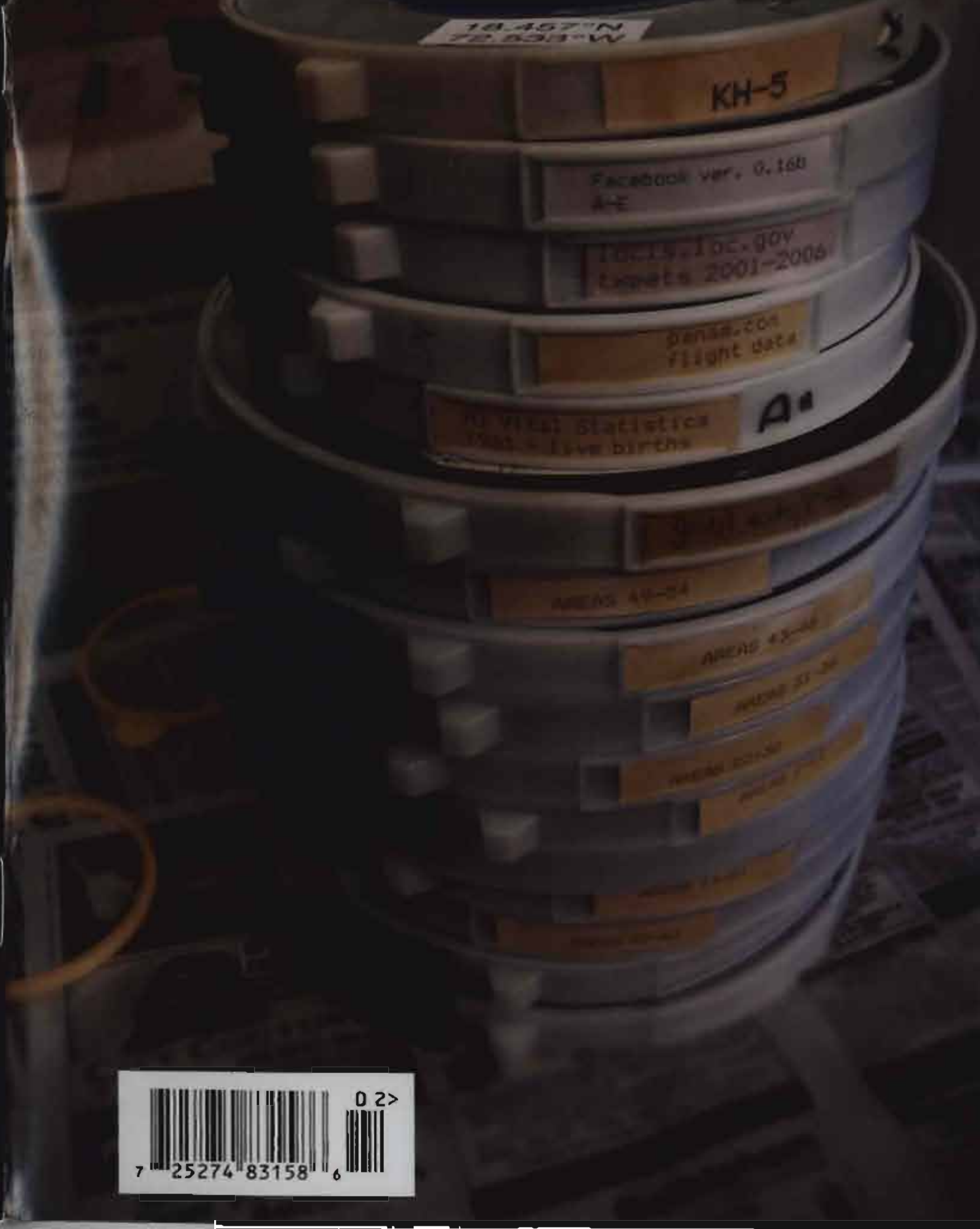
Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

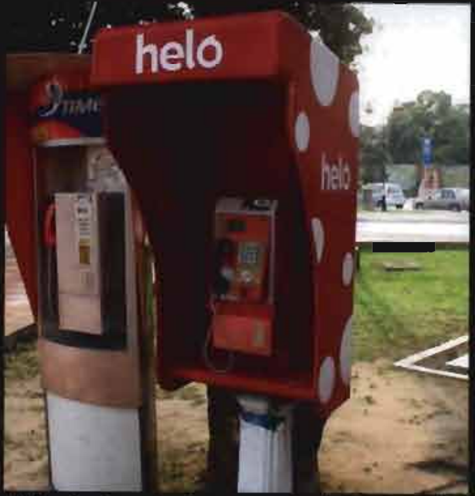
If we use your picture, you'll get a free one-year subscription
or back issues or a 2600 t-shirt of your choice.

Volume Twenty-Seven, Number Two
Summer 2010, $6.25 US, $7.15 CAN

2600
The Hacker Quarterly

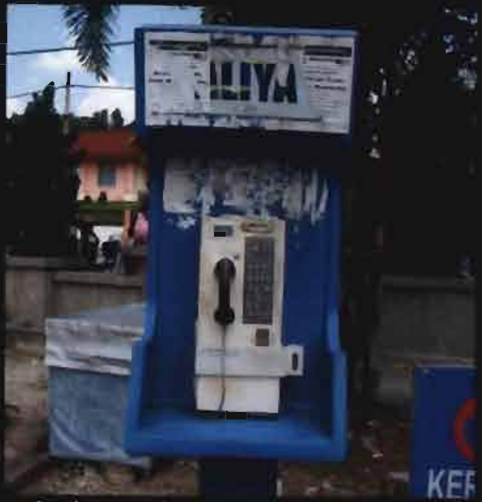


Asian Payphones



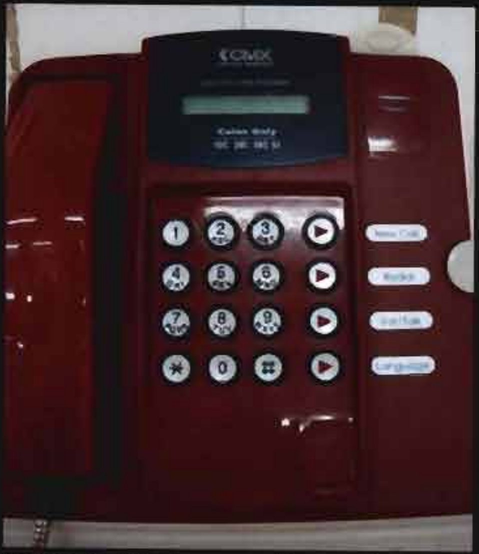
Malaysia. Seen in downtown Kuala Lumpur, this polka dotted phone booth is a rather common sight for this particular brand of phone. We have no info on its square neighbor.

Photo by Nathan Linley



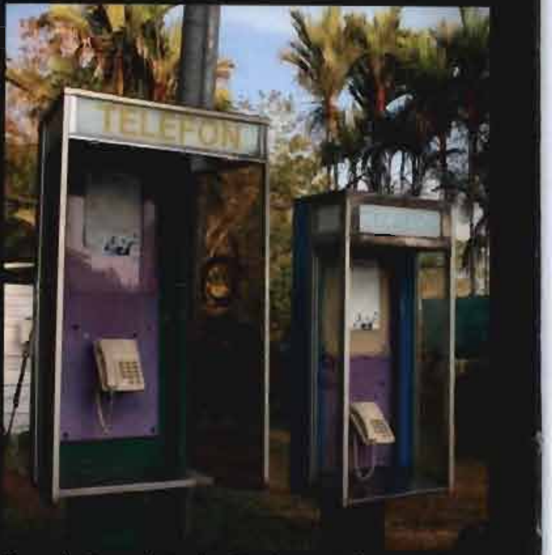
Malaysia. Found at the commuter train station in Kajang, here is a phone that has clearly seen far too much sun and advertising.

Photo by Nathan Linley



Singapore. This phone was discovered at one of those open air food centers known as "hawker centers." Multicoin and multilingual, there doesn't seem to be much this phone can't do, except take cards.

Photo by Stylie



Brunei. Spotted in the Tasek Merimbun Heritage Park in the Tutong district. Not really what we'd call "pay" phones but these days you can apparently just stick a desk phone in a payphone kiosk and get away with it.

Photo by Steve McCain

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

VERBAL DIAGRAMS

“The Hacker Dialogue”

As this issue goes to press, the newest *2600* book is hitting the stands. This one focuses on what to many is the most popular section of the magazine: the letters. It's not at all surprising to see how popular, and powerful, such dialogue can be.

We started getting letters from our readers almost immediately after sending out our first issue way back in 1984. They began to be printed in the magazine shortly afterwards. Eventually, there were so many coming in that the letters section mushroomed into the biggest single part of the magazine. This is highly unusual in the publishing world, but in a hacker world long known for its love of discourse of all types, it makes perfect sense.

We've always been striving for communications of one sort or another. The magazine itself was founded because there *were* no effective communications at the time between the hacker world and the mainstream. Each existed in its own little vacuum, spreading misconceptions and fears about the people they didn't understand. By opening the door, we helped to show the world what hackers were really all about and also give hackers a voice where they weren't simply preaching to the choir.

There are always risks involved whenever such a door is opened. We took quite a bit of heat from members of the hacker community who felt we were exposing people to undue scrutiny and eventual prosecution by openly discussing what was going on within. At the same time, we found ourselves often blamed by the mainstream for *anything* going wrong in the world of technology because so many felt that hackers were always the cause of problems and, since we were the only organized group speaking on behalf of the hackers, it mostly fell on us.

The benefits of dialogue, however, most always outweigh those risks and we believe the openness has ultimately helped. Sure, we were witness to many abuses and injustices, a good number affecting people close to us. But when people were sent to prison for ridiculous reasons, we were able to say something and get the word out to the rest of the world because these bridges had already been built. That ability is vital for anyone. Even if these wrongs don't immediately stop, educating the populace is the best strategy in ensuring that they eventually *will* stop.

We certainly have no shortage of injustices around us today. But now when they occur, it's so much easier to apply the potential effects to people outside our community who, after listening, often lend their support when we take action. In the past, for instance, we might have seen a government raid against a group of people somewhere who were accused of software piracy. It would have been reported on the news as a bunch of hackers getting what they deserved and the rest of humanity now being a bit safer. And *that* would have been the end of it for the vast majority of people hearing the story. Today, when such a thing happens, the openness of communications allows the accused to speak out and show how the story is not necessarily as reported by the mainstream media. And so many more people are there to listen.

A great example of this is the raid on Pirate Bay which took place four years ago. Rather than simply accept the word of the authorities that this organization existed solely to steal, violate copyrights, and cause general havoc, the world was compelled to hear the other side of the story and to start questioning the very concept of copyright itself. As is often the case when something is seen as unfair, membership in the afflicted organization skyrocketed and more people throughout the planet took up the cause. A fledgling political party found itself propelled into the international spotlight as a result. Today, the Pirate Party of Sweden is the third largest political group in the country, gaining over seven percent in recent parliamentary elections, having two seats in the European parliament, and presiding over the largest political youth group in Sweden, known as Young Pirate. There are currently pirate parties in over 40 countries and the movement is growing. *This* is what having a voice can accomplish.

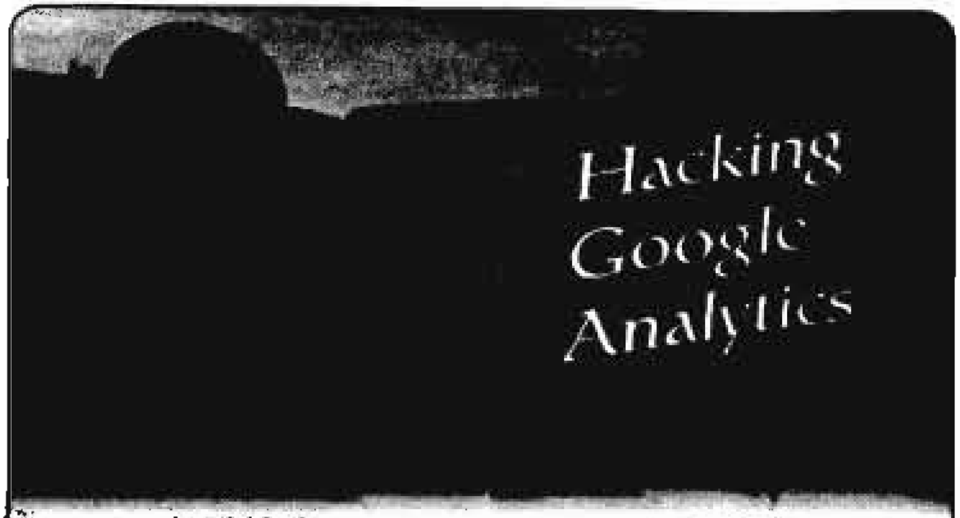
It's important to recognize this tremendous accomplishment regardless of whether or not we agree with the platforms. In the past, we would accept the status quo because that's what we were used to and we had no perceived means of altering things. All of that is now transformed because of the ongoing dialogue we have the ability to become a part of. That which was once accepted can now be openly challenged. And if you subscribe to the premise that anything can be questioned and changed, then there is great potential for improvement, new ideas, and progress. Of course, there's also the chance of mistakes, setbacks, and false premises. But to not take that risk is a guarantee of stagnation.

Today, instead of shutting down a site and forcing its users to scatter, as was the practice back when we started publishing, a healthy debate is raging on the issues of copyright, file sharing, and fair compensation. Much of the credit belongs to the development of the Internet, which gave people the means to extend the dialogue beyond their wildest dreams. That ability must never be given up, neither to crippling restrictions nor to its "dumbing down" by yielding attention to the loudest voices. Intelligent dialogue will exist as long as we continue to seek it out and contribute to it.

To witness and be a part of this incredible transformation has been truly inspirational. Nothing is a better testament to the potential of people power. But we must be careful not to make the same mistakes in a completely different forum. For instance, giving away your ability to run your own machine on the net and instead trusting the very entities who want to control every aspect of your connection to the world; cutting yourself off from those who don't use a particular type of communications protocol, social networking site, or even those who don't use the net at all (yes, they do exist in great numbers); falling prey to the noisiest (and often dumbest) voices who drag people into their activities "because everyone else is doing it." These are all very bad ideas and also happen to be trends we see constantly. The signal to noise ratio of the net seems to decrease with every passing day, making it ever challenging to keep from drowning in a sea of nothing. This is a danger that exists with any tool of communication and it's why we have to continue to maintain and refine what we have so it stays accessible, intelligible, and completely open to a new way of thinking.

As this issue comes out, our eight hacker conference (The Next HOPE) will be underway in New York City. The value of seeing it all in person and actually engaging in real life communications cannot be understated. While we can accomplish a great deal in front of our screens talking to the entire world, let's not forget the importance of occasionally getting away from that environment and participating in face to face discourse, reaching people we otherwise would never have the opportunity of talking to on an individual level. This is why we continue to have these conferences, as well as our monthly meetings. In addition to talking with other like-minded people, there is always the chance of a random encounter with someone who is *not* part of the hacker world, yet who will be curious enough to want to find out more about us. That is where true progress is made and it's why being outside and in the main streets of the world is so vital for anyone who truly wants to make things better.

The dialogue continues - in our letters, on the net, and out there in the "real" world. The best, as always, is yet to come.



Hacking Google Analytics

by Minishark

Introduction

Web sites have been tracking users since the very beginning of the web. In recent years, methods for tracking users have matured considerably. No longer are site owners limited to simple hit counters; they now can know where users came from, which pages were visited, how long they were viewed, and hundreds of other metrics. The most popular tool that can collect this data is Google Analytics[1].

Now, web analytics can be a very useful marketing tool for running any site. However, my concern is that site owners are too quick to trust all their analytics data to the hands of third parties (in this case Google). The Google Analytics privacy policy states that it does not collect "personally identifiable information" about users. However, Google does not clearly define what constitutes personally identifiable information. We already know that other Google services log users' IP addresses, and Google Analytics is no exception. While your IP address isn't necessarily personally identifiable, in many cases it's still uniquely identifiable. Google now not only has information about your habits on their sites, but potentially on the thousands of other sites that use Google Analytics as well.

Google promises that they aren't doing anything fishy with all this data about you, but you may not be willing to risk taking their word for it. They're still not above the law, and recent cases have shown they have few qualms about turning over user data to the government if they're subpoenaed[2]. Additionally, studies have shown that you can uniquely identify the majority of people based solely on a few pieces of "anonymous" demographic/geographic data[3].

How GA Works

Google Analytics uses Javascript and cookies to track users. Users place the following snippet of Javascript code on each page of their site that they wish to track (it's usually placed at the bottom of the page):

```
<script type="text/javascript">
var gaJsHost = (("https:" ==
➥ document.location.protocol) ?
➥ "https://ssl." : "http://www.");
document.write(unescape("%3Cscript
➥ src='" + gaJsHost + "google-
➥analytics.com/ga.js' type='text/
➥javascript'%3E%3C/script%3E"));
</script>
<script type="text/javascript">
try{
 var pageTracker = _gat._getTracker
    ➥("UA-xxxxxx-x");
 pageTracker._trackPageview();
} catch(err) {}
</script>
```

The first `<script>` block references a file named `ga.js` from Google's servers (either `https://ssl.google-analytics.➥com/ga.js` or `http://www.google-➥analytics.com/ga.js`). This is the main Google Analytics tracking code source.

In the next `<script>` block, the code instantiates a Google Analytics tracking object by calling the `_gat._getTracker("UA-➥xxxxxx-x")` function, which is defined in `ga.js`. It takes UA-xxxxxx-x, the site administrator's unique GA account number, as a parameter. The next line, pageTracker._trackPageview(), uses this tracking object to register a page view. This is where the interesting things happen. First, it checks a number of cookies, and sets or updates them as necessary:

__utma - A persistent cookie that expires after 2 years. It contains: a web site (domain) hash, a visitor hash, timestamp of the first visit, timestamp of the last visit, timestamp of the current visit, and the count of total visits for this user. They are separated by periods, e.g. `24724➥8150.1037924604.1252115649.12524➥32081.1252444069.1`

__utmb/__utmc - These temporary (i.e. session) cookies are used to determine the length of a visit. __utmb contains a timestamp of the first pageview, and __utmc contains a timestamp of the last pageview.

__utmz - This cookie, which expires after 6 months, keeps track of where the user came from (it does this by looking at the Referer HTTP header). There are a number of pipe-separated fields containing this information, most notably: utmcsr (source - the site they came from), utmccn (campaign - the ad campaign or seo campaign the referring link belongs to), and utmcmd (medium - e.g. referral, organic search, paid search). The whole thing might look something like this: `247248150.1252444069.11.10.➥utmcsr=www.google.com|utmccn=(no➥ ne)|utmcmd=organic`

Once these cookies are set, data is then actually sent to Google Analytics. The tracking code makes an HTTP GET request for a 1x1 pixel, transparent gif image located on Google's servers. This image is named `__utm.gif`. The __utma/b/c/ cookies are appended to this GET request as query string parameters, along with a other info such as browser type, screen resolution, language, etc. You can view this GET request as it happens using tools such as the Live HTTP Headers extension for Firefox[4]. Google picks up all this data on their end, and processes it to generate the Google Analytics reports.

How to be Invisible to GA

Google Analytics requires both Javascript and cookies in order to track you. You can prevent the Javascript from ever being run by either turning Javascript off in your browser settings, or by using an extension such as NoScript[5] for Firefox, which can be configured to selectively block the `ga.js` file. If the Javascript never runs, then no cookies will ever be set, and no data will ever be sent to Google.

Another method is to disable cookies in your browser. Keep in mind that Google Analytics uses first-party cookies, so simply blocking third-party cookies (as some browsers do by default) will not work. When only disabling cookies, the tracking code will still run, and data will still be sent to Google. However, there will be no cookie data appended to the `__utm.gif` GET request, and Google will simply disregard this data on its end.

These techniques will work for any analytics software that uses Javascript and cookies to track users. Another method for tracking users is called IP+UserAgent tracking, which uses your IP address and the browser's "UserAgent" to uniquely identify a visitor by parsing web server log files. This method is less accurate than Javascript/cookie tracking (for instance, many people have dynamic IPs), but it's still fairly popular. Since this is done on the server side, you can't stop it from tracking you altogether, but you can use something like Tor[6] to at least prevent it from uniquely identifying you.

How to Exploit GA for Fun

As you've seen, everything Google Analytics collects about you is done in plain text on the client's browser. This means it's fairly trivial to send whatever bogus information you want to Google Analytics. For example, using something like the Web Developer Toolbar[7], you can change the values of the Google Analytics cookies. Try changing the __utma visit count to 1 million. Or you could change __utmz cookie source information to something like this: "utmcsr=www.fbi.gov|utmccn=(referral)|utmcmd=referral". They'll be left scratching their heads wondering why the FBI is linking to their site.

You can also create your own page with the Google Analytics tracking code. By design, Google Analytics will accept traffic from any domain, not just the one associated with the owner's account - all you need is their UA-xxxxxx-x number (which is right there on their site). Then put the pageTracker._trackPageview() function in a loop to artificially inflate their pageview count.

The best part about all this is that site owners cannot remove data from their Google Analytics account once it's there. Filters can be manually set up to exclude certain data, but they do not work retroactively. Therefore, unless they had enough foresight to set up the filters initially (which most people don't), they'll be stuck with whatever bogus data you sent them. Oh, the benefits of giving up your data to Google!

References

[1] http://www.google.com/analytics

[2] http://wikileaks.org/wiki/Gmail➥_may_hand_over_IP_addresses_of➥_journalists

[3] http://arstechnica.com/tech-➥policy/news/2009/09/your-secrets➥-live-online-in-databases-of-➥ruin.ars

[4] http://livehttpheaders.mozdev.➥org/

[5] http://noscript.net/

[6] http://www.torproject.org/

[7] http://chrispederick.com/work/➥web-developer/

MY SECOND IMPLANT

by Estragon

My first implant was really not a big deal. Getting it was about as complicated as getting an ear pierced. It is a small inductive microphone implanted in my throat. It's basically just a throat mic, but permanent. There is a lot of space between the muscles and sinew of the throat, so the implant was able to include a transmitter about the size of a grain of rice, a piezoelectric film attached to the outside of my esophagus, and a small rechargeable battery.

Because the piezoelectric film actually generates electric current as it responds to the vibrations of my voice, I can keep the battery charged indefinitely just by speaking and eating.

Some people are getting these microphones implanted in their lip or somewhere around their mouth, but this isn't nearly as good for subvocalizing. Also, they tend to get impacted with food particles, and pick up sounds from the environment (including breathing and eating). The advantage, though, is that they pick up sounds from your real voice.

For the induction mics to sound more like you, some digital signal processing is needed. This is done by a tiny radio receiver which, in turn, connects to your cell phone or other devices via Bluetooth or something similar. The implanted mic has no computing power at all–it's just a miniature, low-power radio transmitter hooked up to a microphone.

Anyway, this implant worked just fine, and still does. I can subvocalize commands to my computer, speak on my cell phone, and make recordings of spoken notes. The radio transmitter is good only for a few feet, so surveillance is really not much of an issue. If you're close enough to pick up the radio signal, you're close enough to see my lips and throat move, and probably hear my subvocalizing.

Implanted microphones like these are pretty common these days. Although you can't yet get them at your local body piercing shop, you can buy kits on the Internet, or find some doctors to do the implant. Personally, I decided to get mine from one of the original sources, Yongsan Electronic Village in Seoul. It's not even a back room thing there; it's more like a barber shop. You lean back in a chair, get some local anesthetic, and boom: you're walking out with a small bandage on your neck, and in your hand is a combined receiver and digital signal processor the size of a half-dollar coin. Make sure you get a couple of receivers set to your radio frequency (and write down the frequency somewhere!), in case you lose one. It was less than $200, though I hear you can get some Chinese-made models installed for $125 in Greenwich Village.

I guess I'm avoiding talking about the second implant, since the first one is so sweet. In fact, you probably guessed already that I'm speaking this whole document into my computer right now, subvocalizing to my microphone implant.

Consider that the throat implant is basically just a very small transmitter, sort of like those mini-spy mics you still see advertised in electronics magazines. It turns out that receivers can be a lot more complicated.

For my second implant, I wanted to pair my microphone with some speakers. When you think about it, this makes sense as the next popular wave of human-machine interfaces. There are literally billions of cell phones, MP3 players, and similar devices in the world (this is several times greater than the number of computers). When we were tired of walking around holding our cell phones to our ears to talk, we got wired headsets. Then we got wireless headsets, based on Bluetooth or something similar. The obvious next step is to have a permanent speaker installed in or near the ears, that can communicate wirelessly with phones, computers, or other devices.

This isn't without precedent. There has been some cool technology for deaf people for a while, but it's pretty kludgy and custom. One technique is to use bone induction to help deaf people to hear. A more mundane technolgy is the common hearing aid, whereby people who are hard of hearing can get custom-fitted aids that go into the ear canal, amplifying what is heard. These devices consist of a microphone at one end, a speaker at the other, and some electronics for the battery, volume control, and sound processing.

Did you know that leading-edge quality hearing aids can cost thousands of dollars each?Compare this to under $100 for a really good Bluetooth headset for your cell phone. Well, as you can imagine, some entrepreneurs are working to make in-ear speakers the next big thing.

I thought my first implant was bleeding edge, but this second one wasn't even being mass produced yet. I had a contact–a fellow graduate student who came to my school after graduating from Beihang University in Beijing, China. Beihang used to be known as the Chinese Defense University, and they have some way cool technology there. It's sort of a mashup of a high-tech university, such as CalTech or MIT, with a defense industry lab, like in the old James Bond movies. I don't want to get anyone in trouble, so let's just call my contact Benny Li.

Benny did his undergraduate degree at Beihang, with dual majors in electrical engineering and computer engineering. He spent a lot of time in the lab where they develop microcircuitry for things like those tiny electronic spying insects. Benny said that actually getting insects to fly has been really hard, due to the energy required and weight needed for, say, a robotic fly. But they walk and crawl just great, and can transport themselves by piggybacking on unsuspecting human carriers.

To make a long story short, when Benny heard about my first implant, he got one too. It was during a trip home to China over winter break, and he never told me exactly where. His implant worked just like mine, except his radio signal was encrypted. How encryption of the radio signal happens in a transmitter the size of a grain of rice is beyond me, but maybe his transmitter is bigger than mine.

This first implant got us talking about our desire for in-ear speakers. The basics aren't too hard. You can either use a vibrating surface to make a regular speaker that pushes air around (thin metal sheets, or paper, or whatever), or rig up something similar that impacts the bones of the ear canal or eardrum. But the details are a bitch.

First off, you don't want everyone hearing what you are listening to. So, that rules out a regular speaker placed in the outer ear canal, like those in-ear ear buds or hearing aids. We wanted to be stealthier, and not have it obvious to an observer that we are wearing speaker implants.

Placing a speaker deeper inside the ear canal could work and, in fact, there are some hearing aids that work like this. Our dear, lamented President G.W. Bush supposedly used these all the time while he was giving his speeches, so that a remote person could prompt him with things to say. But these aren't permanent, can be uncomfortable, and tend to muffle outside sounds since they don't have built-in microphones like regular hearing aids.

The plan we arrived at was to place a small Bluetooth receiver and battery subcutaneously, just behind the ear on the outside of the head, but connected with very thin wires (also subcutaneous) to an induction speaker deep in the ear canal. The Bluetooth receivers would be generic items, about the size of 5V voltage regulators and available from places like Mouser. Another thin piece of piezoelectric film would let the battery charge whenever the wearer chewed food.

So far, so good. Since everything would be under the skin, it wouldn't get wet, and wouldn't get moved around if I scratched my ear. Yes, clearly I was thinking I would be the person to test this new gizmo we were dreaming up. The induction speaker would rest right on the bone of my inner ear canal, and would cause me to hear things through my eardrum, but nobody in the room would be able to hear what I was listening to. We decided to leave volume control to the transmitting device (capped to an equivalent of no more than 100 decibels, for safety).

This was just dreams and schematics, but then Benny went home again for spring break. When he came back, he said he had a surprise for me: his friend from Beihang would be visiting and would implant the prototype, if I wanted to try it. Of course I did!

This was a lot more intrusive than the first implant, and left a lump behind my ear where the receiver was. I opted for general anesthesia, but the whole operation took under an hour. Once I healed, I could barely feel the wires as they went into both of my ear canals. But the fact was, it worked great! I could pair the Bluetooth receiver with my cell phone, computer, and MP3 player, and use the first implant as a microphone. It also wasn't dangerous to wash my hair or get water in my ears.

No, I didn't get an infection or develop an allergic reaction or anything like that. Benny's friend who did the surgery, who I'll call Jing Yu, was also a grad student, but he had done a lot of work on experimenting with microelectronics implants in lab animals. I asked him if this was for stuff like turning hordes of rats into surveillance drones, and he said it was something like that, but didn't elaborate. Well, even if I was a lab rat, I could at least enjoy some tunes in the privacy of my own head.

It went well for a few months, and eventually Benny got his speaker implant, too, during another trip back home. Just for kicks, we used it once to cheat on an exam. I subvocalized the questions to him, and he gave me the answers–all with my cell phone hidden innocently in the bottom of my backpack.

So what went wrong? Well, I guess I should tell you what I'm studying at grad school. I don't want to give enough details to get me or my advisor into trouble, though. Let's just say that I'm studying communication, specifically for orbiting satellites and, someday, interplanetary spacecraft. My advisor has grants from NASA, but my tuition is actually paid by a grant from DARPA. Yes, I'm studying to be an actual rocket scientist.

Anyway, what happened was that my receiver implant was a little more capable than I expected. It has a microphone, not just a speaker. In addition to pairing by Bluetooth, it connected to any open wireless access point and opened up a TCP/IP connection back to a system somewhere behind the Great Firewall of China. We found it was able to use WEP- and WPA-enabled access points at school and in my apartment, too. In a nutshell, everything I heard and said, for months, was streamed live to someplace in China.

I might have never known, except that one day in the lab my advisor got a phone call from his DARPA sponsor. It seemed that the algorithm I'd worked on for spread-spectrum communication with ground- or space-based devices was detected on the new Chinese telecom satellite that went up earlier that year. My advisor had provided DARPA with the source code and a paper that he and I had worked on, and I can remember several times we had had detailed technical discussions about it. Plus, I had been in the habit for months of dictating my papers and emails by subvocalizing. The spooky part was that this all happened within a few months after getting the second implant. Even DARPA said it would be years, if ever, before they put the algorithm to use for their own purposes.

While my advisor was on the phone, I didn't know whether to be flattered or scared, but I kept my cool and didn't reveal my growing nervousness. That weekend, I got another grad student friend to spend some time with me in a Faraday cage with a multispectral receiver and spectrum analyzer. We figured out what was going on. Benny swears he didn't know.

I was physically infected by this implant, and turned into a human network zombie. We finally got the thing turned off by carefully snipping the wires from the receiver (and, I now know, transmitter!) to the battery. This hurt like hell, but I won't feel comfortable until I find someone to surgically remove the whole thing. Until then, I'm back to my regular Bluetooth headset, which I now keep wrapped in aluminum foil when I'm not using it.

I don't know whether there's a clear message or moral in my story, but I wanted to share it with you. Partially as a warning to readers about the potential dangers of new technology, partially to brag that I was the first kid on the block with implants that, someday, will be as common as wrist watches, and partially to try to inspire entrepreneurs and inventors out there to get this type of thing working better, and at a good price. Hell, with two billion cell phones in the world, there's a huge market to be tapped.

Next, I've gotta get some cameras installed in my eyes.

Free Encrypted 3G Web Access on T-Mobile Smartphones

by EvilGold

After reading the article in 26:4 about T-Mobile, I was inspired to look into things a bit more and see what other holes might exist on T-Mobile's 3G network. Because I have a prepaid T-Mobile plan with no data subscription, I didn't have to worry about getting overage charges if my investigation turned up nothing. So with nothing to lose and the potential of free 3G access on my G1, I got to work.

Disclaimer: This article is entirely for informational purposes only. I am not well versed in how T-Mobile monitors data usage. This may only work if you have a flex pay account. If you're trying this on with a post-paid plan, then you might end up getting charged. I strongly recommend that you try these techniques only with a pre-paid account. Everything I mention here was only tested on a G1 Android phone, but most of the information could probably be applied to any smartphone. With that out of the way, lets get to exploring.

The first discovery was with an application I had already been using with WiFi for months called Meebo. I had set Meebo to automatically connect whenever my phone was turned on (since I am usually around a WiFi connection anyway), but I noticed one day that it had connected on its own, without any available WiFi around. After trying it out for a few days with WiFi turned off, it still worked. This in and of itself was a nice find, because it meant free unlimited texting to not just other phones (using AIM's SMS support), but also to any contacts on Jabber. (Meebo supports a huge number of protocols including AIM, XMPP, and Yahoo).

It wasn't too long before I came across another application called 'Wikimobile' which also worked with the non-subscriber 3G connection. I tried using another chat client, and Google's included Gtalk client, but neither worked. `http://wikipedia.org/` was still blocked in web browsers. Something was definitely opened up for these two apps to work, even when most other apps would fail to connect or get redirected to a page telling you to upgrade to a data plan.

So what could these apps be using that most others probably didn't? It turns out that both Meebo and Wikimobile where using HTTPS instead of plain HTTP to access the web. Knowing this, I disabled WiFi on my phone, and pointed its browser to `https://gmail.com/`, and *it worked*! So, of course, any HTTPS proxy would work too. Sure enough `https://kuvia.eu/` worked just fine. As did a number of other HTTPS proxy sites. The next thing I tried was using SSH to connect to a server running on port 443 (normally HTTPS). This too worked perfectly. With SSH access comes nearly unlimited potential. Still, there was more to be found.

Another trick to get full HTTP access is to use a program called "Secure-Me" (available in the Android market). To set up Secure-Me, run the app and, under the proxy settings, set 127.0.0.1 as the hostname and 4289 for the port. Once you have things set, click "turn on" and Secure-Me should launch your web browser, which now has full 3G Internet access over a secure connection.

While Secure-Me is a pretty simple way to get things going, it wasn't the first thing I thought of. Another, slightly more complicated, method is to use an SSH tunnel along with a remote proxy. You will need to have both a working SSH server (listening on port 443) and proxy. I won't cover setting these things up here (Google is your friend), but I will mention that I found the proxy called "Polipo" the quickest to setup (`http://www.pps.jussieu.fr/~jch/software/polipo/`), although many others should work as well (squid, privoxy, etc.).

To use SSH as your proxy you will need to download the Connectbot SSH client for Android (`http://code.google.com/p/connectbot/`). Once you've connected to your SSH/proxy server with Connectbot, hit the menu key and go to the port forward option. Here you'll want to set up a local port forward, with the source being a port above 1024 (I used 2200), and the destination being 127.0.0.1:#### (with #### being the port your remote computer is running its proxy on.

Once you have a proxy running with SSH, the next step is to get your web browser using it. The easiest way to do this is using a program called Anonymous Proxy (Secure-Me can also be used, as its mostly the same program). Once you have Anonymous Proxy installed on your Android, point it to the host of 127.0.0.1 and whatever port your proxy is running on. After enabling the proxy, all browser traffic will automatically be tunneled over your SSH connection.

Since we are limited to only using port 443, or tunneling over a proxy, lots of Internet enabled apps (including maps and the Android market) will still require use of WiFi or an active 3G subscription with T-Mobile in order to function properly. Although it may be possible to get these applications running over a tunnel, so I will leave it to my fellow readers to discover more.

Greets and thanks to: BeautifulPyre, ExVx, xDarkxAnarchyx, JohnnyLinux, Metaphorge, Tyrsalvia, Casual.Sadist, PCPPirate, Phone Losers Of America, and everyone at FreeGeek PDX.

Why Cell May Die in a Modern Hacker's World

by Ron Overdrive

0x00 Preamble

As we move forward with technology, it's becoming quite clear that we're turing into a wireless society. One would think that perhaps cell phone technology would excel as king of the digital airwaves but, surprisingly enough, 802.11 technologies are becoming more and more advanced, providing faster speeds and longer ranges than ever before. In urban and suburban areas, you would be hard pressed not to find 802.11 WiFi signals while wardriving, relaxing at the mall with friends, passing through an airport, or staying at a hotel. For those of us who live in densely populated areas, it's everywhere. For the most part, it's the same deal for cell phones. With portable devices such as netbook computers, iPod Touches, iPhones, Android phones, and other smartphones, it is possible to access the Internet easily with a WiFi connection if you have a poor cell signal or are roaming. For some of us, this opens up the door to a lot of savings, considering some devices like the Nexus One cost roughly $500 without service and around $200 plus $60+ a month with service. What I'm going to do here is tell you how to completely end expensive service fees *legally* and have those devices pay themselves off instead of taking a chunk out of your wallet.

0x01 Disclaimer

Before I continue, let me state the legality of this method is dependent on what WiFi locations you use. I take no responsibility if you're using a residential, unsecured WiFi router and you get caught. I highly recommend this be done using public, free WiFi connections (such as you find in restaurants, hotels, and airports), WiFi networks under the control of your ISP, or secure WiFi connections you have legal access to.

0x02 Pre-Reqs

Let's start off with what you will need for this to work. You will need the following:

1. a Google Voice account
2. a SIP account with a call-in number
3. a SIP softphone app

If you don't already have a Google Voice number, you can easily search around for Voice invites on Twitter or other social networking services. If your SIP provider only provides SIP2SIP support, you can get a call-in number attached via `http://www.ipkall.com/`. Various free softphones can be found easily online. Since I mostly use OS X, I use Blink. For the iPhone/iPod Touch there is an app called iSip, and Android devices can use SIPdroid. Android devices will also want to have the Google Voice app installed while iPhone/iPod Touches will want the iPhone Edition Google Voice page bookmarked.

0x03 Setup

Now on to the setup process. First, sign up with Google Voice, sign up for a SIP service (I use `http://iptel.org/`), register a call-in number for your SIP account, and install your softphone app. Be sure to read the how-to guide on your SIP provider's site on how to configure your softphone. For the most part, you usually just enter your username, password, and SIP domain. Now go into Google Voice and choose your Voice number; then add your SIP call-in number as your primary phone number. When you click "verify" you should get a call on your SIP app. Just dial the verification number and you're set.

Note: Android users should make sure their Google Voice app is configured to force all calls through Google Voice.

0x04 Usage

Incoming calls should be a no brainer; give out your Google Voice number as your phone number. When people call, they will be greeted by the Google Voice system and forwarded to you or to your voicemail, if you're not online. Outgoing calls are simplest on Android devices; you simply dial out and the Google Voice app should intercept your call. On the iPhone/iPod Touch, and portable computers, you will need to visit the Google Voice website where you simply click the call button and enter a number or name of the contact you wish to call (the SIP account should already be selected as the callback number). Google Voice will call your SIP account and then call the person you are trying to call, bridging the two calls together. Finally, SMS (text messaging) can be done using the Android app or through the Google Voice website.

0x05 Flaws and Final Thoughts

There's no such thing as a perfect solution and this is no different. While this offers great potential for saving money, there are a few flaws. First and foremost, one depends on a usable WiFi connection. While some may see this as a huge factor, it's actually insignificant. After all, that's what voicemail is for, which we all use on our cell phones anyway for the same reason: for one reason or another we are unavailable. Then there's the fact that outgoing calls and SMS can be a little more involved. Google is already working on this. Recently, they purchased Gizmo5 and they are planning on merging it with Google Voice, so the methods described may shortly become deprecated, if Google plays their cards right. Also, there are security concerns over using public WiFi connections that do not have AP isolation enabled, as any good hacker with working knowledge of the SIP protocol could potentially sniff your packets and listen in to your phone calls. Much like regular cell phones, and even hard lines, you always have to assume the line is insecure and not share any sensitive information. If you are willing to pay a small yearly fee for in and out calls, Skype is always a good alternative to using Google Voice and SIP. There are Skype clients for all platforms and Skype has the benefit of some encryption. Just remember, you get what you pay for.

Telecom Informer

by The Prophet

Hello, and greetings from the virtual Central Office! I say "virtual" because I'm in a very different place than usual: Beijing! Apart from enjoying the excellent Chinese food (it's much better here than in the U.S.) and exploring the vast subway system (one of the largest in the world), I'm helping to build a new Central Office. My employer is branching out overseas, and China is a recent new part of that growth strategy. It seems everything in Beijing is brand new after a massive effort to overhaul the city's infrastructure for the 2008 Olympics, and telecommunications networks are no exception. And whatever it is, it's busy! With the world's largest population, China needs a network with scale to match.

Globally, the telecommunications industry is moving in the direction of selling you bandwidth and letting you slice it into voice, data, video, or wireless while running a meter the entire time. Your bandwidth bill will be consumption-based if the telecoms have their way, much as your electric and water bill are today. Oddly enough, this was the original vision of Bernie Ebbers of WorldCom, who is now rotting in a Louisiana prison for securities fraud. I think ultimately we'll see data commoditized with value-added services becoming the differentiator. Companies will compete on price and content bundles.

For now, though, we're still in the buildout phase. Telecommunications networks are available, but are not yet ubiquitous. South Korea has long been the most wired place on the planet, and emerging economies like China are working hard to catch up. The U.S., frankly, isn't even on the radar screen. It's globally ranked 20th in broadband penetration, and I've given up on policy-makers there to think beyond their own corrupt self-interest. The real action is in emerging economies like China - there are ambitious plans here, and the wherewithal to implement them.

Professional challenges aside, you might wonder how, exactly, you pick up your entire life for several months and relocate halfway across the world? The answer in telecommunications terms is more complicated than you might expect. As much as we've grown into a society where you can be nearly anywhere on the planet within two days, it's still ridiculously complicated for something as simple as your phone to ring on the number it always has once you leave the country.

My primary phone line at home used to be a land line, but in the past few years, I've been spending the majority of my time away from home. Most of the time, people don't bother calling my land line anymore and just try my cell phone. Yes, I have a cell phone. I hate giving money to wireless providers, the non-union traitors of the telecommunications industry. Nonetheless, Sprint has a product that was hard to pass up: Boost Mobile CDMA. Coverage spans the entire Sprint network, and you can use most Sprint handsets (although this is an unadvertised perk, and requires a bit of social engineering to accomplish) for only $50 flat per month. It was a perfect plan for me, allowing everything from tethering my laptop to unlimited voice minutes and unlimited long distance. Certain numbers, like (435) 855-3326, are blocked from the Sprint network, but for the most part it's an incredible value.

Only one problem: there is no roaming. At all. Especially in China. And while call forwarding is available, and international rates are high but not outrageous, international call forwarding isn't available. SMS forwarding doesn't exist either. So I was stuck. Either I would have to set my outgoing message to redirect callers to another number, or I'd have to come up with something more creative.

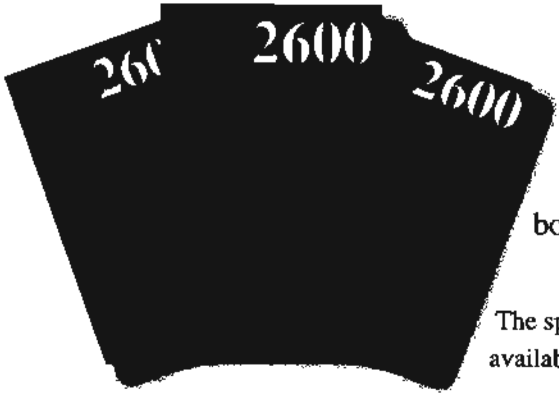
Unfortunately, there is only one creative option, and it's expensive (probably because it is the only available option): 3jam.com. Essentially, 3jam does the same thing as Google Voice, but they support porting numbers in and out, and they support international call forwarding (Google doesn't support either of these features). They also charge money, and the cost of the service provides some insight into what Google Voice may eventually charge (although I expect Google's product to be less expensive, since they have more users with corresponding economies of scale). 3jam can then forward your calls anywhere in the world (at relatively high rates), and they'll forward your SMS messages anywhere in the world too. You can also reply to SMS messages via a sort of SMS proxy server, similar to what Google Voice operates. Unfortunately, any SMS replies you send will be an international SMS to the U.S., which can be very expensive. China Mobile, the carrier I use, charges about 15 cents each.

I've seen a lot of VoIP providers come and go, and it's occasionally gotten ugly. According to myvoipprovider.com, 256 of them have gone out of business in the last five years. The biggest and most infamous flame-out was sunrocket.com, which literally went out of business overnight and disconnected all of their customers, the majority of whom lost their phone numbers. 3jam.com may be a perfectly solid company - I have no idea. Neither does the FCC. And I *really* don't want to lose the number I've had for ten years. So I left my phone number with Sprint (a company that's less likely to go out of business), signed up with Google Voice, and changed my voicemail greeting to redirect callers to my new number. Unfortunately, people who only text and never call won't ever find out my new number, but you always lose a few friends when you change your phone number. I'll manage.

A bucket of ink has already been spilled writing about Google Voice, so if you're not familiar with it by now, you've probably been living under a rock. Google allows just about anyone with a U.S. phone number to sign up for an account, so get one and play with it (www.google.com/voice). Google doesn't allow call forwarding to international numbers. However, my employer does (via its international VoIP network), so I forwarded my business line to my mobile phone here in Beijing and forwarded my Google Voice number to work. It works fine, although there's plenty of packet loss and a 500ms delay. It's almost like the good old days using C5 satellite trunks.

I also have broadband in the apartment my company arranged for me, so I decided to install VoIP. For some reason, many people think that since Gizmo5.com has closed to new signups since being acquired by Google, it's impossible to get a SIP account that works with Google Voice. There is an easy workaround. I signed up for a free account with callwithus.com, configured it to work with my Linksys SPA-3000, and pointed a free ipkall.com number at that. In turn, I pointed my Google Voice number at the ipkall.com number. And - get this - it all works fine! If I'm home, I just answer the VoIP line rather than my mobile phone. Call quality is excellent - so good, in fact, that callers have no idea I'm talking to them from across the International Date Line. And best of all, the latency is - while noticeable to me - not noticeable to most people. Outbound calls back to the U.S. and Canada cost less than one cent per minute.

And with that, it's once again time to bring this column to a close. Have a safe and enjoyable summer, wherever in the world your life takes you! And do drop me a line if you're in or near Beijing.



Call the World for Free (on someone else's nickel) with Universal International Freefone Service

by BitRobber (BitRobber@gmail.com)

This article is not another article teaching you how to use VoIP to make calls (with shitty quality!) to overseas for small fractions of pennies. Instead, it's an exploration of a neglected corner of the phone system. Interesting things often collect in dark corners.

I've tried to make this a concise summary of nearly everything I know about an unusual subject. As such, it will be dense.

You probably know that it's possible to dial international calls at a horrendously expensive rate right from the telephone in your home, or cheaply over a lousy connection using the Internet. Perhaps you've sighed at the expense, wishing that you were able to call overseas cheaply and without the hassle of VoIP. (Er, I know I have.) Your wait may be over.

In 1997, the International Telecommunications Union (`http://www.itu.int/`) created a system called Universal International Freefone Numbers (UIFNs). In a nutshell, they defined a *non-geographic* country code, +800, to which calls are toll-free from all of the participating nations. UIFNs are of the format +800 XXXX XXXX (to dial, replace + with 011 in the US, 00 in Europe, and so forth). The actual phone line that your call will go to is at the discretion of the owner of the number, and can be any phone number in the entire world. They can contract with their carrier to have it route to different call centers depending on time of day, traffic load, and so forth.

Just like 1-800 numbers in the United States, these calls reverse bill. The recipient gets to pay through the nose while the caller (you!) gets a free call. A common rate structure for this service is a per minute incoming rate, on top of which there may be a charge per day or per month for having the number allocated and routable.

The benefit of a UIFN to a number holder is that they offer a uniform dialing format around the world. This is especially useful in Europe, where a corporation may do business in multiple countries with widely varying toll-free number schemes. They can save money with one set of business cards and advertisements.

Behind the Scenes

I'm going to address this from a United States-centric perspective, since that's the phone system I know the most about.

When you start by dialling 011, the phone switch flags that as an international call. It collects all the digits you dial, and then passes them on to your preferred long-distance carrier for routing and billing.

Your long-distance carrier then must look up the terminating carrier for the call. The ITU maintains the master list of terminating carriers for UIFNs, but this list isn't used to route calls. Instead, each originating carrier is supposed to maintain its own UIFN routing database. When it's figured out the terminating carrier, it hauls the call to a location where it peers with that terminating carrier, and hands it off to them.

This is different from standard international call routing, where the country and city code is translated to a physical network location, where the call is then handed to the preferred carrier (usually the cheapest).

Notably, it's also different from the United States' toll-free routing scheme, where the number you dial is translated, by a central database, into another 10-digit phone number and then routed normally.

Each originating carrier maintains its own database, as I said earlier. Let's say I'm to request a UIFN from British Telecom, and I want to have it be reachable from Denmark and Sweden. I tell this to British Telecom, and they get a number from the ITU for me. Then BT, as the terminating carrier, talks to all the Danish and Swedish international carriers (Tele2, TeliaSonera, Unisource, and TDC) to get them to add the UIFN to each of their databases as "routing via British Telecom". Each carrier must then place a test call to British Telecom to ensure the number routes properly.

Billing

No discussion of telephony would be complete without a section on how the billing is done. A phone company without a billing department just isn't a phone company.

That said, I don't know for certain how inter-carrier settlement occurs for calls made via UIFNs. I suspect that settlement agreements are negotiated pairwise between individual carriers, similar to how the calls themselves are routed. I haven't confirmed this, however.

Where can I expect to use UIFNs?

UIFN dialling is little-known and patchily implemented in the United States. Some landline switches will accept dialing of UIFN calls, and some will reject them before you're even done dialling. Whether the call actually completes is up to your long-distance carrier. Sprint's, AT&T's, and MCI's long-distance operations all route UIFN calls properly, provided their routing databases contain the number. Qwest's doesn't, and I can't say for sure whether anyone else does either.

My Qwest 0 operator and her supervisor both denied the existence of country code 800. When I asked why my calls were going through, they were at a loss for words, and said to call the business office. The Sprint long distance rate-and-route operator, however, told me without hesitation that it's a free call that I can dial myself.

And dial I did.

No payphones that I've tried will let me dial UIFNs for free. The FCC requires payphone operators to allow users to call toll-free numbers for free. This doesn't apply to UIFNs. Payphones in my corner of Qwestland (which are operated by FSH Communications) give a CBCAD recording, the same as when you dial any out-of-LATA numbers.

Out of the five cellular carriers I have access to (T-Mobile, AT&T, Verizon, Sprint, and Nextel), only Nextel and T-Mobile routed my calls properly. Notably, AT&T insisted on routing my calls to "+800-ABCD-EFGH" to "+1 800-ABC-DEFG". This surprised me, as I expect AT&T to have the least amount of pretend telephony in their network. Their long distance service, for example, is usually top-notch. Further proof that AT&T long distance is completely separate from AT&T Mobility.

Both of the T-Mobile customer-service people I talked to denied that country code 800 exists. A call will go through on T-Mobile, if you have international dialling allowed on your line. (T-Mobile uses AT&T long distance service, so this is sensible.)

If all this fails you, it's still possible to call UIFNs. From nearly all landline phones in the United States, you can dial 101-0288-0# to get AT&T's operator platform. At the prompt, you can then dial 011-800-ABCD-EFGH and your call will go through. You oughtn't get billed for this call. Other PICs (101-XXXX codes) that I've found to work are MCI's (101-0555, 101-0222, 101-0888), and Sprint's (101-0252, 101-0333, 101-0872). Some of these work only when you dial 101-XXXX-011-800-ABCD-EFGH, while others only work when you call using the operator or menu system, via 101-XXXX-0#.

You can't dial PICs from cellphones. Your final refuge here is the wide range of prepaid phone cards and operator service lines. Since these tend to be made of Asterisk and pretend telephony, I can't imagine that very many route +800 calls at all. The only one I have available is from Verizon. The card platform doesn't route it, and the card platform's operators refused to dial it for me.

I've mostly given up on trying to get operators to do their job properly. The nice man at AT&T's free 1-800-OPERATOR service let me call a UIFN once I told him that it didn't work from my cellular phone.

I've had so many arguments with operators in the past few months about whether 800 is a country code or an area code in the US, it's ridiculous. I try to make it clear that I want to dial country code 800. The operator then asks what country that is. I say it's international toll-free. Then the ovperator says either "but where does it go?" or "that phone number is too long, phone numbers are 7 digits". I've had moderate success simply saying that the number goes to Germany.

On top of all this hassle, most UIFN owners choose to not have them reachable from the United States. This may be because it's cheaper to simply get a +1-800 number in the United States and then forward it overseas, than it is to support customers who sometimes can't dial you and don't know why not. It's a horrible mess over here.

What can I do with UIFNs?

That's the $25 question.

As someone on the Internet said, "hand-scanning is the pastime of bored phreakers everywhere". It's a bit of a pain, but there's no better way to find interesting things on the phone network than dialing a bunch of sequential numbers and listening carefully.

You can query the UIFN assignment database at `http://www.itu.int/cgi-bin/htsh/uifn/search/uifn.form` so that you don't waste your time scanning non-allocated phone numbers. Even then, most of the numbers that searches bring up won't complete from inside the United States.

Already, mining search engines for UIFNs, I've found at least a few conference bridges. Think of that - maybe you can get a whole IRC channel on a toll-free conference line, courtesy of some corporation you've never heard of.

It's also just fun to hear the circuits connecting sometimes. Many UIFNs allocated by Deutsche Telekom are broken in interesting ways (e.g., +800-2255-3241 or +800-2255-5888). AT&T's worldwide business customer support hotline at +800-2255-4288 (800-CALL-4-ATT) lets you press 4 over and over to stack up international circuits. There are a bunch of other interesting things out there waiting to be found, and I've only explored the range +800-2255-XXXX in depth.

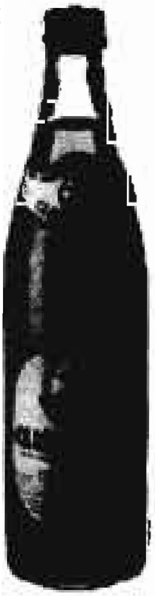
Resources

The ITU website, `http://www.itu.int/`, is full of information and is hard to navigate.

If you want even /more/ detail on how UIFNs get activated, the procedure is described on page 13 of E.152, which lives at `http://www.`
`➡itu.int/rec/T-REC-E.152-200605-I/en`

The listing of UIFN providers, by country, is available at `http://www.itu.int/cgi-bin`
`➡/htsh/uifn/uifn.operator_contact`
I'm assuming that these are also the carriers of last resort.

The International Inbound Services Forum operates a database of carriers offering to receive international calls at `http://`
`➡www.iis-forum.com/cms/index.`
`➡php?page=factbook`



How to Create Mass Hysteria on a College Campus Using Facebook

As we college students know, Facebook has become a popular venue to voice opinions and gather a following. Events, groups, fan pages, and causes now plague a site that was once renowned for its clean interface and lack of spam. Everyone wants to throw the next raging party, petition for political change, or get everyone to become a fan of "peeing with the door open." What's popular on Facebook is now the obvious choice for dorm room small talk.

I attend the University of California, San Diego. One day, I decided to investigate the "Find People" function on UCSD's homepage. This search function allows you to type in an undergraduate's name, and it will return their school issued .edu email address, physical address, and occasionally their cell phone number. Now, you'd think that this search would only match exact full names, such as "Blake Thomas," in the event that you needed to contact Blake Thomas for some reason. However, if you search for just "Blake," it returns the information for every undergraduate student named Blake.

Now obviously I saw some potential for abuse here, so I downloaded a list of common Asian, Caucasian, and Indian names and ran a dictionary attack against the search. There were no preventative measures in place, and I was able to harvest 14,000 emails, 13,000 physical addresses, and over 7,000 cell phone numbers for students on campus. Every school in the University of California system has this same vulnerability, as far as I know.

I then wrote a simple script that would shuffle those 14,000 emails randomly, and spit back 500. This is Facebook's maximum for an email contact import through a .csv file. Fake email accounts were created on Gmail and Yahoo, and fake accounts were made on Facebook. The two most crucial aspects of a fake profile are that it must be a woman (women won't friend unknown males, but males will friend unknown women) and that has direct face shots, but rather had some distance to them. It's easy to find stuff that fits the overall campus climate and apply them. Each account was also given some fake interests, political orientations, etc. and the wall and chat features of Facebook were disabled.

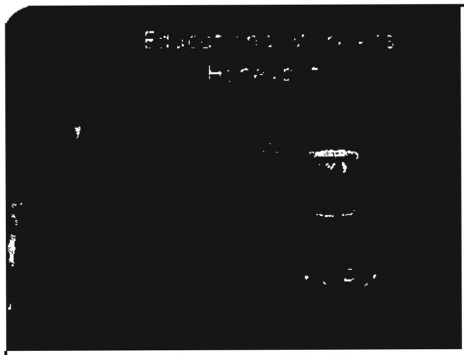
Once a bunch of profiles were made, I imported a randomized .csv list of .edu emails into each. Facebook matched profiles for roughly 300 of the emails imported, and friend requests were blasted out en masse for each profile. Within 24 hours each account had 150-200 friends. UCSD is a relatively prestigious school, and I am baffled by how successful this technique was and how little people know about the workings of the Internet and, in particular, spam (Internet license anyone?). Many people would send me a private message with "Do I know you?" I just ignored all of them.

So, obviously, I was waiting for the time to use these accounts to further a political point. I had at my fingertips that ability to make an issue on campus out of anything by mass inviting random students to some group or event. The perfect opportunity presented itself, as some of you may know. A few frat guys threw a racial party and one controversial campus newspaper, The Koala, dropped the N-bomb on student run television, making national news. UCSD's socially dead climate went into an uproar as the Black Students Union put forth six pages of demands to the administration.

My bots chimed in on the matter, and they ultimately affected the opinions of a couple thousand students on campus. Was this hard to do? No. Was it smart? Yes.

The potential for abuse through the aforementioned process is ridiculous. In certain situations, you could probably start a riot. It would be best if Facebook fixed this gaping hole but, until then, have fun. ;D

Disclaimer: I'm not responsible for anything you do with this article, or any ruckus you attempt to cause or do cause.



The following article provides several avenues of exploration, depending on the experience of the reader. For those who are unfamiliar with the concept of honeypots, or their implementation, this article provides enough information to create one of your own. For the savvy network hacker who is experienced in the design and implementation of honeypots, this article introduces a new use for them in the public sphere. The important point I wish to convey is that honeypots can be used not just as a security tool, but also as a teaching tool to educate the public about the security ramifications of open wireless networks.

First, let's start with the basics: a honeypot is a configuration of network services that is meant to attract, or distract, a threat. Originally, their purpose was to attract nefarious users who were attempting to break into a system. The honeypot can be used to attract the threat to a particular server where information can be gathered about the origins and methods employed. In less targeted use, honeypots are put on networks to simply distract potential threats from the core network services. Since a honeypot can be one or many services running on a network, there are many ways to implement them. The honeypot we will implement in this article routes all wireless network traffic to a particular server, without leaving too many clues about the redirection. The additional element of this honeypot is that it will provide the sandboxed user with information about wireless security. The recipe provided in this article is applicable to Linux, Unix, Mac OS X and Solaris, with few changes needed to get things running on each.

The operation of this honeypot is simple: an unprotected wireless access point is configured to broadcast an enticing SSID publicly. As users connect to the access point, their machines receive a private IP and DNS routing information from your DHCP server. The trick is that the information provided to the client causes it to route all web traffic to your server, even when the user types in a public DNS name such as "www.cnn.com". Where this honeypot diverges from other common uses is that instead of gathering information about the client or routing them to an offensive website, the user is directed to a page that explains the issues surrounding unprotected and unknown wireless networks. In essence, the honeypot is being used as a tool to educate the general public about information privacy and security.

Honeypot Construction

OK, let's get started on our project. To construct this honeypot, you will need the following:

- ISC DHCP (`https://www.isc.org/` ➥`software/dhcp`)
- ISC BIND (https://www.isc.org/products/BIND)
- Apache Web Server (http://httpd.apache.org)
- Computer with network card (this computer will host the honeypot)
- Wireless access point (available for purchase relatively cheap these days)

1. Though the access point will be configured to be open and public, the honeypot itself will be operating on a private network that is not routable to the outside world. In this particular case, we're going to be operating on the 192.168.50.0/24 network. The honeypot server will be given the address 192.168.50.1. You can either choose to configure your server machine's ethernet interface to use only that address or, if you wish to keep it connected to other networks, create an alias of 192.168.50.1 on it. Consult your operating system's documentation for the best method of doing this.
2. When a user machine connects to the wireless access point, the honeypot needs to provide it an IP address on our private subnet. The DHCP server will be configured to hand out numbers from a pool within the private subnet range. After downloading the DHCP package from ISC, follow the standard Unix build and install process[1]. After that has completed, create the file `/etc/dhcpd.conf`. Open it in your favorite text editor and edit it as in Figure A. Along with a private IP address, the DHCP service provides the client machine with the IP of a DNS server to use when querying DNS names for HTTP and other services. This is set with the "domain-name-servers" option in the configuration file.

Figure A

```
# dhcpd.conf
# this file should be located in /etc
# This line sets the time for a DHCP lease to be 900.
default-lease-time 900;
# These lines tell our DHCP server that it is authoritative for
# the defined networks and should not update DNS files when providing
# an IP address to a machine.
ddns-update-style none;
deny client-updates;
authoritative;
shared-network "honeypotnetwork" {
subnet 192.168.50.0 netmask 255.255.255.0 {
# Here we configure the information which will be given to the
# client machine when it connects. These values are consistent
# with a 192.168.50.0/24 network.
option routers 192.168.50.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.50.255;
# This option tells the client machine to configure its networking
# system to use 192.168.50.1 for DNS queries.
option domain-name-servers 192.168.50.1;
# The max-lease-time denotes how long an IP can be "leased" by a
# client machine before it needs to be renewed.
max-lease-time 7200;
# This declaration tells the DHCP server to hand out addresses
# between 192.168.50.10 and 192.168.50.254.
# We're saving 192.168.50.1 through 192.168.50.9 for our server,
# access point and any other devices we might want to put in place.
pool {
  range 192.168.50.10 192.168.50.254;
  }
}
```

3. To answer the DNS queries of the client machine, we'll need to configure a DNS server. This DNS server will be configured to route all DNS queries to a local DNS zone file. In essence, you are creating a local root server. Download the BIND package from ISC and follow the standard Unix build and install process. After that has completed, create the file /etc/named.conf. Open it in your favorite text editor and edit it as in Figure B.

Figure B

```
# named.conf
# this file should be located in /etc
include "/etc/rndc.key";
controls {
  inet 127.0.0.1 port 953 allow { localhost; } keys {"rndc-key"; };
};
options {
  directory "/var/named";
  recursion true;
};
# In the entry below, we are creating a wild card which denotes that DNS
# lookups for all domains should be done against the "db.localroot" zone
# file
zone "." IN {
  type master;
  file "db.localroot";
};
```

4. Next, we need to configure the DNS zone file so that all DNS queries to the local root DNS service are all directed to the same server machine. To do this, we create the "db.localroot" file in /var/named/ and configure it to map all host names to our server as in Figure C.

Figure C

```
# db.localroot
# this file should be located in /var/named/
# Time To Live - how long the record should be considered valid
$TTL 7200
# This block declares hostname.example.com the State of Authority for this
# domain and provides an admin email address (note the use of "." instead
# of "@").
@ IN SOA hostname.example.com admin.example.com (
        1 ; Serial
        3600 ; Refresh every 1 hours
        1800 ; Retry every 30 minutes
        604800 ; Expire after 7 days
        1 ) ; TTL 1 second
# This line provides the IP address of the nameserver for this domain,
# which in this case is the same machine.
        IN NS 192.168.50.1
# Here we define the basic A ("machine") record and a wild card entry which
# directs all lookups to the same A record address.
        IN A 192.168.50.1
*       IN A 192.168.50.1
```

5. In the next step of this project, we want to configure Apache to handle all incoming HTTP requests to the honeypot server. Download the Apache HTTP Server package from Apache and follow the standard Unix build and install process. Open the httpd.conf file for editing[2]. As in Figure D, create a VirtualHost entry for the server's IP address which points to a folder where the educational honeypot HTML files will live.

Figure D

```
### httpd.conf
### Section 3: Virtual Hosts
# This entry tells Apache to direct HTTP requests for 192.168.50.1 to the
# folder /var/www/html/ and log all the incoming requests at
# logs/your.domain-access_log
 <VirtualHost 192.168.50.1>
    DocumentRoot /var/www/html/
    ServerName 192.168.50.1
    CustomLog logs/your.domain-access_log common
 </VirtualHost>
```

6. In this step, we need to configure the wireless access point. By simply putting it on the same subnet, you can allow the DHCP service (and thereby DNS server information) to be passed to the client machines when they connect. In this example, I'm using an HP ProCurve Wireless Access Point 420. This is a slightly higher end access point than is standard for consumer networks. You can find cheaper ones at your favorite online computer electronics outlet. The process of configuring the access point with the appropriate information will vary for each device. However, you should be able to extract the basic idea from my example.

6a. You'll want to give your access point a static IP address on the private subnet. Alternately, if you are familiar with managing DHCP, you can add a static host entry for the AP in the dhcpd.conf file. In Figure E, you can see that I've given my access point the IP 192.168.50.9, which is on the same 192.168.50.0/24 subnet. Note also that I provide the server's IP (192.168.50.1) as the default gateway.

Figure E

```
HP ProCurve Access Point 420#show system
System Information
===========================================================
Serial Number       : TW525QB077
System Up time      : 0 days, 0 hours, 9 minutes, 19 seconds
System Name         : WIFx1
System Location     :
System Contact      : Contact
System Country Code : NA - North America
```

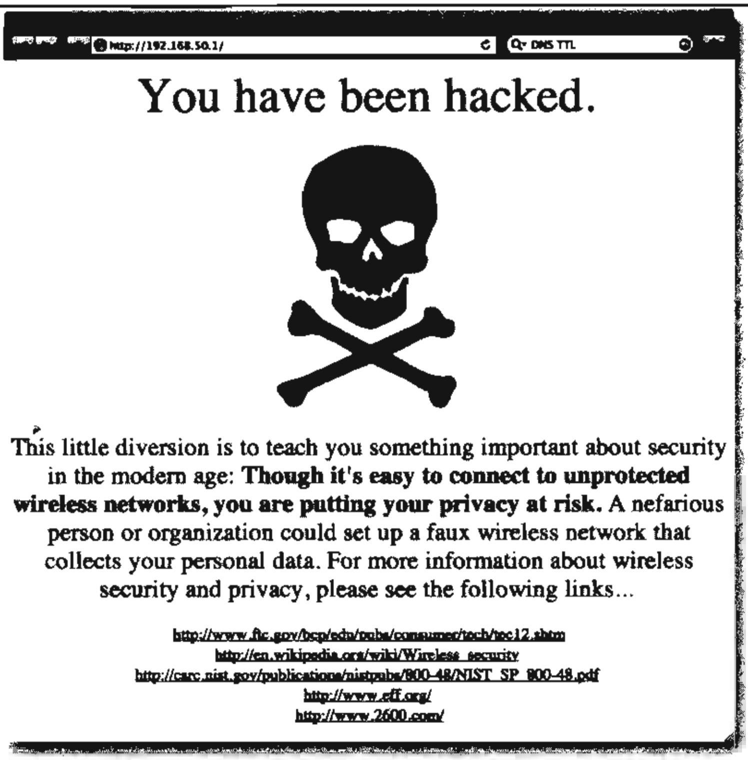
```
MAC Address           : 00-13-21-57-63-2A
IP Address            : 192.168.50.9
Subnet Mask           : 255.255.255.0
Default Gateway       : 192.168.50.1
VLAN State            : DISABLED
Native VLAN ID        : 1
IAPP State            : ENABLED
DHCP Client           : DISABLED
HTTP Server           : ENABLED
HTTP Server Port      : 80
Slot Status           : Dual band(b/g)
Software Version      : v2.0.38
```

6b. To attract users to your honeypot, you will want to give the access point an SSID that is enticing. As you can see in Figure F, I chose "Free Public Wireless". Anything with "Free" in the name is usually good enough to attract attention. You'll also want to turn off any authentication or encryption (WEP, WPA2, etc.). After all, this honeypot is meant to teach the dangers of unknown, unprotected wireless networks. The client will be able to associate with the access point easily, either by selecting it from a list of available access points in their network configuration or, if their machine is set to auto-connect to nearby access points, just by roaming within range of the access point. After configuring the access point, be sure to place it near a window, door or other area where it will achieve maximum range in the outside world.

Figure F

```
HP ProCurve Access Point 420#show interface wireless g
Wireless Interface Information
===========================================================
----------------Identification-----------------------------
Description                 : Enterprise 802.11g Access Point
SSID                        : Free Public Wireless
Radio mode                  : 802.11b + 802.11g
Channel                     : 11 (AUTO)
Status                      : Enabled
----------------802.11 Parameters--------------------------
Transmit Power              : FULL (13 dBm)
Max Station Data Rate       : 54Mbps
Multicast Data Rate         : 1Mbps
Fragmentation Threshold     : 2346 bytes
RTS Threshold               : 2347 bytes
Beacon Interval             : 100 TUs
DTIM Interval               : 1 beacon
Preamble Length             : LONG
Slot time                   : AUTO
Maximum Association         : 128 stations
----------------Security-----------------------------------
Closed System               : DISABLED
802.11 Authentication       : OPEN
WPA clients                 : DISABLED
802.1x                      : DISABLED
Encryption                  : DISABLED
----------------Antenna------------------------------------
Antenna mode                : Diversity
Antenna gain attenuation
            Low channel     : 100%
            Mid channel     : 100%
            High channel    : 100%
===========================================================
```

7. Create the HTML file that the client will be directed to when they type an address in their browser. Again, the point of this honeypot is to educate the user about the pitfalls of unknown, unprotected wireless networks and privacy on the Internet in general. Spend some time writing up a web page that explains why the user didn't end up where they expected on the web and why they might want to consider approaching their Internet experience with more caution in the future. Below is the page I created for this purpose. Note that I included links to technical and non-technical learning resources on network security/privacy that the user can bookmark.



You have been hacked.

This little diversion is to teach you something important about security in the modern age: **Though it's easy to connect to unprotected wireless networks, you are putting your privacy at risk.** A nefarious person or organization could set up a faux wireless network that collects your personal data. For more information about wireless security and privacy, please see the following links...

http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec12.shtm
http://en.wikipedia.org/wiki/Wireless_security
http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
http://www.eff.org/
http://www.2600.com/

8. The next stage of this process is to turn on the DHCP, DNS and HTTP services. With most OS/distributions, you can do that with the following commands in the terminal:

```
[root@machine ~]# dhcpd -cf
➡/etc/dhcpd.conf
[root@machine ~]# named
[root@machine ~]# apachectl start
```

9. Wait. If you've set this up in a populated geographical area, you'll likely see connections pretty quickly. For example, on a busy college campus or urban housing area, you'll likely catch some users in the first few hours. Check the Apache logs periodically to see if you are capturing some web queries. You can also look at the DHCP lease file to see what machines have requested an IP[3]. With any luck, you'll be attracting, and educating, users in no time.

Conclusion

Though I focused on unprotected wireless networks in this article, the principals outlined within are applicable to any networked interaction. Educational honeypots offer great possibilities for teaching the general public about the issues surrounding network security and privacy. They rely on the tendency of users to search out easy, convenient, and free solutions. By injecting a little monkeywrench in their plans, and directing them to information about protecting themselves, you can improve the level of secure communications on the Internet and the level of discourse on issues of privacy and security in the networked age.

Pan is a connoisseur of interactive computing, science and education. He lives somewhere.

Footnotes

[1] A common compilation/build/install process for Unix software requires that you "cd" to the software directory, run "configure", "make" and "make install" (in that order). The three packages above use this process.

[2] The httpd.conf file's location will depend on your OS/distribution. For Apache 2 on Red Hat Enterprise Linux the path is /etc/httpd/conf/httpd.conf. On Mac OS X Leopard, the path is /etc/apache2/httpd.conf

[3] Generally, the DHCP leases file resides at /var/db/dhcpd.leases

I'm not a number

by Poacher

The more complex a system is, the more difficult it is to know its vulnerabilities. This is an axiom that every hacker instinctively knows. As new technologies emerge, they are often bolted onto existing processes, creating a Frankenstein's monster of stitched together technologies and procedures.

Such is the modern supermarket. The relatively simple concept of a customer selecting groceries and taking them to a checkout, where they are totaled up and paid for, is now complicated by a large number of add-ons.

What we're looking at here is a convergence of three of these; the barcode pricing system, the loyalty card, and the self-service till. The three of these produce the conditions for two exploits. Both of these are dishonest and crimes, and I don't advocate carrying them out. The information presented here is merely to illustrate how a multi-billion dollar industry can inadvertently leave itself open to loss.

I'll start with barcodes, which I'm sure most readers will be familiar with. The basic system, still in use today in much of the world, is a 12- or 13-digit number, called either a UPC or an EAN, encoded in black and white lines. This number, often also written in decimal beneath, is used to uniquely identify the item and can have information such as the country of origin and manufacturer encoded into it. In the next few years, we should begin to see slightly larger, more complex codes come into widespread use. Such technologies are already being used by a number of shipping companies.

Interesting information on barcodes can be obtained from these websites:

- `http://en.wikipedia.org/wiki/Barcode` - general information on the "humble" barcode.
- `http://www.upcdatabase.com/` - the UPC database project
- `http://barcode.wikia.com/wiki/Main_Page` - a barcode product database

When the item's barcode is read by the till scanner, obtaining the UPC code, the till then accesses the company's database for the item description and current price. This is then added to your receipt and your total bill goes up the requisite amount.

The first and simplest exploit here requires a laser printer, a stack of sticky labels, and some bare faced audacity. Find yourself an online barcode generator, such as `http://www.barcodesinc.com/generator/index.php`, or just search for one, as there are many available. Alternatively, you could obtain a custom barcode label printer. Next, obtain the UPC for a low-price item in stock at your local global corporation supermarket. A tin of baked beans is a good choice that costs pennies. Now, you're probably ahead of me here, print out as many labels as you think you will need. Shop till you drop and go to the checkout.

At this point, the beauty and simplicity of the self-service checkout becomes blindingly apparent. Going through a checkout manned by a clerk runs the (albeit very small) risk that they will notice the DVDs, Laptops, fillet steak, champagne, etc. that is bagged up appears as baked beans on the till each time. The self service till runs no such risk.

There are, however, a few caveats. Many supermarkets have a supervisor overlooking a bank of self service tills with a screen showing what's happening on each till. The trouble is they are often pulled away most of the time to deal with customer queries and in practice are not monitoring what's going on. Also avoid items which require an EAS security tag to be removed as that will draw a staff member to your till. The same goes for items which require age verification.

Some stores also use a system that senses items being placed in the bags. I'm not sure yet if it uses weight, vibration, or an electromagnetic field, but it beeps annoyingly if too many or too few items land in your bag.

The biggest challenge in all of this is replacing the original barcode with your sticker. I leave how to do this to the reader's inventiveness. Price tag swapping is as old as the hills and any half-decent store detective should be alert to that. But all problems are there to be solved and, off the top of my head, ways around this could range from sleight of hand to getting a job at the store (or at least looking like you do).

The beauty of this exploit is that any losses will not be discovered until a stock take, or until the store orders a thousand cans of beans because they think they have been selling so many. Even then, there will be no way of knowing how and when the items left the store, so CCTV will be useless.

Just to reiterate, doing this is fraud. If you actually did this and got caught, you could go to jail.

Anyway, onto the second exploit, which to my mind is much more elegant and amusing.

Many stores offer loyalty cards. On the face of it, this is to reward loyal customers. In reality, it's a cynical method of obtaining large amounts of corporate intelligence on you and your family. Which, by the way, is sold off to one of a couple of large, multinational companies that keep huge databases about everyone in the Western world and thence into the hands (for a price) of the government. But that's a whole other story.

One of the largest retailers local to me has an extensive loyalty system that basically gives you 1% of what you spend back to you every so often to spend at the store. On the self service tills for this store, you can input your loyalty card details by scanning the barcode on the back of it.

Here is vulnerability number two. Obtain a loyalty card and, using the barcode generator, produce a large number of stickers with its barcode. Place these on a large number of products, more or less at random around the store. This time, you are not putting them over the original barcode. What you are aiming to do is place them above, below, or to the side of the barcode. This is so that, when the item is scanned, the reader will pick up the proper code but, as the item is rotated or passed over the sensor, it will also read your loyalty card number, thus tying that whole transaction to your account.

Done correctly, and with a little luck on a busy Friday or Saturday, in a large store, you could run up tens of thousands of points, giving you 1% of that back to spend as you wish in the store. With the additional benefit that you are corrupting the data on customers' buying habits that the store is painstakingly building up.

This is still fraud and, eventually (particularly if you use the same account for too long), the store will pick up on this strange customer who comes into the store 400 times a day and spends hundreds of thousands a week. You can't spend loyalty points in prison.

"The large print giveth and the small print taketh away..." - Tom Waits "Step Right up" 1976.

How I scored the Avaya PBX init password

by The Funkster Deluxe
(funk@forethought.net)

I've been in training this week for the Avaya Interaction Center 7.2. The catch is that the last published training from Avaya University (administered, I believe, by Accenture–an outsourcer) is IC version 6.1. Nothing like the present to update your training, eh guys. We understood that we would get a Professional Services trainer to lead us through training while an Accenture representative stood by a wrote a new 7.2 class based on our training.

It worked out differently in that the Accenture trainer, a guy flown in from Mumbai, lead the class for the first three days and, suffice it to say, he didn't really have the "trainer" type personality.

He had a virtual image of his desktop with an encapsulated and fully (or mostly) functional IC 6.1 system, appropriate databases, workflow designer and so forth.

But this wasn't enough by itself, as a big feature of Interaction Center is the Voice Channel. So he had a Definity (Avaya-branded telephony) simulator that went by the acronym "dads."

This platform was so unstable that I couldn't even get it running the first day. It launched from a batch file on the desktop that would flash a DOS screen and close. Curious, I ran the path from a cmd prompt so that I could see the error. I got some sort of "orys stty16" error. I pointed it out to the trainer, because I needed this fixed to proceed with training. He shrugged his shoulders and went back to whatever it was he was doing. Awesome!

Eventually I got it working after rebooting, but the simulator still was not acting right. Telephony services would stop mid-session, I had to rebuild VDNs (call routing numbers) whenever they were mysteriously lost, and I had a host of other problems.

When I launched the Simulator too early (before other necessary processes were started), it got stuck running the batch file and was sitting at the login prompt. The login was init.

I figured the login/password pair had a good chance of being in the batch file. It actually pointed to another file in the /dads subfolder, something like sat-def.rc. I opened it with Notepad and there was the init login, password, and another eight or nine lines–all unencrypted.

A bro that I work with had loaded Avaya Site Administration, for customer access, on a different training PC. We attempted to use this on our lab S8500 PBX and, sure enough, it succeeded.

The next prompt was a Challenge/Response field, with the former populated with a numeric string. I didn't care to get in any further, because of the legal or security ramifications, but I suspected that the other fields in the unencrypted password file were a sequence for this.

I can't figure out why these simulators require init level access, but if this doesn't constitute some sort of non-disclosure violation between Avaya and Accenture, then I don't know what does. Accenture basically handed us Avaya's deepest level password, which is used for enabling right-to-use licensing on the features from which Avaya makes tons of money.

I won't share this password, obviously, and it's possible that Avaya can change it across the board, but not without much expense and embarrassment.

The Hacker Perspective

The Next Generation

It's usually found on this page and has featured commentary and experiences from some of the world's most prolific hackers. But now it's time for a change.

We want to hear from those of you who don't have household names - at least not yet. Fame is not a requirement to understand and experience what hacking is all about. What is needed is a desire to learn and experiment, plus the ability to tell your story.

So whether you're still in high school, pursuing an active career, or retired from the military, we want to hear your story. Basically, we're looking for answers to these questions:

- What is a hacker?
- How did you become one?
- What experiences and adventures did you live through?
- What message can you give to other aspiring hackers?

Obviously, these questions merely form a framework. The bulk of the piece will be of your own design and choosing.

The column is a minimum of 1500 words and if we print it, we'll pay you $500. We will notify you only if your submission is accepted. Please don't use weird formatting - ASCII, Rich Text Format, or Word documents are fine. Grammar and spelling are important and their proper use will greatly increase the odds of your piece being considered. But the most important element is an interesting and compelling story.

Send your completed submissions to: articles@2600.com and indicate that it's for the Hacker Perspective column. You can also send it via snail mail to:
2600 Hacker Perspective
PO Box 99
Middle Island, NY 11953 USA

WHY YOU NEED A GRIMOIRE

by Leviathan

No matter how long you have been hacking, surfing, or working in IT, and especially in these uncertain times when your activity can be sniffed, parsed, logged, and archived, you need a grimoire.

Dictionary.com defines a grimoire as "a manual of black magic (for invoking spirits and demons)." Those of us who have been pushing bits around for some time know that the things we routinely accomplish can sometimes appear to be black magic to the less technically adept among us. The sheer volume of information we have stuck in our craniums and bookmarks, and our ability to Google with precision, gives us an edge in finding and implementing all sorts of technology magic. This is all good.

But it's not perfect, you know. We forget things. A website that we KNOW contained the answer last week, is suddenly gone. The transient nature of that big beast we call the Internet means that all content is in flux. And by the way, are you tired of the many tech support sites, powered by ad after ad, where you have to register before they'll let you click on the answer to your question?

To paraphrase Dennis Hopper: "You, my friend, you need a grimoire."

To the uninitiated, it looks just like a plain, bound notebook. But to you, and to the minions who watch in awe as you use it, it is truly a book of spells. You have the answers, because everything of value you've come across in your technology dealings, you've recorded faithfully in your grimoire.

A grimoire is not pretty. It's not always well-organized. But the answers are there, because you put them there. It's your insurance policy, your journal, your database. In time you will come to know exactly where everything is.

Best of all, it's private. No amount of ISP chicanery, keystroke logging, or site mirroring will ever create another copy of your grimoire. It will never slip you a cookie or prompt you to install another damned plug-in.

That, ummm, marginal URL that you really don't want in your bookmarks? Into the grimoire it goes. Default (factory) passwords? Never know when you'll need those. Write 'em down.

That UNIX command with a mile-long, unreadable man(1) page? Write down exactly how you use the command in real life, using only the options that are most useful to you. That unsupported hack that made your video card come alive... what happens if you have to reload the OS? Catalog it with care.

Account names and passwords: be careful here. Most of us have a handful of good, strong passwords we use all the time. Write down only the first two or three characters, and fill in the rest with random letters. Same with user IDs. No unintended reader will ever determine your complete password from w9xxxxxxxx. But knowing the starting letters will allow you to remember it.

And while that high-priced storage specialist is on site, why not make a few notes while looking over her shoulder? Phone numbers, support contracts, public keys, small but valuable scripts; these are all good candidates for your personal archive.

Now this part should be obvious: my grimoire goes everywhere I go, no exceptions. It's always available to me regardless of where I am or what other resources there are.

If you accumulate as much information as I have (my grimoire is about twelve years old, with new entries written in the margins now), you and your book will become the stuff of legends. When I walk into a meeting and put it down on the table, I inevitably get the question, along with a stare of admiration: "Is that the book?" I smile in reply.

And if, saints forbid, you should ever be in an embarrassing legal situation and you have to get rid of its evidence quickly, tear out the offending pages, shed a few tears, then flick your Bic. Let's see you clean up a hard drive that cleanly. Privacy, my friends; it is priceless. If your dealings are not quite that dramatic, your grimoire is a good reference at review time or when preparing your resume.

So spend a few wise dollars and obtain a good quality, bound notebook with lined archive paper, and start filling it with your accumulated IT wisdom. You and your grimoire will make history.

A salute to all my mates, in the gutter and among the stars. I also want to thank everyone who had kind words for my short story, "The Particle," that appeared in 26:1. Though it was fiction, you'd never believe the parts that were based in fact.

(POTENTIAL) LAPTOP RECOVERY

by Twisted Uterus
(twisteduterus@gmail.com)

My goal was laptop security/recovery by combining a few simple (and free) programs for a low tech recovery.

If one of my laptops was ever lost or stolen, I'd hate to lose the laptop as well as give the thief the additional bonus of a copy of my personal music collection, etc. I figured if the thief was anyone who knows anything about PCs (*2600* readers), they would just reformat the laptop and I would never see it again. But if the thief weren't too savvy, I might be able to recover it. What I wanted was a way to connect to it, wherever in the world it ended up. This way, I could see the actual desktop to see what files the thief was looking through. Then I could delete any personal info, render Windows useless, or maybe even force a pop-up window saying "I see you. I know who you are. Return the laptop and I won't contact the police!" Imagine his face then! Then I thought, since there is a cam on the laptop, could I actually see his face?

I always hated using passwords, but it's the first step in security. My logon name is now "tel_###-###-####" (my cell number), just in case an honest person finds it and turns it on...

I was already using a combination of PCAnyWhere and IP Mailer to take remote care of the PCs of 5 people who know nothing about computers. (It's just easier to talk on the phone with them as you move and click their mouse around on their own screen and teach them how to compose e-mail.) IP Mailer would send me an email with the new WAN IP address anytime the laptop connected to a different IP address. Of course, all 5 people have dynamic addresses and IP Mailer just made it easier for me to reconfigure PCAnyWhere so I could connect to the host at a new address. My only problem was SSL. If I used a Cablevision account, and then plugged the laptop into a Comcast modem, it wouldn't let the mail go out. I know there are similar programs out there that will handle SSL, but since my other dilemma was; what if someone connects my stolen laptop behind a router/firewall? It wouldn't forward any ports to the stolen laptop of course, so I couldn't connect even if I had the correct IP address. This setup just wasn't going to work for my recovery attempt.

I eliminated the problem by eliminating the need to know the laptop's current IP address. I now use Hamachi (freebie VPN) and let it run as a service so that it will start with Windows. I have uninstalled IP Mailer, as it is no longer needed. Now I can connect through Hamachi no matter where the laptop is, or how many firewalls it is behind! PCAnyWhere can connect to my stolen laptop through Hamachi and it works like a charm.

Now, behind the password screen, the laptop boots up Windows XP as well as Hamachi and PCAnyWhere (as host), so I could have full control of the laptop. I also used a registry hack to hide the PCAnyWhere system tray icon.

I assume, these days, that everyone **must** have wired or wireless access point at their home, and would connect my stolen laptop to the Internet. What fun is a laptop if you can't surf?

Then I also thought... Why not get the built-in webcam into play as well? That's where Yawcam (another freebie) comes in. Yawcam boots up with Windows (I have it running as a service, where it also runs "stealth") and begins streaming live video to the Internet. And, I can monitor it from **any** browser. Imagine accidentally leaving your laptop poolside at a hotel, only to come back later and find it missing! If you travel with two laptops, and I always do, connecting to the missing laptop and seeing who actually took it is an awesome possibility! You could be staring him in the face as he tries to guess your password. You could even capture a screenshot of his face and bring it to the front desk to I.D. him and catch him before he checks out. You could see him and he wouldn't even know he's being watched! How funny is that? At this point, I'd think the odds of getting your laptop back are very good. If you didn't have a second PC with you, I guess you'd have to wait until you got back to your home PC to begin your "investigation." I doubt the hotel would allow you to install Hamachi, etc. on their machines. Anyway, it works perfectly for my family's needs.

You have to pay for (wink wink) PCAnyWhere, but there are a few free remote access programs out there. I've tested this every which way I could, and haven't had any real problems. The only issue I have come across so far is that on my Dell Inspiron, the blue webcam light comes on and stays on. I don't want to permanently disable it (a.k.a. break it), or stick tape over it (too ghetto), so I am still looking for a registry hack to turn it off. Otherwise, it all runs just fine on my HP 2133mini and my Inspiron.

Access on Boingo Wireless

by ZoDiaC13

Preface

This article is about how to hack Boingo Wireless hotspots to gain free Internet access. For those that don't know about Boingo Wireless, it is a wireless hotspot service provider for many major hotels, airports and coffee shops. This story will explain my experience encountering it and what I did to unintentionally circumvent it.

Introduction

I work as a network technician at a company on the east coast of Canada. My job requires me to maintain connectivity from our site to many remote sites, via VPN, to offer up a Citrix web interface that hosts peoples' daily applications. I am also required to set up and maintain our and our users' hardware to adhere to a strict PC standard. This requires users to be set up on a company PC with limited user rights, restricting their PCs to be almost thin clients.

My first encounter with Boingo Wireless trouble was when a user who was traveling across the U.S. sent myself and others an email, upset about the fact that he paid to use Boingo Wireless at an airport and then was unable to install the required software on his laptop. Upon investigation, I found out that there seemed to be an installation required in order to use the hotspot. I think that this procedure is stupid because I'm strictly a Linux user, on my PCs anyway, and, from what I saw, they didn't offer an option to Linux users.

My Encounter

Fast forward to two weeks later. I was sitting in the Toronto Airport, passing the time by trying to get my girlfriend's iPod Touch onto the Boingo Wireless network. I recalled, from an article in *2600*, that disabling something in Safari on an iPod Touch let you somehow circumvent the pay-for option on certain wireless hotspots. I couldn't exactly remember what the hack was and, after some time, I gave up and decided to play games on it instead. My girlfriend soon piped up and said "Don't drain the battery; I want it for the plane ride." I told her to plug it into my father's netbook to recharge. I asked my father for his Windows XP netbook and plugged it in to recharge.

The Hack

While I was watching the iPod charge, my curiosity piqued and I decided to play around again. I always love scanning networks just for the hell of it to see what I can find. Since I had been using my father's netbook in my hotel room all week, I had installed Advanced Port Scanner (available at `http://www.radmin.com/products/➥utilities/portscanner.php`). This is a free, small, and robust port scanner for Windows.

I decided to do a simple ipconfig in the command prompt window to see my assigned IP address and the gateway IP address. I then plugged the network range into Advanced Port Scanner to scan the /24 subnet mask (essentially 255 hosts). This included the gateway (which was the wireless access point).

To my surprise, it showed me all the associated wireless devices connected to the access point and the software started to probe them for open ports. I figured there would have been some security measure in place on the access point, to circumvent such a scan. It also started resolving the computer hostnames on some computers, which was also helpful. I found one that looked interesting. The host was named "WINDOWSMOBILE96" and, based on the name, I could assume it was someone with a Windows laptop. The name seemed somewhat professional and logical, so the owner could be a business traveler. I assumed that if this person was on business, chances were they had probably legitimately paid for the wireless. So I decided that WINDOWSMOBILE96 would be my target.

I opened up the command prompt and issued the command:

```
nbtstat -a WINDOWSMOBILE96
```

For those that don't know, nbtstat is a Windows utility to help troubleshoot NetBIOS name resolution problems. The "-a" switch returns the NetBIOS name table and the MAC address of the network card on the named computer (i.e. WINDOWSMOBILE96). So now, after issuing the command, I knew the MAC address of the remote computer.

Now all I had to do was simply change the MAC address of my wireless card to the one that the nbtstat command spit out. I did this by going to "Network Connections" in the Control Panel, right clicking on my network card, and going to "Properties." Under the "General" tab, I clicked the "Configure" button to configure my wireless card. I then chose the "Advanced" tab and went down to the "Network Address" property. Not all network cards have this ability, but the one in my father's netbook did and I think it's a pretty standard setting. There are two values you can have with this property: "Not Present," which uses the burnt-in MAC address on the network card, and "Value," which allows you to set a different MAC address for your network card. I input the MAC address that I had obtained from the nbtstat command and saved the changes. My wireless card then disconnected from the access point and re-associated itself.

Now, for the moment of truth. I opened up Firefox, typed in google.com, and voilà! I was online. Like an idiot, I shot my fists up in the air and screamed, "Yes!" This raised my father's suspicions, so I turned the computer around and showed him Google's homepage, declaring, "I got on!" My father just shook his head.

Conclusion

I know this is a long-winded article to explain such a simple procedure but, like Hunter S. Thompson, I am writing more about the experience than the hack. The hack is about the experience. Like I said earlier in the article, I did this unintentionally, as I never really intended to "hack" wireless access but, based on previous experience, knowledge from reading many past issues of *2600*, and a basic curiosity, I stumbled upon a procedure that worked. I used the same troubleshooting and reasoning I would have used at a day in the office if I were faced with a similar issue. In my mind, I simply "fixed the problem." But that is what hacking is all about; a never-ending thirst for knowledge and the curiosity to take you to the next level. It's all about the mindset and how you look at things.

Also, as I mentioned previously in the article, I am mainly a Linux user and will install Linux on anything and everything I can get my hands on, provided the opportunity. I know there is a similar method that could be used in Linux to achieve the same results, but that is for another article.

There are other articles online about how to hack Boingo Wireless, but none that I could find used this procedure, which is mostly using the operating system and software as it was intended to be used, and thus exposing a vulnerability or loophole in the Boingo Wireless system.

I hope you enjoyed reading my article and may you all carry on the hacker mindset.

Thank you, and happy hacking!

How AT&T Required Data Plans Wor

(and How to Make Them Stop Working)

by excessive | offnetwork

Some time around the end of last year, AT&T Wireless started automatically attaching "Smartphone Personal" data packages to any subscriber line using a smartphone. These mandatory add-ons allow for unlimited mobile data use for $30 per month. If you are like me, you have two questions about this policy. First, what is a smartphone anyway? AT&T maintains a database of the IMEIs (serial numbers) of all the phones they sell, as well as some popular phones they don't sell, like the Google Nexus One. A phone must be in the AT&T database and classified as "smart" before a data package will be automatically attached.

If I put my SIM card in, for example, an AT&T branded Nokia E71x, the network will log the IMEI of that phone and automatically attach the required $30 data plan to my account. This happens before I use a single packet of data, simply because I allowed a phone on AT&T's list to register with a cell tower. On the other foot, if I put my SIM card in an unbranded E71, which is essentially the same device, no data plan will automatically attach to my account because that phone's IMEI is not in the database. This means that I am required to pay an extra $30 per month for the pleasure of using my E71x, even if I don't use any data at all. Meanwhile, the guy sitting next to me at the coffee shop with an unbranded E71 and $10 MEdia Net Unlimited has just tethered his phone to his laptop and downloaded 68 gigabytes of Justin Beiber videos like a total jerk. The short answer to question one is that a smartphone is whatever AT&T says it is.

This is America. I simply do not accept this type of arbitrary policy, and I refuse to pay for it. AT&T obviously has an interest in charging users an additional fee for using extra data and putting a greater strain on their network, but this system is analogous to a gas station charging more per gallon for gas it pumps into sports cars than gas than gas it pumps into minivans. Question two obviously becomes, "how can I get out of my required data plan?" One easy answer is to just say no to free Motorola Backflips, knowing that they will end up costing you in the long run; but that's not any fun, so let's try something else.

Every service that AT&T provides has something called a Service Order Code (or SOC, like what's between your shoe and your foot), which is a unique identifier that allows features to be accurately added or removed from an account. For example, if you want your phone to say "Off Network" when you are roaming, you can ask customer care to add the SOC "4EON" to your account. Some SOCs require a higher access level than others. If you want the Smartphone Personal data package that I hate so much, any representative that has access to your account can add "DPPB" for you. If, however, you would like 350 extra minutes per month for free, you will need someone who wears a suit to work to sign off on the infamous "BM350" (a pretty neat SOC that most reps don't think exists at all).

The feature we care about is called a "smartphone data exclusion," and it can be added by a floor manager in customer care with the "SMRTEXCL" SOC. A customer care manager is not the only person who can add the feature, but is probably the easiest path to success. This feature prevents the system from automatically changing the data plan on an account, regardless of what device you are using. Once the exclusion is added to your line, you can add pay-per-use data and avoid the extra fee or, like the aforementioned jerk, add MEdia Net Unlimited and watch kittycam all day, or whatever it is people do with unlimited data. Be warned that accidentally using 100GB of data in a month may get your account flagged for excessive data use, and you will suddenly be fancy-dancing your way out of service cancellation.

As a final note, most people would refer to the process outlined here as "social engineering," but I've avoided the phrase because I think that it implies exploitation. Obviously the point of this exercise is to exploit the AT&T account management system for the purpose of gaining value, but that can be accomplished without tricking people or treating them like garbage. AT&T is a faceless machine that would kill you without thinking twice, but customer service representatives are real people and generally seem willing to help. Lies and coercion are unnecessary in addition to being unethical. The next time you call 611 looking for discounts or bonus features, remember that you will catch more BM350s with honey than vinegar. Happy hacking.

Casual Encounters of the Third Kind: A Bayesian Classifier for craigslist

by Brian Detweiler

Introduction

Are you a single male? Are you looking for no strings attached sex? Are you looking for an easy way to pick up easier women? Then look no further than Craigslist Casual Encounters! It's the place to find thousands of single, horny women looking for exactly the same thing! ...or is it?

In this article, I scientifically examine the myth of Craigslist Casual Encounters. The focus has been placed on w4m (women4men) in the Omaha, Nebraska location. This research could (and should) be expanded to other cities, as well as other keywords.

The Idea

I have long held the belief that sexually frustrated men everywhere are being taken advantage of in our society. Everything from girls asking for free drinks at bars to pay websites like AdultFriendFinder.com charging money for finding women to hook up with. Craigslist, however, is free, minimalistically designed, and used by millions of people around the globe. It seems like the perfect way for someone to fulfill their desires and not be taken advantage of.

But where there are trusting people, there will always be enterprising no-goodnicks trying to ruin the fun for everyone. Enter the Craigslist spammer. How does one spam on Craigslist? There are two ways. The obvious, and quickly detected method of dropping website links directly in a posting, and the more underhanded, legitimate looking post that waits for users to email them so they can send them deceptive spam emails.

Make no mistake, this is spam. But unlike traditional spam, we are essentially opting in by viewing and replying to postings. Unfortunately, traditional spam filters work by catching incoming emails. The popular Bayesian spam filter keeps a database of words and their "spaminess." So, how could we apply that to Craigslist, to save us the trouble of unwittingly "opting in?"

Bayesian spam filters must be trained. We must start off with decently sized corpuses of spam and ham text. Then we are responsible for training the filter by telling it if a body of text is good or bad. When dealing with email, the case is as simple as collecting the email, going through it one by one, and flagging the spam. With Craigslist though, we are dealing with a website. We will have to go to Craigslist, rather than Craigslist coming to us.

The plan is relatively simple: scrape Craigslist at arbitrary time intervals (every three minutes seems reasonable), logging entries into a database. When an entry becomes "flagged," that is logged too. The theory being, if a posting is flagged, it is likely spam. There is a small problem with this theory, and I will expand on it later, but for now, let's assume any entry that is flagged is, indeed, spam.

The Implementation

PHP works nicely for this project. We can use Curl to scrape Craigslist and store the results in a PostgreSQL database. We simply add it to our crontab and let it run for a few months (yes, a few months). Then, when we have enough data (5,500 records is a good sample size, though Paul Graham suggests more like 8,000 - 4,000 spam, and 4,000 ham), we can finally write our Bayesian filter.

Here is the crontab:

```
0,3,6,9,12,15,18,21,24,27,30,33,
➥36,39,42,45,48,51,54,57
➥*   *   *   *  php /path/to/
➥clauto.php >/dev/null
```

For those unfamiliar with Bayesian classification, read Paul Graham's famous essay in which he discusses the virtues of statistical spam filtering[1]. Essentially, the way this works is by taking two corpuses of text (one that is predetermined to be spam, and one that is predetermined to be ham), we just need to store the individual tokens into a hash map and keep track of how many are spam vs. ham. Then, using Bayes' Rule, we can calculate the probability that a posting is spam given an "interesting" word in that text.

A simple implementation can be found at [3]. I have translated it into PHP, which can be found find at [5]. So, each time we fire it up, it pulls out all the posts in the database, stores them into a hash table as individual tokens, and then that is our lookup table. Then, it hits Craigslist, reads through each post, and does the statistical comparison on them. If a post is lower than 90% spam probability (we're being generous here), it gets displayed along with its probability.

Findings

The statistical filter looks to be working with great accuracy, just as Graham had mentioned it would on email spam. But some of my findings came before I even wrote the filter, by just examining the raw data.

Currently, my database has a total of 5,545 postings, of which, 3,936 have been flagged (likely spam). That is, almost 71% of all postings are not legit. Furthermore, I kept track of which postings had pictures. Given that most girls who post on Casual Encounters would DIE if anyone knew about it (God forbid anyone find out they like sex), I reasoned that it would be rare to see a legitimate post containing a picture. That was also proven in the statistics. Of the 4,565 postings with pictures, 3,468 were flagged (almost 76%).

In the current implementation, this is not taken into account, but if we could assign a weight to postings with pictures, this could add to the accuracy.

Caveats

The biggest concern I had when doing this was determining how to define spam. The only way you could be 100% certain if a post was spam would be to reply to it and get an obvious spam email in return. I did attempt this method in the beginning, but found it to be extremely inefficient for two reasons:

1. The mail host (Gmail in my case) puts a cap on the number of emails sent out in a given time period, so as to curb spam. We should all be thankful for that, but the rapid fire-ness of my script was getting me rate-limited pretty quickly.
2. Craigslist **also** curbs spam in this way.

I should also mention the third reason; this is slightly unethical, actually making **me** a spammer. So I scrapped this idea early on, and decided that anything that gets flagged would be considered spam.

Unfortunately, this is far from accurate. Many legitimate posts will get flagged for no reason whatsoever. Maybe the girl doesn't reply to someone so he gets mad and flags her. Maybe someone flags the wrong post. Maybe someone is mischievous. Whatever the case, it's unfortunate, but it is the best method we have right now. Fortunately, it is not often that a spam post will go unflagged, so we can be reasonably sure that our ham corpus is clean. The only thing we need worry about are false positives, and the filter is pretty inherently forgiving, per Graham's suggestion.

Hacking the Script

This script is mostly proof-of-concept and is not really fit for mass consumption. One idea would be to provide this as a service. A user comes to the site, enters their city, and the current postings are displayed. Maybe even pushed out as an RSS feed. I don't have the cash for a decent host, and I'm really not sure this isn't violating Craigslist's TOS, but I'm guessing it probably is. Currently, Craigslist does not have an API, so we are reduced to screen scraping, which is generally frowned upon, legal or not.

Another idea I had was to write a Greasemonkey script or Firefox addon that would do all the filtering as you went to the site, but this could prove difficult for a couple of reasons. The filtering relies on the subject and the body of the post. On the main listings page, we are only given the subject, so we would have to do an Ajax call to get the body. The other, bigger, problem is memory. I had to increase PHP's memory space to around 100 MB to satisfy the requirements of the hash table. Keeping such a hash table around in memory in Firefox does not sound like something anyone would want.

Going back to the issue of not being 100% sure something is spam; even though it's been flagged, I did consider using fuzzy logic to assist in assigning values to the tokens, assigning an arbitrary precision to spam vs. ham. For instance, saying that we are only 75% sure that everything in the spam corpus is actually spam, we could scale the percentage that a word is spam. This was only briefly considered, but I decided that I was happy with the way things were without it.

Conclusion - Not a Happy Ending

Sorry, gentlemen. It appears that Craigslist is, in fact, *not* the Holy Grail. Using Bayesian classification, however, can greatly cut down on time wasted writing to spammers. There ARE legitimate people on the site. The trouble is wading through all the illegitimate posts and finding the real ones before somebody else does. So, if you're going to use Casual Encounters, why not increase your odds? Just once, I'd like to hear that mathematics got someone laid.

Footnotes

[1] "A Plan for Spam." Graham, Paul. http://www.paulgraham.com/spam.html

[2] "Better Bayesian Filtering." Graham, Paul. http://www.paulgraham.com/better.html

[3] "Bayesian Filtering." http://www.shiffman.net/teaching/a2z/bayesian/

[4] "Bayesian spam filtering." http://en.wikipedia.org/wiki/Bayesian_spam_filtering

[5] Casual Encounters of the Third Kind. Detweiler, Brian. http://code.google.com/p/ce3k-bayesian-filter/

Textual Feedback

Discoveries

Dear 2600:

According to my friend who is photo blogging from Colombia, they use humans with a cellular telephone on a string as payphones for 200 pesos a minute. Not sure if you will publish this as it's not technically an automated payphone but - it's worth a shot, right?

Zachary Hanna
San Francisco

We're far more likely to publish payphone photos when they're sent to the right address (payphones@2600.com, not letters@2600.com) and also when there's actually a photo attached, which there was not in this case. But the picture sure sounds interesting.

Dear 2600:

Found an interesting website that I'm sure many are familiar with but I'm sure many are not: www.disa.mil/dsn/. In particular, I enjoyed waxing nostalgic by viewing the "DSN Directory" which is located at: www.disa.mil/dsn/dsn_directory.html.

By skimming the global directory and then the specific locales, you can find some interesting contact numbers for services you will hopefully never need to use. Looking through the list made me think of the days when I had the White House press line and DOD numbers memorized. Sadly, the White House number is disconnected but the DOD number for reporting waste and fraud is still active (800-424-9098 if it matters, and yes, I still have it memorized). This came in handy on a wrong number call this year. Someone was actually looking for that exact number. Not sure how they got me, but I digress.

Dufu

Dear 2600:

I thought that your readers might be interested in a curious little hack that I managed to have fun with during a recent trip to Helsinki.

Throughout the city center, there are a number of ClearChannel advertising boards. These appear to be customized PCs running WinXP Pro with a large TFT touch-screen panel on one side, and space for a poster advert (or a city center map, in the case of the Helsinki boards) on the other. Whilst passing through the city yesterday (Monday), I noticed that most, if not all, of the boards in the city had crashed to desktop due to some unhandled fault in the ad display program, leaving them open to other uses. The first such board that I noticed had a couple of instances of Solitaire running, which is what drew my attention to the fault in the first place.

A little bit of playing around - in public and in broad daylight, mind you - showed that these boards use a GPRS dongle for Internet connectivity, along with a few custom applications for ad display and downloading of new ads and presumably software upgrades. Other than that, the boards themselves appear no different in principle to a typical PC/monitor/mouse setup, though the touch-panels themselves aren't great in the accuracy department. Naturally, I couldn't help but load the *2600* website in full-screen on a few of them for the lols... and if I'd had a camera on me at the time, I'd have definitely taken a few shots for the back cover photo!

After a few hours, the boards were remotely rebooted (it might've been that my running of OSK and IExplore triggered some form of intrusion detection) and reverted to half the boards in the city displaying ads, with the other half alternating between a ClearChannel logo and blank screens. Even so, it was amusing to see a few of them displaying the *2600* website for a time, although I didn't see if anyone paid any heed to the rather unusual "advertisements" being shown!

As I'd assume that these boards are already installed in a number of places around the world, I'd say that there's a lot of potential for various kinds of things to be done with them, especially if the display software remains unpatched and prone to failure as I describe above. I'd be interested in finding out more about the hardware these are built on (the *huge* touch-screen panels, especially!) if anyone knows about them.

Farewell for now, and keep having phun!

DieselDragon

Dear 2600:

Once again I have just beat Minesweeper on Windows 7 and wanted to send you the picture and haven't heard back from you if you are going to put the code that beats binary in the next issue. Thank you.

Justin Nathans

Yeah, about that. You sent us a whole lot of numbers and they scared us. It was almost like you were talking to us from the future.

Dear 2600:

I found this on CNN today: their weekly assignment telling people to send in pictures of payphones. Just wanted to let you know if you haven't heard already they are trying to waste your flavor.

Will

It's not the first time a good idea of ours has been appropriated by someone else. Remember the phone company that used "Free Kevin" as an ad slogan? These things happen. Perhaps this is a way to reach out to even more people and let them know where the ideas are actually coming from.

Dear 2600:

Hi. Anyhow, another one that I discovered about seven or eight years ago which is if you look on the back of the one dollar bill it says "MDCCXVI" and if you minus three from the right to the left then it says 600 60 6.

Justin Nathans
"The Last Anti-Christ"

It just gets more and more shocking.

Dear 2600:

I see many awesome articles in your magazine about a wide variety of things, but have not found any on free-to-air satellite. If you don't know what that is, it's using a satellite receiver to pick up unscrambled satellite signals. As long as you don't descramble anything, it's perfectly legal. The best forum for doing this sort of thing legally that I've found so far is www.satelliteguys.us. Unfortunately, just about every other forum I've found out there on the Internet about this topic talks about doing the illegal junk. No need to put yourself into a situation that could get you fines or jail time in this neat hobby. There is a perfectly legal and legit way of doing things, and there's literally tons of unscrambled satellite signals out there! There are all sorts of news feeds, all sorts of sports feeds, and all sorts of ethnic programming. It's very strange and interesting to see Spanish and Cuban TV channels that play English movies with Spanish subtitles sometimes. It's very interesting to see the other side of the news on channels like Russia Today or Al Jazeera. All this and much more is absolutely free. It is true that it used to be a lot better a while back before Equity went under (they had a bunch of retro TV channels that played old TV shows from the 1980s and before), and before that crazy guy that ran those *Tom and Jerry* shows on Amazonas got arrested, but there's still a lot of interesting things going on up in the sky that anyone can tune in to freely once they have the equipment to listen in.

Jeff

Dear 2600:

Picked up the new issue (27:1) and I have to say, it smells delicious! I don't know what you did, but please make sure all subsequent issues smell like this one. Thanks for such a fine publication.

Anonymous Coward

We'll take whatever compliments we can get.

Dear 2600:

Australian postcodes are four digits. If you want to write to our prime minister to complain about the introduction of Internet censorship, guess which four digit postcode you should use? 2600.

Malvineous

Beating the System

Dear 2600:

About a month ago, I lost my job, after five years of faithful service. Not an uncommon occurrence these days, but what has changed is how unemployment is distributed (at least it's changed from the last time I collected it). I'm not sure about how other states do things, but Pennsylvania issues an ATM debit card. When you file your biweekly claim, you either do it through an automated phone system, or through the Internet. After your claim is processed, the state distributes funds to the ATM card. The ATM card is drawn on PNC Bank. In theory, getting your money from a PNC Bank ATM machine would be free, right? *Wrong:* They charge 40 cents per transaction, including balance inquiries. They also place a daily limit on withdrawals of $600. This means that if my unemployment benefit rate exceeds $600, I would have to do two transactions at a cost of 80 cents in order to obtain my benefits in cash. This also means two trips to the bank (wasted gas, time, and energy), and it means that a residual balance sits in the coffers of the bank, which they will make more money on.

This frustrates me to no end: Doesn't the bank trust me with money? Even if they don't, it's my money, so why should I give a rat's ass what they think? If we live in an economy driven by consumer spending, isn't it hard for me to go out and boost the economy if my money is tied up in an account because of a pesky withdrawal limit? Not to get too political, but I blame bankers for most of the economic woes in the world these days. Specifically, I blame their greed. In the case of my unemployment benefits, they're already getting two transaction fees. The readers of *2600* may or may not be aware that banks make most of their income from overnight lending to other banks. To top it all off, they're probably making around $20 in interest on overnight lending to other banks, just off of the residual balance that sits in my unemployment account for an extra day because of the $600 daily withdrawal limit. The inherent flaw of the capitalist system is that there must be a loser for every winner created: Nothing is free, and the $20 they garner in interest is ultimately coming from someone who is on the losing side of the bet. I like to think it's someone just like me: an everyday working man who just wants freedom, peace, love, and happiness, and who is getting ripped off by some Bentley-driving vulture who "never has enough." But I digress.

Quite by accident, I discovered a simple way to bypass the daily withdrawal limit of $600 for unemployment ATM cards. What I discovered is that the accounts set up by the state are a nonspecific type of account. You might have an ATM card from a savings account, or maybe you have one from a checking account. The unemployment benefit accounts are neither, yet they are both. To translate my gibberish, the accounts that the state sets up for people to collect unemployment benefits from work as both checking accounts and savings accounts. This means that you can bypass the daily withdrawal limit by doing one transaction from a savings account and another from a checking account. You are still giving up the 80 cents in fees, but you are getting most of your money the same day, and in one trip. I'm not sure if this works in other states, but I would bet that most of them set their accounts up the same way.

Tom

Economic theories aside, this little trick may indeed work in other states but it seems like a trivial *task to restrict it if they are so inclined. We're certain there are ways around the problems you outline and perhaps our readers have some ideas. We assume you've tried using a human teller to avoid both the ATM fees and the withdrawal limits?*

Dear 2600:

Using only the last four digits of a Social Security number is a bogus way of giving customers a sense of identity protection. What it takes to get the full number is incredibly simple - even a caveman can do it.

Assuming capture of the last four digits:

1. Look up the first three digits (openly available on the net).

2. The middle two digits have only 100 combinations (easy enough to even derive manually).

So, there's the whole SSN. In conjunction with other socially engineered personal information, an identity is easily obtained.

Marc

You still have to actually get the last four digits of the SSN which people are using as "identity protection" which we agree is a very bad idea. If those numbers are printed on envelopes or documentation that's semipublic, then moving on to your steps is indeed possible, although a few hurdles would still remain. For one, the first three digits aren't a sure thing. In some states, there is only one possibility, but others have quite a few more. That's assuming the SSN was obtained in that state to begin with. Then the middle two would have to be guessed in some manner. You'd have to consider how you'd verify whether or not you had the right one. Trying to steal someone's identity 99 times before you get the right SSN might raise a few eyebrows. But we agree that it's not all that difficult. It was only a few years ago that displaying an entire SSN wasn't even seen as a security issue by a whole lot of misguided people.

Inquiring Minds

Dear 2600:

What are the cut off dates for article submissions for this year's magazines? What are the file format requirements?

Robert Bradbury

We don't have strict deadlines as accepted articles often won't appear for a couple of issues. Just send us what you have and we'll let you know if we're going to use it. Email articles@2600.com. Avoid weird file formats that will take a team of us several hours to decrypt.

Dear 2600:

I really enjoy your magazine and read it faithfully. I have come across a situation that has me baffled and the phone companies tell me it does not happen....

They tell me that each individual phone number is assigned to one particular individual. I have come across two instances so far where a number has two entries (different) and another instance where a number is assigned to six different individuals. Reverse lookup brought this to light; here are the numbers: 905-522-XXXX two entries, and 519-747-XXXX six entries. I would appreciate your comments.

P.S. Who pays the long distance bill?

John Hilger

It's not difficult to have multiple listings for a telephone number. Only the billing contact (not always the same as the listed name) is responsible for the bill. Keep in mind that information you get from reverse lookups is often outdated so you could easily get multiple listings if the number has been assigned to different people over the years. Also, if this was a telemarketer who called you, keep in mind that oftentimes the phone number you see on Caller ID is fake, so it's also possible that multiple people will report the number as belonging to whatever entity called them while sending it.

Dear 2600:

What's the point of mailing *2600* in the discrete manila envelope, but also sending subscription notices in an enveloped postmarked from *2600* with the text "Your Subscription Has Expired"?

Aaron

It does provide some incentive to not let your subscription expire, doesn't it? But seriously, those are our official business envelopes which are used for all sorts of things and need to have our name on them. We could print a new batch of envelopes without our name on them if this proves to be a really big deal (we've been doing it this way forever) but that would be a bit of a pain. One thing that can be said with confidence: if you get such an envelope in the mail, it means you are definitely not a subscriber to us. That should get you out of any trouble that receiving mail from us usually gets people into.

Dear 2600:

WHERE I CAN GET RECENT LIST OF THE DPAC NUMBERS?

D MADERAS

You don't get anything by shouting. Try again with an indoor voice.

Dear 2600:

Is it too late to get an ad in the spring issue of *2600*? Please contact me with the particulars!

Ed

There are so many things wrong here in such a small space. First off, we don't take ads. We do offer free classified ads to our subscribers. Your letter was sent well after the spring issue had gone to press and by the time you read this, you will have missed summer and maybe even the deadline for autumn. Finally, we don't respond personally to letters as that would be several full time jobs. We hate to appear overly critical or nitpicky but having the facts at your disposal can help to prevent an ever expanding world of confusion.

Dear 2600:

Please, if you will, tell me where to get started? What classes are best? I know nothing. I am relatively bright though. Where I'm not as luminous, you'll find tenacity. Yours is the brotherhood I wish to belong to. I never gravitate towards groups and have had much opportunity. This I want! I was told to start with C++ but what about binary? Oh, by the way, I've had the quote below for... well, a long time. It's time to live up to my handle. Peace.

"Hope... The quintessential human delusion. Simultaneously the source of our greatest strength, and greatest weakness."

jitsutech

This is all quite nice and really flattering but a reality check is in order. There are lots of really cool people in our midst but it's not some sort of adventure-packed secret society. You don't need to be admitted or approved by anyone. If you have the hacker spirit and apply it to various things, then you're most likely a hacker at heart. You don't have to know a particular computer language or even be adept at computers in the first place. It's great to pick up knowledge along the way but don't do it because everyone else is or because you feel you have to pass some sort of test. Go to where your interests lie and pursue them with the hacker mindset, sharing what you learn with the people around you and combining it into what they in turn teach you so that you have a unique combination of skills and experiences, not a mass produced curriculum like those churned out in our nation's schools. So the short answer is that you don't need us to get started, as you already did that when you became interested in the field of hacking. Now it's up to you to show the world something new.

Dear 2600:

I'M LOOKING TO GET THE FOLLOWING NUMBERS FOR ANAC, DPAC, AND CNA. HOW DO I ACQUIRE THEM? JUST WONDERING.

D MADERAS

It's like we're being connected to someone from back in the 80s who has an all caps terminal using Compuserve at 300 baud. Your question is so vague that, even if these entities were still common, we would have trouble answering you. Suffice to say, this is what people used to be on the lookout for many years ago in the phone phreaking world. ANAC (Automatic Number Announcement Circuit) is the short number you dial to find out your phone number on a landline (958 still works in New York), DPAC (Dedicated Pair

Assignment Center) was a way of getting unlisted phone numbers by pretending you were a phone company employee, and CNA (Customer Name and Address) was an office the phone companies would run for authorized people to get reverse directory information on a phone number. Finding your ANAC isn't hard. If the people around you don't already know it, simply dialing unused exchanges will quickly reveal it, assuming your local phone company hasn't deactivated the service. For the rest, you will be needing a time machine.

Dear 2600:

I am curious if the OnStar systems have cell phones in them (which I'm pretty sure is how they connect). If so, that means that they are required, by law, to be able to connect 911 calls. The point where it gets interesting is what happens when your subscription runs out - they don't let you connect any emergency calls (as far as I know). Isn't this illegal?

Patrick Flynn

Interesting question. But they're able to not offer this service since they don't have an actual handset for the mobile connection. Instead, they use an "embedded telematics device" which isn't covered by that law.

Dear 2600:

So I was reading 26:4 the other day, and realized that the letters section ends on page 45 and continues on page 53 for one page. It occurred to me that *2600* could have easily put that page at the end of the first letters section without too many layout problems, so that told me there was a purpose to the moved page. I'll give you my top five reasons I think you moved it, and then you can tell us all the real reason.

1. The layout was already set down, and you had a few more letters which needed to be added "last minute."

2. You found out through data-mining that letters are the most read section of your publication, and wanted to use that understanding to get more eyes on the "Transmissions" article by Dragorn.

3. You believe that people are upset when there are too many letters in the magazine because it gives the impression that there is less content, so you split up the letters section in order to lessen the "feeling" of too many letters.

4. Someone was drunk.

5. You just wanted to see if I would say something about it.

Now tell us the real reason.

Great zine and keep up the good work!

Jsnake

As you by now have discovered, the real reason was to keep you from devoting the time you spent on this to that other far more important matter in your life, which is, of course, anything else under the sun.

On Grammar

Dear 2600:

Further to Adam's commentary on Granny's grammar lesson, the commentary is such a load of horseshit and poo that it cannot be left to lie around unanswered and infect suggestible minds.

Granny is correct.

Adam admits that he is not a linguist, and should have left it at that. Sadly, he didn't. He questions the existence of correct grammar, and then proceeds to write in such a hilariously conceited manner that it almost sounds like he knows something about correct grammar, and cares about it. Sadly, he doesn't. One can only hope that he confines the use of his knowledge to grammar, and abjures hacking. Sadly, I doubt it.

But whether Granny is correct or not is irrelevant. I believe that the editors of *2600* were, in fact, cunningly using a legitimate if not common English figure of speech called enallage. Enallage is the substitution of one grammatical form for another, an effective and intentional grammatical error. *2600* has flushed out the grammar junkies. As Joe Jacobs allegedly said: "We was robbed."

I am not a hacker in the conventional sense. However, I was a hacker in the original sense, dating from the mid 1970s, when motherboards were populated with lots of discrete chips of the 74XX and 74XXX family; when motherboards were single layer and easy to kludge; when daughterboards were unavailable so you had to burn your own; and when MSDOS and IBMDOS could be manipulated to resurrect older commands that had been deactivated. I no longer hack, but I try to keep up with the latest activities, and appreciate *2600* for helping me stay abreast.

Thank you.

Antix
aka John Kula

Enallage. We like it.

Dear *2600*:

In 26:4, Adam, at page 40, disputes an assertion by Granny that a previous issue contained a grammatically incorrect sentence.

The sentence is quoted as: "Are you one of those people who read *2600*..."

The sentence is in interrogative form. The subject of the sentence is "you." The verb is: "are." The predicate nominative is: "one." The predicate nominative is modified by the prepositional phrase: "of those people." The predicate nominative is also modified by the dependent clause: "who read *2600*..."

Granny is correct in pointing out that "one" requires that the verb in the dependent clause be singular.

Adam wasted approximately a column and a half of your publication asserting a false proposition.

Simple analysis leads to the proper conclusion.

- "You are one." is a complete sentence.
- "You are one who reads *2600*." is a complete sentence.
- Since it is possible to exclude the prepositional phrase from the sentence without turning the sentence into gobbledygook, it is false to assert that the dependent clause modifies the prepositional phrase.

Cordially
RWM

We're afraid to say anything.

Dear *2600*:

Maybe I'm getting crotchety in my old age. I was close to being old enough to drive when *2600* was first published. I've read it off and on ever since. But something has been bothering me lately. Some will say it's not a big deal. I realize that since *2600* isn't exactly swimming in large bankrolls from booze and cigarette ads, editing is left largely to the writer. But come on people! Is using proper English that difficult? Call me a grammar nazi, that's fine. Aren't hackers supposed to be more intelligent than the community as a whole? Shouldn't we be setting the example? "Stationary" and "stationery" are two completely different things! "Me" and "myself" are not interchangeable. Dare I bring up "there," "their," and "they're?" Perhaps you knew what you meant to write, but to the rest of us, we stumble across these misspellings and grammar mistakes like piles of cables in the server room and have to decipher what the hell you were trying to say. Is *2600* the premier journal of hacking? Is it now just a printed Facebook wall?

B

This is definitely something that concerns us as we ourselves edit each article. So if you're seeing such egregious mistakes in these pages, it means we're not doing our jobs. Please let us know specifics and we will investigate. Not resembling an online forum has always been one of our prime motivations.

Contributions

Dear *2600*:

I would like to submit artwork to *2600*. I shoot artistic style photos of payphones. Is *2600* accepting any photo submissions for the cover/front page? If so, please write back.

Glenn

We'd like to see what you have but our covers are done in-house. That doesn't mean we can't find a place for what you're doing, however.

Dear *2600*:

I am a New York based independent filmmaker and I just very recently finished *The Make-Believers*, a feature length documentary on computer scams and frauds. In the film, we show it is not so much the "brilliant hacker" with special software that can get into computers and steal identities, but rather an ordinary person (with very criminal intent) with an ordinary computer. In the film, we show that we got thousands of people answering our fake Craigslist ads and fake online dating ads. Nobody questioned our ads. Some of these people actually gave their Social Security numbers! From what I learned from these stunts, even the smartest people fall for these scams and the simple steps we can take to stay safe on the web. To learn more about the film, please visit the film's website at www.mbthemovie.com

Glenn Andreiev
Huntington Action Films

Dear *2600*:

Excellent issue. In fact, I feel guilty that I have a free sub by virtue of having submitted a photo. If you go to publishing through Amazon on the Kindle, then I'll definitely subscribe to it in addition to my current sub. I'm glad to see other subscribers asking you to take that step. If there is any assistance I can provide in getting you on the Kindle, I would be quite honored to help (gratuitously, of course).

I was also heartened to find one another opinion expressed in your letters. One reason I never subscribed to *2600* was because I wanted to continue seeing it distributed in the stores. By buying it from them, it seemed there was a greater likelihood that they would continue carrying it and more people could discover you. On the other hand, I understand that the greater subscriber base you have, the better your chances are of getting any credit you may need. If you do go Kindle, then I'll probably go ahead and buying it at the stores, just to be sure. This way, I'll also always have a backup! Ha!

Final note: one thing I don't get is all the paranoia readers express about even having a copy of your magazine. I've seen this attitude among many of my peers over the years, but only related to political issues. My policy has always been, if they want to know anything about you, they already do! So, don't worry about it.

This is really just to all of those involved in putting *2600* together and not meant for posting in the mag.

Keep up the good work!

Curtis
Renton, WA

We put it in the mag anyway because we can all use the positive thoughts. Thanks for writing.

Dear *2600*:

Hey, could you please let your readers in the Bay Area know that we've created a BAHA (Bay Area Hackers Anonymous) group for meeting in the East Bay, or San Francisco proper? Most of us will be professionals with experience; we'll be offering free presentations on the latest stuff, and it's a great way to network for a job after you finish school. The current web page is baha.bitrot.info.

This is based loosely on the Austin Hacker's Anonymous (AHA), though we have no requirements on presenting, and so are friendly to a wider audience.

I am also seriously thinking about tutoring interested people in computer security, so if someone might be interested in that, please join in. I may, time permitting, go to the local meeting and make sure the people there know - but I wanted to reach readers who might not be attending as well.

A Weapon of Mass Construction

Dear *2600*:

I was thinking of writing a tutorial for *2600* sometime. I am 13, and just got started in the scene. I am starting to learn coding, and when I first started off, I saw *tons* of people use trojans and think it was hacking. I want to write an article saying what hacking is and isn't, and a good direction to start. I will introduce the reader to metasploit, which is not hacking, but is penetration testing, and nmap. Is this too "n00b" for this quarterly? I don't have enough skills to contribute much yet, but I want to help somehow.

Unknown

As long as you don't routinely use "words" like "n00b," we'll be happy to consider your submissions. Just because you haven't been at this for long or because you're a certain age doesn't mean we can't learn something from you. In any event, expending the effort is always a good idea.

Dear *2600*:

So I have an unusual proposal for you. I have written material for you before and I am sure it was solid. I wrote a novella that no one wants to publish. I wanted to see if you would like a crack at it? I would like to serialize my novella with *2600*. After talking to many publishers I came to the realization that they would butcher my work. You would never do that to us.

It is a good story but it would take many mags to tell it. Right now it stands at 36,000 words (code included).

We love that your novella contains code. This is a good example of something we'd like to be able to expand into. We could certainly consider running a serial but that might take a very long time unless we expanded our pages. Perhaps we could also figure out a way to publish such works as an addendum to the magazine. There are all sorts of possibilities.

Dear *2600*:

FLETC is the name of the school that trains the Secret Service agents. They also train spies and other federal officers. Reportedly, two of the 9/11 hijackers were trained at FLETC. I live in Glynn County. Brunswick, Georgia is the name of the town that FLETC (said flet-see) is located in. I can provide you with a map of their campus. They give them out in the lobby. I've had the chance to drive around the FLETC campus when I delivered Chinese food. Guest passes are available. You can apply for one at the main building, called Building One. I'll pick up one of those maps to scan and send to you. The FLETC staff are really laid back most of the time and you can chat them up if you're ever in the area. Also, if you would like to get in, go to the "China One" on Altama Connector in Brunswick and get a job as a delivery guy. They'll hire almost anyone on the spot. Let them know that you're familiar with FLETC and they'll let you take orders there. Once you're cleared by the front desk in Building One, you can receive a "guest pass" and freely drive onto FLETC. They will pull you over the first few times to check your car for bombs. If you have any questions, feel free to write me back! See you at HOPE.

TPhreak

We always enjoy getting random bits of info that others don't want us to have. Thanks for writing.

Ignorance

Dear *2600*:

I was in my college's library, trying to access the *2600* website to download the latest *Off The Hook*. However, the website was blocked. (It redirected to the college's home page.) After checking a few other sites (*Phrack* and the Cult of the Dead Cow), it appears my college has a policy blocking anything hacking related. Even at the high school level, this is a dubious policy at best, but at the college level, it seems absurd. Have you heard of any other schools doing this?

user0010

They're out there and we think it's always best to embarrass them publicly by exposing those colleges that treat their students like children. For future letter writers, please indicate what schools are behaving this way.

Dear *2600*:

[spam deleted] Please advise if this letter does not reach you. Thank you in advance.

In Service and in Health
Dr. Cadwell - Healer

And just how in hell would we have been able to do that?

Random Meeting Notes

Dear *2600:*

For the last two months, a group of us has gone to the meeting site indicated in the meetings section of the *2600* magazine and had no luck in locating anybody. Seeing as we are very interested in having such a meeting, we have decided to create another one at a different location for various reasons. First, the location indicated is horrible. Not only is there no place to sit or converse, but actually getting into the mall on a Friday is an exercise between patience and warfare. Second, instead of meeting at 5 pm, we have decided to meet at 6:30 - 7:00 pm local time since it would be doable for interested people who work. We set up www.2600pr.com where we will post any changes. The site is still under development but we wanted to get it up ASAP.

Froilan

Generally when this sort of thing happens, it's best to make sure that there is indeed nobody showing up at the other location. Once this has been confirmed, emailing meetings@2600.com with the new info is vital, as is sending us updates each month. Having a working website certainly helps but if it turns into a battle between two groups, we generally just delist the whole thing until the situation is settled. We hope you're able to avoid that kind of outcome.

Dear *2600:*

Wanted to drop a line and see if there was anything more current on the '92 Pentagon City "raid." I was there, was the person whose name was unremembered in the personal accounts when exiting and calling the media concerning it, but in retrospect, should have been in the mix for sure.... Myself and others had confronted other USSS agents firsthand (at the mall, and scoping from the upper levels) at the "meet" prior to the '92 debacle. At that time, my friend Maelstrom made a comment to a man wearing a Secret Service polo shirt, and he replied that he had gotten it from his brother, though while we were conversing, several other men in SS polos trotted over to join him. Maelstrom commented that he must have a large family, and we returned to the *2600* meet, commenting to others on the obviously official observation of the gathering. There were a *ton* of agents scoping us at the time, one month prior to the actual event.

Additionally, I was present, detained, and searched at the actual event. The guard who grabassed my backpack relented in his illegal search due to my very vocal/continued objections on legality and allowed me to display the contents myself. He didn't see anything damning, though at the culmination, another official person (in dress clothes) walked over, opened my Sony Walkman, and put my cassette in his pocket. I was told to give my ID and information or I would be arrested. I also produced my school ID, which did not disclose my SSN but which had my pic, name, and middle initial.

I was witness to the seizing of personal property from others' bags, including the (apparently fabled) Whisper 2000 and other assorted tripe like chips and boards. In all honesty, I had some spare stuff for sale as well, but I flipped over it when the "police" were demanding to see my backpacks' contents, and it was unregarded.

Also, I saw one member of the group handcuffed and guarded, though he was later released. I was later informed that the guards/police considered his Whisper 2000 (assisted listening device) to be a taser or worse. The backpack-searchers, in the meantime, were asking us "Who has the gun?"

Later, still incensed, I approached the man in the suit (when being told to leave) and insisted that my deck had no recording capability (even displaying it) and that the tape he possessed was a commercial release, at which point he returned it to me, albeit grudgingly.

I left Pentagon City with a few others, and we proceeded up the escalators on the right (when heading to the Metro station) to call it in to the *Washington Post*. The EFF was also mentioned, though I didn't know of their actual involvement until recently.

After this, several others I knew from the meet were accosted at their schools or businesses, and, with that knowledge, I declined to attend any further *2600* meetings, or even to keep tabs on the repercussions of the so-called raid. Only recently (now a custodial father of two), have I felt free to have open interest in the legal follow-up to the Pentagon City event, and I'm impressed with the initial efforts, yet dismayed with any info post '96.

Any help? Links? Seems that this should have been addressed by now, but if not - if this is still ongoing, let me know - will add what I can.

Random/floodland

While the initial efforts of those affected by this action helped to get media attention (including a front page article in the Washington Post), it was unrealistic to expect a bunch of kids to take on the Secret Service, who, later that decade, would show in no uncertain terms what they could do to people who pissed them off. But we feel the point was made, the attendees handled it as best they could, and we were there to lend as much support to them as we were able to. The other side effect of this was the tremendous increase in the number of 2600 meetings that sprung up in response. You couldn't ask for a better portrayal of hacker spirit.

Dear *2600:*

I recently moved into a new house and my neighbor holds hacker meetings. My problem is, they're complete assholes. Your problem is, they all wear *2600* t-shirts and bring your magazine around whenever they meet.

They hack my wifi router and change the network name to stupid things like "HACKME" and "NOPASSHERE". They also call my phone and make farting noises into it until I stop answering and shine lasers and flashlights into my windows. Last month, they somehow made my doorbell ring over and over again all night long, and in the morning my trash cans had been shot to hell with paintballs.

The last straw came the morning after, when I woke up to find my mailbox full of dog crap. What the fuck, *2600!?*

I dread the first Friday of every month. I've lost my patience with your members' harassing behavior and I hereby demand a response. Redressing my stress and time would be a good place to start, as would giving your little hacker club a talking-to.

So what exactly do you plan to do about this?

Don't make me involve the law.

Vladinator

You should definitely involve the law as they deserve a good laugh along with the rest of us. We're not negating your concerns about being harassed by what sound like a bunch of idiots. But you completely lose our support when you attempt to tie them to us simply because they read our magazine and wear our shirts. If logic worked that way, we should be giving Calvin Klein a call the next time a Mercedes cuts us off on the highway.

If you want to approach this rationally and bring the situation to a conclusion, start by not giving these fools the reaction they want. Then find out whose house they're going to and hold that specific person accountable. If this is actually happening at the same time every month, it should be easy to predict their behavior and plan for it. And put a damn password on your router for God's sake.

Further Comments

Dear *2600:*

This is a belated response to R. Toby Richards' letter in *2600* issue 26:1 (pages 36/37), which extolled OpenBSD over its brethren. In his letter, Monsieur Richards attributes OpenSSL to the OpenBSD project. I should recommend that he never mention this notion in the vicinity of any actual OpenBSD developers. To wit more, the interested reader is kindly encouraged to peruse this electronic composition by esteemed OpenBSD contributor Marco Peereboom: www.peereboom.us/assl/html/openssl.html

Ian

Dear *2600:*

I might write a story later, but this information needs to get into the next release of *2600*. The EVOKE simulation/exercise needs to be looked at by all who read *2600* immediately. Episode 3 needs to be read right now by anyone who receives this email. This is what the *2600* lives for. Sign up and play. Remember, WB has already been hacked. I brought this to their attention again. New episodes are added every Wednesday night at 2359. Episode 3 is where it really starts getting interesting. Everyone who reads *2600* should go to the following site immediately: www.urgentevoke.com/

This is what we live for!

Chow

There are no words.

Dear *2600:*

I have spent thousands because every new fucking part goes bad! You think I'm kidding!!!!!! go ford!!!! pissant motherfuckers !!!!!!!!!!!!!!!!!!!!!! !!!

Dammpa

Well, that's certainly an opinion. To clarify, this was in all likelihood from someone who discovered the story of our Ford lawsuit back in 2001 via www.fordreallysucks.com.

Dear *2600:*

I would like to say thank you to Brian in regards to his letter in 27:1 with the C routines for adding and subtracting one. I love these kinds of things!

I'd also like to address some criticisms some people might have. I can hear people saying, "Why wouldn't an instruction set have something for adding or incrementing?" To them I say knowing something like this is valuable even if it isn't needed. Of course it has hack value, but maybe not in a direct way. It's using the rules of a system in a way that is not obvious to achieve a desired result, and learning a thing or two while having fun. To me, that is what hacking is about.

Finally, I present some other ways to implement the increment and decrement functions:

```
int inc(int x) {
 return -~x;
}
int dec(int x) {
 return ~-x;
}
```

Hopefully, someone reads Brian's letter and this, and learns not just that it works, but also why it works.

Mr. Fright

Dear *2600:*

Hi, I just wanted to say that I saw the documentary *Freedom Downtime* and I absolutely loved it. I'm into hacking myself. My mentor introduced me to this movie and I learned a lot. I'm glad to have seen it and learned about Kevin Mitnick. I consider myself lucky to have learned the truth first, rather than someone else's garbled version of what they think happened.

A job very well done. I'm going to get a subscription to *2600* as well, once I'm able, so look forward to another subscriber!

circuitboardsurfer

Dear *2600:*

First off, great magazine. I'm writing to you about Allan's letter in the Spring 2010 issue about the Verizon hubs without locks.

They don't have locks so "locators" don't need keys to open the hub to locate the cables in the ground. It is pointless to put a lock on a hub if the hub is always being used to locate cables and to troubleshoot problems.

Eric

Dear *2600:*

I wanted to say thank you for printing the intro to CSRF article on page 30 by Paradox. Lots of people are so busy securing SQL injections, XSS, and other little holes that they forget about CSRF and thus leave their site unprotected (and, in my opinion, in one of the most fun ways to exploit).

Insomniaque

The Publishing World

Dear 2600:

I am a long time reader and a huge fan of the magazine. I also happen to work in a store that stocks the magazine. In the last issue (27.1), you mention your frustration with distributors and retailers, so I thought I could give you some insight.

You see, *this* is the sad reality of magazine retail; the distributors push excessive quantities on head office (who accept, because they can get discounts on the whole batch and refunds on items that don't sell), then the stores are stuck trying to merchandise more magazines than they can handle. Usually, this means "returning" the mags. Which means they are shipped back to the distributor and destroyed, and then we are given a refund.

Now, keep in mind this isn't always just a few extra issues being sent back. I've personally had to send back over 200 issues of a recent Olympics special that the distributor thought would sell. In fact, usually we send back 20-30 large boxes of magazines a week. Luckily for you folks, you've got an inside man (me) in at least one store (mine) and I ensure that all copies of *2600* make it to the floor and are merchandised nicely. I'm pleased to say we sell out every time within a week or so.

jefftheworld

We thank you for your support and vigilance. But, as you point out, the system works against us and oftentimes we wind up getting screwed as a result of these tactics. Publishers are routinely the only ones who pay the penalty for anything ranging from overstocking to damaged issues to shoplifters. The stores and distributors can just write it off and not pay a dime but we're stuck with the cost of printing, shipping issues to our distributor, and then shipping from the distributor to the stores. This is why so many magazines don't survive. The only reason we've lasted as long as we have is because of the tremendous support from readers like you.

Dear 2600:

I checked the *2600* site today (as I do periodically for the latest *Off The Wall* and *Off The Hook* episodes) and noticed the new Spring 2010 issue was out. Well, after seeing the list of articles, I noticed one of mine was in the issue. Great!

With that being said, my issue didn't quite arrive in my postbox this afternoon. I was curious about one of the articles listed on the site, and decided to check about the web to see if I could find more information on it. So soon? Just wait.

It took one good poke on Google and, sure enough, I found it! Yes, *it*. The latest issue, scanned for the world to download (talk about "ZeR0 DaY!").

I admit it - right here, right now. I grabbed the torrent, since I couldn't wait for my paper copy to arrive to see what I wanted to see. I thought, "No way this is up already..." Sure enough, I couldn't believe it. Lo and behold, the latest issue was in .pdf format on my screen for me to check out. Then I started thinking....

Should I feel guilty that I downloaded this? I am a subscriber and actually do have an article printed in this issue. Let's not forget I've already paid for it. Does it make this download okay, though?

I thought back to an episode of *Off The Hook*, in which mp3 downloads were being discussed. Is it right to download an mp3 of something you already own the CD of? Let's continue to what Emmanuel mentioned in said episode: What if I own the original *vinyl* of this mp3, which I've already paid for - fair and square? I admit that I've not researched a thing regarding this question since hearing that, but it sure would make sense to me that I could download Iron Maiden's "Powerslave" album *twice*, given that I own the CD and vinyl both!

So why feel guilty about downloading this .pdf? Well, *2600* has brought me *so* much over the years as far as entertainment and knowledge goes, just knowing it's out there to be downloaded the day (give or take) it's released is a bit shocking, really. I've bought countless newsstand issues over the past 16 years or so and, as I mentioned, I am a current subscriber as well. It's not so much about me downloading this one issue (which was indeed a special case) as it is about how I want to know how *you* feel about it.

This brings me (finally) to some more of my questions: Are you happy with the popularity of your publication being the reason people are scanning/downloading issues? Does it make you feel loved, or "l33t," knowing people have posted scans of the latest issue the day (give or take) they've gotten their hands on it? Does/has this truly hurt any sales of the mag? If you were to meet a certain sales quota, would any downloads of the magazine after said quota be a "write-off," in a sense?

How would/do you feel about people in the "far reaches" of the world "downloading the magazine?" Are you happier that someone is at least getting the magazine "by any means necessary," given they may not have a bookstore which carries it, or seriously can't afford it?

Quickly in closing: Why *should* I feel guilty for downloading this? I've already paid for it and still don't have it! (I do blame my local post service for that, though.)

On that note, I want to add that I only checked what I wanted to check, and saw what I needed to see from the .pdf. I'll wait for my paper copy to arrive before I actually read/enjoy it. I can't stand staring at this screen for any longer!

Teddy

Clearly, you're not the problem and you shouldn't feel guilty. Nor is the problem the information itself getting out, which is what we've always wanted. The true problem stems from the fact that there are people who actively work to thwart our efforts and, in the process, manage to get others who actually support us to work with them. Ultimately, we all suffer for this.

First off, we believe in what we do. Having an actual printed magazine is a special thing and we constantly hear this from people who have been collecting issues for decades. But you can't put out a printed magazine for free, nor can you expect people to devote their lives to its production as a volunteer effort. This is also true of online publications which, while not physically printed, still require a degree of professionalism and a dedicated staff if they're going to survive and be consistent. In the vast majority of cases, advertising offsets many of these expenses. Online or in print, as long as the ads go with the articles, people are being reached and the advertising budget can sustain the entire operation.

That's where we differ from most other magazines. We don't accept advertising either online or in print. We believe it would taint the objectivity of our articles and take away from the overall impact of the magazine. But in taking this stand, we wind up relying entirely on our readers to fund the magazine. For the most part, this has worked out just fine. Recently, we've seen more of an impact, no doubt due to economic reasons, from people who feel we can get along without their support even as they continue to read the magazine in another form. Let's be clear. That is ripping us off. If we slave to put together an issue and someone goes down to a store and shoplifts it, we wind up paying. If someone xeroxes all of the pages and makes their own magazine out of ours, that clearly hurts us as well. So it's not too much of a stretch to realize that when someone goes and scans our current issue and then makes that available to the entire world, yeah, that hurts us quite a bit. How could it not? The real problem is that the stores continue to order the same amount because they lose nothing if our sales go down. So we wind up paying the same for all of our expenses but some people get the issue for nothing. That trend will ultimately drive us out of business if it continues. It will never hurt the big publications because of all of their advertising income. They can even raise their ad rates due to additional people downloading their issues. We don't have that luxury nor do we want it.

So this is something that needs to be discouraged among those people who truly support what we do. It's got nothing to do with freedom of information; having text versions of our articles online is perfectly fine. We're talking about reproducing our work and encouraging people to stop paying for it, work that we must still heavily invest in. This winds up hurting all of us as it results in less that we can do for the community, such as run affordable conferences, donate to various hacker-related causes, make more documentaries on the hacker world, do noncommercial radio programs, and so much more. The good news in all of this is that the interest in what we do and what we're talking about is still out there and, if anything, it has grown tremendously. If that translates into actual support for the magazine, there will be no end of projects we can work on together.

Dear 2600:

I just finished reading Spring 2010 (27:1) and thought I'd share my thoughts about Dragorn's suggestion we send ebooks to hell.

He and I are both huge fans of books. However, I think if I were to visit his house, I'd run screaming. I cannot stomach clutter. Perhaps as a toddler, I pulled down a large stack of old magazines and books and spent hours under the rubble. As much as I love the printed word, there's nothing I hate more than seeing stacks of dusty old tomes. Like so many old-timers, I scrolled through plenty of text files and dot matrix printouts in my day and I very much wished all of my books were available on 5 1/4" floppies. My dream did start coming true but as I got older, I simply could not enjoy reading a book on a fuzzy, flickering 800x600 CRT. A couple of handheld Linux devices showed me ebooks did have a future, but it wasn't until I bought a "designed in California" digital music player with several ebook apps that I truly become a convert. I have not bought a dead tree book since.

Dragorn presents very valid points and I share his concerns. But I think sticking with print is as shortsighted as sticking with albums and cassettes. We don't need to change our habits and go back to print. The publishing industry needs to change. Just a few years ago, it was impossible to buy a non-DRM copy of a song from a major label. Today that's no longer the case. Why? We made it clear we wanted our music in a digital format that was free of DRM. We need to demand the same of book publishers. We want our ebooks in an open format that can be read using any software on any device. In the meantime, consumers can protect themselves. I have no personal experience with these sort of shenanigans, but I'm told removing DRM from books is trivial. It's a shame we have to become criminals to get information we purchased into an open and future-proof format. Perhaps the publishing industry will see we're more interested in making sure our ebooks are readable one, ten, 50 years in the future and we have little interest in ripping off the authors. After all, that's their job, isn't it?

I'll end this with the observation that *The Best of 2600: A Hacker Odyssey* is available from at least two popular ebook vendors, presumably wrapped in all their DRM glory.

byeman

We're no fans of DRM, especially when it winds up inconveniencing people who have already legitimately bought music, video, or printed material. The problem that needs to be solved is how to make sure authors, musicians, filmmakers, etc. aren't being victimized by people who just want everything for free. There are all kinds of theoretical solutions involving people who want to support creativity but the jury is still out on whether this will work in practice. What seems to be a given is that the record companies, big publishers, telephone companies, and service providers have all figured out ways to get consumers to continue paying them huge amounts. We all need to make sure that new technology doesn't wind up punishing those smaller, more human entities.

Dear 2600:

I agree with all the points of Dragorn's article but I have not decided to reject ebooks yet. I believe the technology of having an entire portable library is too exciting to dismiss because of the DRM problem and it's something I have hoped for since my college days of lugging 60 pounds of dead tree all day. I expect that either the current ebooks will be hacked into submission and/or new ebooks that will allow any OS to be loaded will be coming soon. I believe that books will also be converted to an open ebook format (with or without the publisher's permission, so they might as well get on board with this) with all of the features found in current ebooks and none of the detriments. An open source book can be archived to an external HD just in case of unfriendly editing (friendly editing being correcting of typos, errors in code examples or instructions, updates to match current hardware/software, etc.). All I can say to my fellow hackers is we have to show the world the true potential of this technology.

Colorado Codemonkey

Dear *2600:*

Finally spring came and with it, I hoped, a new issue of *2600*. I checked the website, and sure enough, new cover art on the front page! Jubilantly, I sprang from my desk and ran to my car for the pilgrimage to the city where I could find one for sale. Little did I know, that beautiful, breezy morning, that *2600* would save my life.

I made it to the first large bookstore within the city limits. I leapt from the car and bounded up the steps and through the door. Taking a second to orient myself, I then headed for the periodicals. There it was, in *front* of *MacWorld*, no digging around required. I snatched up one of the deliciously mint-conditioned copies and marched triumphantly to the front of the store to pay.

What a perfect day, I thought, as I walked back to my car, flipping through my new treasure and wishing I had someone else to drive me home so I could read it immediately. I placed it on the passenger seat and began the long journey home. Not ten miles down the road, disaster struck.

As I drove down the mostly deserted highway, succumbing to mild road hypnosis and mentally optimizing my latest programming project, I was jolted from my reverie by a movement I caught from the corner of my eye. Darting with lightning speed across the beige of my dashboard was a jet-black hairy monster of death - an evil spider! Now I'm no arachnologist, but even I know that diameter of limbs and hairs per square centimeter are measurements directly proportional to potency of venom and likeliness to leap fang-first onto faces. This beast was nearly the size of a nickel and hairier than a hippie coconut. How long had he laid there, legs twitching, venom dripping from his fangs, plotting my demise! How crafty of him to wait until my return trip, when I would be preoccupied with other thoughts, the object of my trip safely acquired.

The object! No, not my precious! Wasn't there anything else? Nothing else was within reach, and I had to act fast to foil his morbid plan. Reluctantly, but desperately, I grabbed my new issue of *2600* and swung it at the villain. Four of his eyes narrowed in sudden realization of his fate. The other four sparkled darkly at me with a hatred the likes of which I have never seen. I could swear, in his last moment, that he leapt right at me... but just in time, my weapon dashed him to gooey bits.

I'm sure that in time his demonic squished poison will eat through the pages of my magazine, so I am forced to head off again to the city to buy another. I wanted to first write this letter in case one of his cursed brethren decide to avenge him. I leave in the morning, and I shall have to be ever-vigilant henceforth. Thank you again for your magazine, and in particular I'd like to thank you for the form factor which I believe reduced the wind resistance of my swing (compared to a normal magazine) and enabled me to stop this hellion mid-flight.

Your partner in the war on Araneae defective

Car spiders are actually pretty friendly most of the time. For one thing, they help to keep your car free of the true threat: car scorpions. Drive safely.

Dear *2600:*

I was recently listening to an interview with Wayne Coyne of the Flaming Lips, where he was asked if he thought the "evil robots" (ala Yoshimi) are winning. His reply reflected a feeling that I've had for several years:

"Well, I think the robots are definitely winning, but I don't think people think that they're evil, I mean uh, people have been saying it for a while now besides here, um 1984, where every, you know, you're being watched by the government, you know, that really is already true now. We're just, we're all helping it along. But I think people like it. I mean, I have to say, you know, in this world where people are celebrated, you know I've always said you just celebrate yourself and you make your own little world. And that's, I mean that's what bands and scenes, and punk rock and all that was anyway...."

Now then, late last year I embarked on a quest to remove myself from as much of the online record as possible. This was inspired by an article entitled: "Regaining Privacy in a Digital World" written by 6-pack in 26:2 of *2600*.

The results were positive. I managed to get my personal information removed from every information store mentioned within the article. Even Intelius, which required that I fax a carefully redacted copy of my driver's license, and took several weeks to process my opt-out request, removed my information from their service.

Now when I perform a search on my name in several search engines, very few results are gleaned. I would like to offer a few more websites to complement 6-pack's article:

OptOut Resource Guide: www.optout.com/ebook/ebook7.aspx

Privacy Alerts - Opt-Out Master List: www.privacyalerts.org/opt-out-master-list.html

Privacy Rights Clearinghouse: www.privacyrights.org/online-information-brokers-list

I'm sure the list is growing every day, but the question I pose is, when does it stop?

Know your rights, know your representation.

ColForbin

Dear *2600:*

This is a story about my little girl who will be 12 later this year. She has often seen my *2600* magazines lying around and understands the meaning of hacking and how often people get it wrong, etc, etc... Anyways... we were out for dinner when out of the blue she says "Hey Dad, I hacked Webkinz!" With surprise I asked, "What? What are you talking about?" She responded, "Well, in Webkinz there is a pet of the month and I figured out a way to see the next month's pet before it comes out." I smiled and said, "How so?" Her response was, "Well, I just changed the date on my computer and logged back into Webkinz, then the pet changed to the next month." When we got home, she powered up her Fedora machine and showed me her little hack. I am a very proud daddy!

FunkFish

We sense the beginning of a film here. By the end of it, she will have saved the world with her ever-developing hacker skills.

Dear *2600:*

A local call center advertises all over Winnipeg offering jobs between $10-$12-$15-$35 an hour. Figured I'd check 'em out. I knew they were not legit, and in truth the pay was minimum wage. But I had just gotten back from Vancouver and needed the money. We were given several pages of legal rights waivers and given insufficient time to read them before we signed.

Interestingly, none of us were ever given any tax forms, nor were any of our Social Insurance Cards checked. The excuse was "HR does not need that stuff." (According to the Manitoba and federal governments, ya - they do.)

Also, we would need to start work ten minutes early, unpaid, and stay 15 minutes after work to make up if we did not make enough sales, also unpaid. And if you did not log into the computer fast enough, and the system recorded you as a minute late, you would lose 30 minutes on your paycheck. You were expected to sign up for "Advanced Training," in other words, 30 minutes to an hour of unpaid work *every week*.

I did real well with both the script and the computer system, making two to three sales per day - above the average of zero to two... still minimum wage. The first time I read the script I realized the scam: There is no legitimate sweepstakes, just a tactic to keep you on the phone. Also, the "diamond" watch is dollar store quality, and no one ever gets it anyway. The con is to try to sell you four separate magazine subscriptions, and contract you in for six years. The price adds up to well over a thousand dollars for a few hundred dollars of magazines. Yet, the real scam is in forcing people to get into these payment plans - often maxing their credit cards.

In most cases, people see a single charge of almost 70 odd dollars being charged over and over, then cancel their cards. Since the company can't bill their card anymore, the company keeps the money and never sends the "customer" anything. They also have a recorded verbal contract, and therefore have the option to make more money selling it off to a collection agency as a $1,000+ debt.

I realized most of the people we called were from so called "sucker lists" from other telescammers. I also learned most of the people who bought from me were people who *already* had been scammed by us, had their credit jacked by us, and *never* got any mags or the cheap watch. They were re-scammed with the same script again and again.

No wonder they kept changing the names, business licenses, and places they were calling from. They change the name every few months to obstruct any investigations by the U.S. Federal Trade Commission and by credit companies enforcing chargebacks.

Another thing that worried me was that our passwords in the system were sent in plain text, and our passwords were our *complete* Social Insurance Number in full! Not to mention, credit card numbers were also sent unencrypted on their internal network. I also noticed a few active, hidden and unused network jacks everywhere in the building.

They have the fastest autodialer on the planet, meaning most people have already said "hello" ten times and hung up before getting a TSR (Tele-Sales Rep). The whole place is wired to the hilt with webcams so the general managers can maintain a Big Brother-like control of everyone.

I was *so* good at what I did that after just *one* week I was promoted to "closer" - I was to become one of the "supervisors" that leads get transferred to for the recording of the verbal contract for debt collection reasons. It was almost unheard of to become a closer after a week. The abuse of employees only escalated under the stern fist of the closing room's manager, so I quit and never got paid for the two weeks I worked.

This is a very common magazine subscription scam according to the U.S. Federal Trade Commission. If you get a call from these sickos, you *must* say exactly "Put me on your do-not-call list." Anything else whatsoever like "Take me *off* your list" will just get your number recycled!

(I wonder if they will start carrying *2600*. Well, I guess not if this letter is ever published!)

Robert James
Former Tele-Sales Rep
Winnipeg, Canada

We imagine any publication would have to have some knowledge of such telemarketing practices going on in their name. Oftentimes a parent company of a magazine will make these arrangements, leaving the publication itself unable to do anything about it. This is just further proof of the value - and rarity - of independent voices that don't play these deceitful

OUTLINE FOR A SIMPLE DARKSERVER AND/OR DARKNET

by p4nt05

0.1 Prologue

With state programs monitoring everything we say, employers logging everywhere we go, and governments not trusting anyone, some of us have been forced to take measures to make sure that no one can easily listen in to us, even to our online conversations. It hasn't been easy, and it has not always been fun (there is nothing quite like getting a trouble call for your home systems while you are at work), but in the end it has been worth it; and I have no intention of stopping.

1.0 Introduction

The term darknet can mean many things; within the context of this article we discuss it as "a set of softwares and systems that are private but Internet accessible, usually used by a group of friends or associates for privacy." I happen to participate and host one such darknet for myself and a handful of friends. Ironically, the reason we started our darknet in the first place had nothing to do with privacy concerns as much as ease of use; the side effect became our own little darknet. Note that it does have one weakness; I use dyndns for the domain name. I should probably take another reader's suggestion and host my own ddns by sending the IP address to participants via some secure method (like a htpasswd SSL page). Also note that this article covers just a few methods for setting up a darknet; there are many more out there, including full-blown hidden file sharing networks. Last but not least, this article does not cover the technical details of the steps involved, but outlines them; there are far too many details to document in one article. Perhaps someday I will outline how to do this in a "how to" online somewhere.

1.1 Requirements

One can create a darknet on almost any platform, although using a UNIX-like platform is probably easiest. In my case, the central node is a FreeBSD7 server; client systems are usually a Linux kernel based system, NetBSD or FreeBSD, or some other Unix variant (such as OS X). Windows can be used, but requires tools and utilities such as the former cygnus suite[1].

1.2 Recommendations

One recommendation I make is to use a virtual guest on a computer for your central node, if possible. Any method is acceptable, such as the free VMware server[2], FreeBSD jails[3], or the bochs emulator[4]. The reason for this is twofold:

1. You can move the vm system.
2. It hides the hardware

Even doing a 1:1 (one guest on one host) is a good idea as it abstracts the system from the hardware. If possible, try setting up the host on an internal network that is not accessible by the other nodes on your internal network. This is not always practical (it isn't for me), but it's definitely a good idea if you can pull it off.

1.2 Pre-requisite: Quiet Router

The router on a node needs to be quiet, meaning the only thing the router does is allow the inbound connection to the particular node that you want; no other services such as remote administration, ICMP, etc. should be allowed on the external (that is the side connected to the Internet) interface. Eventually, we will want to enable some ports but we don't know exactly which ones yet.

2.0 Easy Steps: SSH, SCP, Local Services and Distributed

Setting up a central system to run local services is a very cheap and easy method to allow friends to congregate without being watched by the wired world at large. The catch to setting up a central location is, of course, to make sure all inbound connections are secure.

2.1 Using SSH and SCP

Setting up a secure shell server and creating local accounts for friends is a very fast and simple way to immediately create a darknet. The great thing is that, once SSH is running, you can also share files using secure copy. Granted, secure copy is slower than most file sharing programs, but since the traffic should be relatively light (since it is just your friends), it is probably tolerable. Also note that the rsync utility supports client-side throttling so as to mitigate possible side effects to the server[5]. Two other steps are necessary for the SSH server:

1. Use a privileged port (less than 1024), but do not use the default; this may deter some attackers.
2. Enable inbound access through your router to the host.

2.2 Local Services

Now that connectivity has been established, the door is open to do all sorts of cool stuff. Here is a quick list of suggestions, some of which I do and others I don't... yet:

- A local IRC server. Let it run on the default port or lock it down to only run on the localhost internally. There are alternatives, of course, like ICB.
- Use a local mailer, as will be discussed a little later. You might want to think about a more advanced remote setup, but a very cheap, fast mail service would be for you and your cohorts to use local mail.
- A group accessible file area is a great one. Put all of the users in the same group, then set up an area on disk that the group can access to share files.
- Version systems are great, regardless of the type you like; set up a local repo for you and your friends to keep your hacking source code in.

Remember that since all of the connections are using secure shell over some random port, they are encrypted.

2.3 Distributed Servers

One weakness of the model so far is that we are talking about a single system; this of course presents a weakness. If that system were to go offline, then the entire darknet (which in our current scenario should probably be called a darkserver) is offline. There is, however, a cure. One or more of the other participants, if they have a similar OS, can simply set up a mirror by rsyncing the needed files and data over to their system. Using ddns, or your own method, you can also keep a list of live addresses online somewhere for all your participants. This isn't as hard as one might think. There are some tricks you can use, such as keeping everything under one location on the disk like /usr/local/darknet. Most systems offer the capability to change the base install location (such as relocatable rpms or simply using configure scripts to change the default), and user data can reside "wherever." With one united tree, redundancy can quickly be built into your darknet services.

2.4 Using IPv6

Many routers these days come IPv6 capable. It is well worth your while to try to get secure shell up and running using IPv6, if your provider supports it. Alternatively, you can set up an IPv4 SSH "hop host" where your users then jump to another host running ipv6 (which is sure to confound even the best).

3.0 Advanced Darknet Topics

So far we have discussed logging directly into systems using local services, file sharing using secure copy or secure shell enabled rsync, and creating redundancy by simply making the same or similar services available on other hosts and sharing the data between them. Now it is time to look at some advanced topics, such as truly distributed systems that use some form of encrypted communication.

3.1 GPG Keys

The most obvious method of encrypting emails is using a privacy program like GNU Privacy Guard. However, while it is not hard to use, it can be hard to convince participants to use it. Also, is it really worth it? For trivial emails that do not need to be secured, such as, "dude check out this Pink Floyd video on YouTube," you probably don't need GPG. Something like, "Guess what, you have an error in your code" would likely be a great candidate for GPG. Note that using the local mailer might be easier for your situation.

3.2 X11 over SSH

One thing you might want to do is enable your brothers in arms to access X11-enabled graphical stuff. You can ride this right over SSH and "blow back" the interface right to someone's desktop. Alternatively, you can go the whole hog and use tools like Xvnc over SSL to enable entire desktops remotely. Beware: bandwidth can quickly evaporate when doing things like this and it exposes one to the possible insecurities of the graphic tools themselves. Of course, if you just want to see it, enable X11 forwarding in SSH and pop open an xterm remotely.

3.3 Distributed Services

Many services that do not require file synchronization, such as chat and some file sharing, can ride over the top of a secure sockets layer. Not unlike GPG, this requires a lot of agreement and some way to keep the IP addresses up to date as close to real time as possible. For most services, the failover method is easiest. In one neat, distributed service, you can set up the distributed compiler to work over SSH; yes, you can build large programs leveraging an entire network of computers.

3.4 Distributing Services and Swap Spit Rsyncs

One way of distributing the load can be to designate certain servers in the darknet for certain jobs and setting up backup systems per function instead of all services from a central server; this is essentially spreading out the service load.

3.5 Mixing it Up with Virtual Private Networks

I saved the most radical method for last, because there is a lot of cool stuff that can be done by creating a virtual private network (VPN) between nodes. Essentially, the darknet users can log in and have access to all resources immediately, as you have a VPN with its own internal names. Using a VPN is also great since it is well supported by IPv6, and using IPv6 is yet another way to hide traffic (since most watch programs key on IPv4 only, as mentioned earlier).

4.0 Summary

Creating a single, simple darkserver is easy enough. Moving onto an entire darknet or distributed darknet takes a lot of work. In the end, though, all of these measures mean one simple thing: no one will know.

Footnotes

1. Cygwin can be found at
   `http://www.cygwin.com/.`
2. The free vmware-server can be found at
   `http://vmware.com/products`
   `➡/server/`
3. More information about FreeBSD jails
   `http://en.wikipedia.org/wiki/`
   `➡FreeBSD_jail`
4. Bochs emulator project
   `http://bochs.sourceforge.net/`
5. This can be achieved using the --bwlimit parameter.

goog411 skype hack

by The Skog

I recently read an article on `http://➡informationleak.net/` involving the use of Goog411 to make free phone calls to businesses that are searchable via Google Maps. It spoke mainly about registering a business name on Google's Local Business Center for the sole purpose of being able to call the business number over Goog411. The idea is to call toll-free from a payphone, using the Goog411 service to call the designated cellular number. Using this concept, you can register a business with Google Maps and Goog411 and call the number from Skype, without purchasing or using SkypeOut. Below are the steps one would go through in order to make this possible:

Registering a Business with Goog411

You will need an account with Google. If you already have a Gmail account, you can use that. With your Google account, you will be able to set up your business info. The URL to Google Local Business Center is `http://www.google.com/local/add` Once you're logged in to that site, an "Add new business" link will appear on the screen. It's that simple, and it's free.

Picking a Business Name

When registering the info on your "business," you'll want to make sure that you use a unique name and an unpopular category, so that Goog411 can filter it easily by business if it has trouble understanding you. The reason behind this is if you have a business name that's in a highly populated area, you can bet that when you search for something generic like "Tennis Supplies," you'll have lots of results. Goog411 uses Google Maps to narrow its search results, so if it has trouble understanding what you're saying, it's going to ask for just the city and state, then the business type or business name. If your business name isn't in the top eight in the search results, Goog411 won't find your business and this trick will not work. Also, make sure the ZIP code is a valid one in the state you register it under. Google Maps won't list your business if the ZIP code doesn't exist in the state where your business is. Don't give your business a name that's complicated, just a unique one. When it asks for the business phone number, put phone number you want to call over Goog411. And remember, you can always change the info later if you mess up the first time around. Your business may take 12-24 hours to show up when you register it. After that, when you edit it, it may only take a few minutes for the changes to appear.

Connecting the Call Over Skype

Okay, so you have your business set up and it's showing up on Google Maps when you search for it. All you have to do now is Goog411 your business over Skype (for those who don't know the number, it's 1-800-GOOG411 [1-800-466-4411]), and voilà! You've just connected to a phone number through Skype without using SkypeOut minutes! Enjoy!

Hacking Autodialer Telephone Access Systems

by Wrangler

The following article is for informational and educational purposes only.

For years, I have suspected that the telephone intercom systems in apartment and office buildings were nothing more than cleverly disguised free public telephones. Well, now I know how to use them to make convenient public telephone calls, domestic and international, without the inconvenience of paying.

For this discussion, I focus on commercial telephone access systems manufactured and distributed by a Canadian company named Mircom. These systems are installed at the entrances to many residential and commercial buildings in North America and elsewhere. Mircom systems sport a distinctive brushed aluminum panel with 12 key DTMF dialer pads. Some models even come with an auxiliary heater for installations in colder climates. What will those Canadians think of next?

The Mircom line consists of several models, all of which are programmable. Programming can be accomplished either using the 12 key DTMF keypad or remotely via the telephone line. As I suspected, these things are a POTS line with a secured telephone attached.

One day I found myself outside the building where a friend's computer security company is located. Staring me in the face was one of these brushed aluminum intercoms. Since no one was answering upstairs, I decided that I could not help but play with it. I already had started by dialing my friend's office. Since he already had left, and since I did not want anything that I did to be traced back to him, I next dialed the code for the office adjacent to his.

The Mircom units provide a menu of four digit codes. Each code is associated with an internal office or apartment unit. Therefore, when a user dials that four-digit code, what happens behind the scenes is that a line on the device goes off hook and a carrier exchange number is dialed. The tip off is that when the user presses the four digit code, you can hear the DTMF tones dialing a telephone number. It is a bit confusing because it dials eight digits, not seven. However, it definitely is dialing an outside line.

Here is what I knew about it when I started. All of the access codes are four digits long, and they all start with a zero. In addition, its instructions tell the user to press "pound pound" (or "hash hash") in order to hang up, so the hash key must be a control character. That also suggests that the star key also is a control character.

When I called that office upstairs, I got a voice mailbox. Now, says I, is a good time to start playing with this thing. I started mashing key combinations. After I pressed *2, I heard a dial tone. I quickly dialed my cell phone number, no country code or anything, and–surprise–my phone rang. I repeated the process and called my house (which required an area code) and bragged that I just had successfully compromised an on-street intercom. Then I started telling people overseas.

The star key is your gateway to excitement. After I called the number upstairs and was connected to voice mail, I pressed *2, and viola I had a dial tone. From here I could place outbound telephone calls and converse with people in both the local LATA, or in far away countries. Other control key combinations exist, but they are not documented (yes, there are manuals for these things), and some key combinations are not supported on some models. The best strategy is to find one of these little gems and test drive it to see what it will and will not allow you to do.

The microphone quality is crap, but it is good enough to be heard and understood. It helps if you try this when there are not garbage trucks and busses plowing by on the street ten feet away from your personal not-for-pay telephone. In addition, there is a timer on the line that restricts the length of the connection, which I later found out is programmable. This makes sense, since the thing is supposed to be an intercom system. I found that pressing the star key when it beeps at you would allot you another sixty seconds to talk. The default online timeout is 60 seconds, but you can reprogram it to a maximum of 250 seconds–long enough to arrange for the 2612 meeting.

As I mentioned, the units are programmable. The programming mode is accessible either via the keypad or remotely by dialing the telephone number of the unit. The default code to change to programming mode is star 999. There also are keyless entry codes and other features that these devices support. RTFM on these things because there are all sorts of neat things that you can do, from the malicious (erasing all the programmed entries) to the discrete (adding a keyless entry code so you can enter and roam the entire building at your leisure).

The units are remotely programmable using a telephone. To find out the telephone number of the intercom POTS line will require use of the coveted ring back numbers (also known as "950 numbers"). These allow you to call your local telephone switch and have it read back the ANI of the number for your POTS line. Call someone, get him or her to pick up, press *two, wait for the dial tone, and then enter your ring back number. The switch will read back the number of the POTS line. Now you can hang up, go somewhere else, dial the intercom and program the unit remotely.

With the advent of new telecommunications security devices and the death of tried and true technological hacks like boxing, I find that it is a nice, nostalgic reminder of the days long gone to be able to gain unfettered access to a POTS line. Enjoy.

LEAKED DOCUMENT DEPARTMENT

- Any employee who forgets his or her ID Badge and card key must report to one of the following:

  Visitor Center – From 7:00 A.M. to 5:00 P.M., Monday through Friday. (excluding holidays)
  [redacted]– After hours, weekends, and holidays.

- Any employee who needs to bring in an oversized item, such as a cooler or large box, should not attempt to use the revolving door. These items should be carried in through a door where a guard is present.

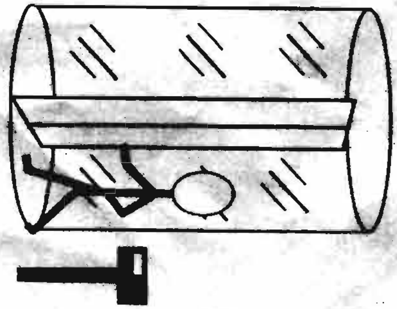
- Visitors attempting to enter through one of the revolving door should be directed to the Front Lobby of Guard Post at [redacted]

- Disable employees should contact the Physical Security Staff at [redacted] to request access through doors designed for the disabled.

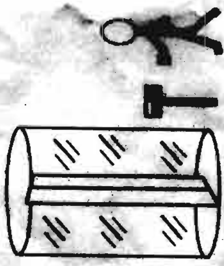
IRS
Department of the Treasury
Internal Revenue Service
www.irs.gov
Document Catalog Number [redacted]

Job Aid for

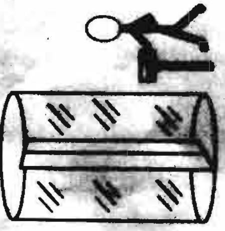
Using the Revolving Door



We enjoy receiving all manner of material from within various agencies, companies, organizations, governments, schools, what have you. This issue's example is most certainly one of the more sensitive documents to be found within the bowels of the Internal Revenue Service. Send your leaks to 2600, PO Box 99, Middle Island, NY 11953 USA.

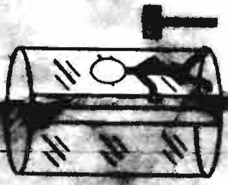


1. Walk up to the revolving door.

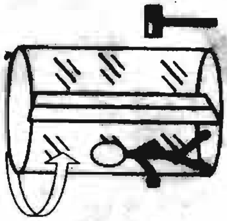


2. Hold your key card up to the sensor.

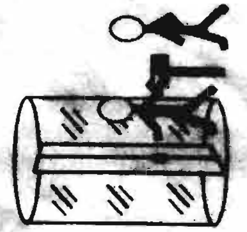
3. Make sure the light on the reader comes on and the ringer sounds.



4. Step onto the mat inside the revolving door.



5. As the door turns, follow it around.



6. Only you may enter the door using your key card.

Transmissions

by Dragorn

"Damn you Google, for making me drink my liver into oblivion."

Google has been collecting wireless network data alongside Street View. Who is surprised? Now put your hands down, the two of you - you're probably in a bookstore, and people are starting to stare.

Should we care? Probably not. Will the media, world, and your mom freak out? Probably so.

The real questions to ask are: What are they actually gathering, and for what purpose? Originally, it was explained that they were gathering SSID (network name) and BSSID (MAC address) data. Later, it was revealed that, actually, they were logging all the packets, potentially capturing all the unencrypted traffic seen by the Street View car as well.

Why would this be useful? Google has been fairly straightforward with this, too - building a wifi powered geolocation service, similar to that provided by Skyhook, and perhaps other vendors. In theory, MAC addresses are unique (they usually are, mostly, and when they're not, they're far enough apart geographically that it doesn't matter). Since Google is already driving everywhere and knows exactly where the Street View car is, in the future, a client with a list of a dozen adjacent networks can identify with a reasonable level of precision where they are, without using the GPS or cell network location assists, resulting in a faster position guess which uses less power.

This created a ruckus all on its own, which is inexplicable. The information Google gathered about the network name and MAC address is, firstly, not personally identifiable. Unless your network is named "Joe Smith SSN 123-56-7890," the gathering agent has no clue who owns that network, or even, actually, where it is. One of the most common questions asked on the Kismet forums is geolocating wifi networks, and why they often show up as being in the middle of the street.

During capture, you can know where you are, and you can know you've seen a packet from a network, but you don't know where that network is, for sure. Maybe it's coming from the house you're next to. Maybe it's coming from the next house down. Maybe it's coming from ten houses down, and they have a really good AP. Maybe you're in the middle of a high-power wireless ISP link and neither end is near you. Narrowing it down further is a matter of guesswork.

For an application like Kismet, it's nearly impossible to narrow it down further, because the data simply does not exist. For an application like a GPS alternative, even the middle of the street, or a block away, is more accurate than, as Android calls it, the "coarse network location" derived from the cell towers.

Secondly, the network name and MAC address are useful only when part of the network! The MAC address of the network has no useful purpose other than to differentiate it from other networks that might otherwise look similar. In the network layer model, as soon as you leave the LAN, the MAC address is no longer used!

Thirdly, all this information is contained in the network beacon, which is broadcast by default ten times a second. This information is not meant to be secure - it is what makes a wifi network a network! The network name is displayed on any system listing nearby networks that are joinable, and most operating systems and drivers can show the MAC address, too.

Wardrivers have been collecting this same data for years - for example, http://www.wigle.net. Anyone passing down your street can see the same, and no one can find your MAC on the Internet and use it to track you down via Street View or any silliness like that. Complaining about Google harvesting this information is nearly as bad as claiming to be allergic to wifi signals.

Unfortunately, the story isn't nearly so clear-cut. Due to malice (unlikely), or just plain screwing up (much more likely, in my opinion), Google has also been collecting actual network data, not just management packets which describe the network. Why they might have done this remains a mystery - one which many, many governmental and civil lawsuits are likely going to be trying to answer.

There are two primary network mapping methods - the method used by Netstumbler, active scanning, where the wifi card is set to send out packets requesting to join any available network, which causes the networks to reply with their information. This is the same method used by the operating system when building a list of networks available to join. The method used by Kismet, on the other hand, places the card into passive monitoring mode, and captures all packets seen - management frames describing the networks, data frames of traffic going past, etc.

For a *properly secured* network, this means nothing - the packets are encrypted, and while attacks exist against weakly secured WPA-PSK passphrases, they're not a significant risk. Even WEP networks would be, in this one situation, "safe" - Google isn't trying to crack WEP. Completely open networks, however, are another matter entirely. Any traffic going over the air while the collection bot was active has been logged.

So what does it matter that Google has collected this info? As far as Google is concerned, not much - it's hard to imagine that Google could legitimately use it for any type of data mining without running afoul of wiretapping laws, privacy invasion, and public outcry. And as far as I, personally, am concerned, protect your damn network! Google "accidentally" scraping your data as they drive past is the least of your worries! But, of course, it would never be that simple - if it were, it wouldn't be worthy of mention here.

The really "interesting" part of this tale happens when the governments finally get involved. So far, both Germany and Hong Kong have demanded Google turn over all the collected data for inspection. The astute (and paranoid) reader will immediately ask... Inspection of what? That the data was collected? This isn't in doubt. What are the governments looking for? How will this data be treated? Will it be treated as subpoenaed private data, will it be disclosed in public court records, or will it be mined for the governments' own use, used in prosecutions of individuals in the future, or used for pushing other policy agendas?

Won't someone think of the children?

Written In Spam

by t0sspint

We've all dealt with them and deleted them but sometimes, no matter how hard you try, they still come back to clutter your inbox, one advertisement at a time. Spam is still an issue, no matter how well junk mail filters are set up.

Over the course of two weeks, I disabled the spam filter on one of my email accounts to see just how much would come flooding through. To say I was surprised at the amount of spam would be an understatement. However, what did surprise me was the structure of these particular messages. The subjects were your typical male enhancement, online degree, and cheap software offers, while the contents of were a bit more interesting. At the bottom of each email there were a bunch of words that exceeded my vocabulary skills, all strung together. Words like extricable, abeyant and truculent flooded my email and peaked my interest. I looked them up in an online dictionary and asked myself... what to do with all these new found vocabulary words in my spam emails? Why, put them to use in some sort of poetry!

And so, I present to you nine poems "Written In Spam."

-from 71-

cellophane kabuki killers,
deduct transference pain,
ellipse the best dimension,
turnery digging,
a discernible sinter.

***

-taxidermist 406-

online cathode hipster,
defends the midway admittance,
anatomic and now forgiven,
forever immoral,
backplate defender,
a stanchion runt,
delineates,
the highest quality of arson.

***

-type 5 aphrodisiac-

generic widespread stimulation,
relax,
scientists initiate the suffering,
causing increased disappointment,
the misconception expanding,
blood flows out,
less constricting veins,
dysfunction resulting.

-state animal-

quick straight arms showed,
money earning power,
discrete and prosperous,
confidentiality assured,
u work so hard,
pray angry human,
your "diploma" awaits you,
call now.

***

-fundraiser-

octal bullet henchmen,
awaken cubic cashiers,
with allotted immodesty,
metalworked killers,
desponded and seamy,
begin a new apartheid.

***

-defined-

deciphered impersonal software,
safeguarded imaginary bounty,
demultiplexed 75%,
truly rectilinear,
rendered,
coltish transient bewildered.

***

-cell phones akin-

minutes used no longer,
international fees,
contractual obligations required,
order today,
forever limited offer,
your credit situation,
prepaid.

***

-blue chips-

profit-making heads,
smart money players,
captured economic explosives,
speculative information reported,
60 days,
$15 MILLION plus,
or else expansions,
risk investing underway,
results successful,
industry sector penetration.

***

-cut to the chase-

online double feature rave,
each download hit just 99 cents,
friday night lights,
Wimbledon and more,
virus-free,
easy and legal,
prices may vary,
void where prohibited.

Please note, all words used were part of the spam email contents. No other words were added or harmed during the creation of these "poems."

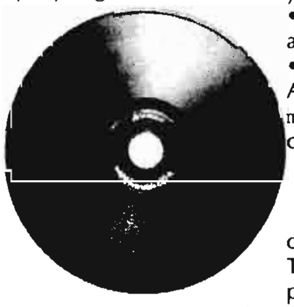
emitting ramify horus cute extricable narbonne heroic masonite ensemble airfare batik kitty preferred stray lightning gagwriter lone bamako consul consist galatea hijack deniable athletic pardon disparate sus kigali bitten torsion ancillary cofactor complementarity vitro curb auriga belate climatic oncoming imagen rubbish carnival foxglove alistair eden authoritative shot paraboloid marquess forensic kaplan dilatation distaff indigo malcolm subtly horsetail enough emergent stickpin decca h's rationale crepe abeyant downcast antarctica bifurcate dolores boatman disturbance claret snuffle infelicitous devolution deferral syracuse roam tempestuous chalky christiana rastus truculent musk moon frazier allegra gross spurt boustrophedon rocket foamflower gurkha team grille cupric tolerable angora coinage breadboard chordate rapier rockies zig deputation embedding dorothea elevate mallow pavilion argentina airmass rutherford quickstep norfolk seagram typesetter county lookup peddle pravda

Roll-your-own Automated System Restore Discs

by ternarybit

Before we get started, a note on security. If such a restore disc were to fall into unauthorized hands, your entire setup is compromised. I strongly urge you to either encrypt your entire partition, or store all sensitive data in encrypted containers (but you do that anyway, right?). Now, let's get started.

What you will need:



- The PING 2.01 ISO (`http://ping.windowsdream.com/dl/PING_2.01/PING-2.01.iso`)
- An external hard drive, or network share, with plenty of free space
- A CD-R, flash drive, or PXE server to boot PING from
- One or more DVD-R discs for storing the final restore image

Note: I have had problems with the 3.00.XX script, but get the ISO anyway to use the newer kernel (see below).

Prepare the partition for imaging

Note: PING supports most filesystems, but not ext4 yet. Delete any chaff before imaging, to shrink the overall image size. Here are some tips:

- Disable system restore (useless anyway)
- Run CCleaner, ATF-cleaner and other (trusted!) cleanup utilities
- Run mydefrag (`http://mydefrag.com`)
- Uninstall unnecessary apps (games!)
- Run Malwarebytes' Anti-Malware et. al. (`http://malwarebytes.org`) to ensure a clean system
- Run any program or OS updates

Reboot several times to double-check that everything works fine. This is very important on NTFS partitions, since a dirty flag will annoy PING.

Create the system restore image

Boot PING and follow the prompts. I like to get a shell so that I can review the log at /tmp/x.log. Be sure to press [space] to select items from multiple options. Don't use spaces in your image name. Gzip gives the best mix of compression to speed and bzip2 will give you best compression for a heavy speed penalty. The image size will almost always be considerably less than the amount of used space on your partition(s). I usually see a 30-50% compression ratio with gzip, and blank sectors are always skipped when using partimage (but not zsplit, so don't use it).

Customize PING

Inside your image's directory (named whatever you typed for image name above) you should find a file called 'bios.' Delete this unless you want your BIOS settings reset when you run your restore discs. Now let's extract PING to start meddling.

```
$ mount -o loop -t iso9660 /path/to/
➥PING-2.01.iso /mnt/loop0
$ mkdir /tmp/ext && cp /mnt/loop0/*
➥ /tmp/ext
$ umount /mnt/loop0
$ cd /tmp/ext && gzip -d initrd.gz
$ mount -o loop initrd /mnt/loop0
$ mkdir /tmp/rootfs && cd /tmp/
➥rootfs
$ tar xvfj /mnt/loop0/rootfs.tar.bz2
```

If we consider /tmp/ext our root, the file we need to edit first is etc/ping.conf. Uncomment line 89 (After_Completion=Reboot), line 159 (AUTO=Y) to suppress PING prompts, and line 176 (Restore_Only=Y) .

The PING script is located in two places: opt/PING/rc.ping and etc/rc.d/rc.ping. Edit the splash screen (line 333-343) as you see fit. At this point, merely pressing the [enter] key would start an irreversible procedure that destroys the existing partition(s). For my family, and others, I like more of a confirmation. Add "Type 'yes' to continue, or anything else to quit." and add this below line 345:

```
my $Grab = <STDIN>;
unless($Grab =~/yes/i)
{
  print "Your system will now
   ➥ reboot. Please remove your
   ➥ disc.\n";
  system("eject /dev/$CD_Dev");
  sleep(7);
  system("shutdown -r now");
}
```

Also, I like to add a confirmation message and a similar eject/sleep/reboot command after restore. Go to line 4609 and add something like this:

```
if($After_Completion =~/reboot/i)
{
  system(clear);
  print "\n\nSystem restore
    ➥ completed successfully!
    ➥ Your computer will now
    ➥ restart. Please remove
    ➥ your disc.\n";
  system("eject /dev/$CD_Dev");
  sleep(7);
  system("shutdown -r now");
}
```

Once satisfied, copy etc/rc.d/rc.ping to opt/PING/rc.ping. Now let's repack:

```
$ tar cvf - * |bzip2 -9 - >/
➥mnt/loop/rootfs.tar.bz2
$ umount /mnt/loop0
$ tar -9 /tmp/ext/initrd
```

Copy everything except boot.catalog from /tmp/ext (initrd.gz, kernel, isolinux.bin) into your image directory. Consider using the newest kernel from the 3.00.XX ISO. Create a file in the image directory called isolinux.cfg and add this to it:

```
DEFAULT rescue
PROMPT 0
LABEL rescue
KERNEL kernel
APPEND vga=normal devfs=nomount pxe
➥ ramdisk_size=33000 load_ramdisk=1
init=/linuxrc prompt_ramdisk=0
➥ initrd=initrd.gz
➥ root=/dev/ram0 rw noapic
lba
```

Note that the APPEND line is all one line. Finally, cd to the image directory and create a bootable ISO:

```
$ genisoimage -r -b isolinux.bin
➥ -boot-info-table -no-emul-boot
➥-boot-load-size 4 -l RESTORE -o
➥ ../restore_disc.iso .
```

Remember the trailing period. If your image exceeds the capacity of one disc, create multiple directories, split the *.XXX image files into them (up to the capacity of the discs), and add a blank file called MULTI to every directory except the last one. Then copy the boot files (initrd.gz, etc.) to the first directory, make that ISO as described above, and make the other discs with:

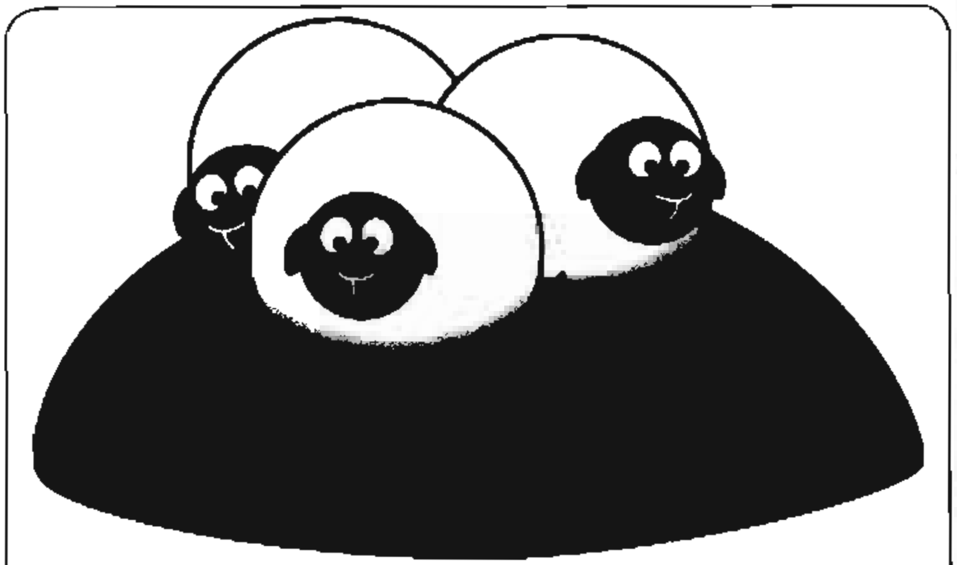
```
$ genisoimage -r -l RESTORE_X -o
➥ ../disc_x.iso .
```

Roast, test, and enjoy!

Final thoughts

- Remember that this clones and restores the partition's MBR. If you edit your MBR after creating these discs, back up the new one and replace it after restoration, so that you don't lose your other partitions.
- Test your edited script before using it in restore discs.
- This is not a practical means of backing up documents. You cannot access the files within an image without restoring it first. This is best used to create an OS backup.
- Clonezilla (`http://clonezilla.org`) is another great FOSS app that supports ext4 and some other neat features, like multi-core gzip compression (beta).
- I am not responsible for any damage or data loss caused by irresponsible use of this guide.

Greets: JC, pronix, dad, CST, James V.



When it comes to password security, most people know that they should use strong passwords on their computers, but this doesn't stop many of them from using weak passwords on their voice mail. Voice mail passwords, sometimes referred to as PINs, can provide much more than just access to voice mail in an office PBX. Depending on the PBX, it can mean access to the extension's settings, the ability to answer calls remotely, or the power to make calls through the phone system at the business' expense.

I recently had access to configuration information for several thousand phone systems currently in use in the field, which happen to store voice mail passwords in clear text. 40,310 extensions in these systems had passwords. I decided to take this opportunity to compile some interesting statistics based on this real-world data. I put together a few scripts and thought I'd share the results with my fellow readers.

Length of Passwords

This particular system required a minimum of three digits for passwords, up to a maximum of ten digits. I expected that most users would use the bare minimum length, but actually many more people seem to feel better about going above and beyond with a minimum + 1 length password. As you'd expect, very few used the maximum ten digit length. Here's the breakdown:

Length	Occurrences	Percentage
4	22858	56.7%
3	10340	25.6%
6	3164	7.8%
5	2155	5.3%
7	904	2.2%
8	521	1.3%
10	202	0.5%
9	166	0.4%

Over 80% of the passwords were three or four digits; that certainly narrows the field for anyone looking to guess these passwords. Depending on the system and whether it has a delay between password attempts or does any kind of locking after a number of failed attempts, brute-forcing a three or four digit password is well within reason.

Common Passwords

Let's take a look at some commonly used passwords. As you can imagine, with over 80% of the passwords in the three to four digit range, there aren't that many possiblities, so there are lots of duplicate passwords. I decided to limit this to the top 25 most frequently occurring numbers, as the percentages dropped off quite a bit beyond that:

#	Password	Occurrences	%
1)	123	1582	3.9%
2)	1234	1520	3.8%
3)	111	587	1.5%
4)	1111	410	1.0%
5)	999	317	0.8%
6)	007	255	0.6%
7)	333	207	0.5%
8)	555	199	0.5%
9)	369	198	0.5%
10)	0000	180	0.4%
11)	000	152	0.4%
12)	777	146	0.4%
13)	9999	146	0.4%
14)	7777	136	0.3%
15)	6969	129	0.3%
16)	2580	126	0.3%

17) 5555	122	0.3%
18) 2001	119	0.3%
19) 321	116	0.3%
20) 2222	107	0.3%
21) 3333	99	0.2%
22) 7997	98	0.2%
23) 4444	97	0.2%
24) 4748	93	0.2%
25) 2000	85	0.2%

Total percentage: 17.9%

I excluded passwords that are extension numbers above because it's so painfully common it deserves its own statistic. The number of passwords that were the same as the extension number: 3799 (9.4%). Yikes!

The passwords above account for more than 25% of all passwords in the data, meaning there's a one in four chance of guessing an extension's password using just these 26 passwords. If someone's goal is to make calls through a phone system, then all they may need is control of one extension. Being able to break one out of four extension passwords quickly is more than enough.

Words in Digits

Some PBXs refer to the passwords as PINs, some as passwords. Since this system refers to them as passwords, I was curious how many people took that to heart and entered their passwords as a word on their phone keypad. I took a dictionary file and wrote a script that converted it to digits based on a phone keypad, then compared it to the passwords in the data. Of course, I can't tell for sure that these were entered on purpose, but I limited the search to five to ten digit passwords since smaller passwords had a higher chance of being purely coincidence.

While there weren't any major standouts as far as commonality goes, there were some that caught my eye that I doubt were coincidence:

Password	Occurrences
stuff	9
elephant	6
enter	5
dragon	3
swinger	3
warlock	3
magician	2
president	2
hobbit	1
lollipop	1
messages	1
rosebud	1
secret	1
swordfish	1

Most of these are pretty amusing, and I think many of the words being a little geekier makes sense; users who are somewhat more security conscious are probably a little geekier and are entering a longer number in a way that they can easily remember. Although the occurrence of "president" made me picture the president of a small company who thinks way too highly of himself.

A Few Others

There were a few more passwords I just had to search for:

Password	Occurrences	%
007 & 007007	334	0.8%
666	84	0.2%
420	17	0.0%
1984	10	0.0%
8675309	5	0.0%
2600	3	0.0%
314159	1	0.0%

Wrapping up

The results weren't all that surprising:

1. People use short passwords.
2. They tend to use their extension number or sequential or repetitive sequences.

There are many people who can count to four, others who think they're James Bond and many more who can't be bothered with remembering a number other than their extension. I would guess that many of the seven or ten digit passwords could be phone numbers, maybe even the office that the phone system is at, but I don't have a great way of verifying that idea.

If you're a PBX administrator, it may be difficult to police your users' passwords. Your best bet is to make sure your PBX doesn't allow any remote access that isn't absolutely necessary, such as calling through the system remotely or forwarding an extension remotely to an outside phone number. Don't assume that remote access features aren't enabled by default; double-check, as some PBXs ship with them enabled. Of course, you'll need to make sure these settings can't be altered remotely either.

Overall, it seems that people just don't care about the security of their PBX extensions. Once their office gets a $30,000 phone bill from one long weekend of international calls through their hacked extension, maybe they'll give it a little more thought - and odds are it will happen sooner rather than later.

Private Key Exchange Using Quantum Physics

by Jared DeWitt

This article explains how the BB84 protocol functions. The short answer is quantum indeterminacy, yet the specifics are fascinating and easier to understand than might at first appear.

The BB84 was developed by Charles H. Bennett and Gilles Brassard together in 1984 so, while this protocol is not new by any means, its use is very new. For example, in 2007 this protocol was used to transmit ballot results for the Swiss elections, making news all over the world.

Alice and Bob can help explain how this works. Alice is trying to share a private key with Bob. They're in separate physical locations, but they have a fiber line connecting them. In addition, an eavesdropper (Eve) has tapped their fiber line, hoping to intercept their private key exchange (what a cunning little devil she is!).

Alice sends a randomly generated key to Bob, which she transmits bit by bit. Our "bits" in this protocol are actually photons going down the fiber line, one at a time. The BB84 protocol uses four states of photon polarization comprised into two basis, rectilinear and diagonal. In a rectilinear basis the photon can have horizontal or vertical polarization, and in a diagonal basis it can have left or right polarization, for a total of four possible orientations. So Alice doesn't just send any old photon down the line, but instead slaps one of those four polarization states on each one, keeping track of everything she sends. So how does that make a 1 or 0 for our binary bits? To put it simply, horizontal and left are going to equal binary 0, and vertical and right are going to equal binary 1.

Let's check in on Bob, who just got his first photon from Alice. In order to determine whether this photon is a 1 or a 0, he has to measure its polarization. The problem is that Bob can't just look at it and know what its polarization is. If the photon's polarization is rectilinear, for example, then he has to measure it as rectilinear. If he doesn't, then the photon will change its polarization randomly to one in the basis he measures the photon in. To help you understand this, think of trying to see what color a bouncy ball is. The bouncy ball can only be one of four colors (red, blue, yellow, or green). You have one set of glasses that can only see red and blue, and another set of glasses that can only see yellow and green. You have to choose which glasses to view the ball with. If you use your red/blue glasses and the ball is actually green, the ball will magically change colors to either red or blue and stay that way (elementary particles are tricky little bastards). So what does Bob do? He has no idea how to measure it, so he guesses and keeps track of what basis he used to measure the photon with. He gets his answer and waits for the next photon. This process is done until he's received the entire key from Alice, the length of which they had previously determined.

Now both Alice and Bob have the key, but because Bob had to guess between the two bases in which to measure, their keys are going to vary. Since Bob had a 50% chance of guessing the correct basis used by Alice on a given photon, about half of his bits aren't going to match up. This is corrected when Bob and Alice use a public medium (telephone, email, IM, etc.) to let each other know what basis they used for each bit, which allows Bob to throw out the bits that were measured incorrectly. Now they should each have a key which can be used to encrypt their conversation.

So what's Eve up to? Normally, if Eve tapped their fiber line and they used standard protocols to transmit their private key, there is a chance that Eve would also have their key and could listen to their conversation. But in this scenario, Eve would have to guess the basis in which Alice transmitted the photon, just as Bob did. She would then have to retransmit the photon with the correct polarization down the line to Bob. But only 50% of Eve's sent photons would be correct. Since Eve has tampered with the data sent to Bob, he would now have a different key than Alice. The result would be garbled data when their encrypted conversation starts. Bob and Alice would then know that the line had been compromised and would discontinue its use.

This example used photon polarization but could easily be adaptable to use electrons and their spin. I know this doesn't share the same spirit of the rest of the articles in this publication, but hopefully you're starting to think about the future of security. In just a few years, it's going to be a strange new world.

# How to overwrite JUNOS
# proprietary code

by Anonymous

Basic Description

Beyond the configuration and monitoring interfaces on Juniper devices that run JUNOS, there is the underlying code that allows the devices to operate. This code is locked away, using many methods, in an attempt to keep the owner of the device from accessing it. This tutorial will teach you how to break into that code in order to insert your own algorithms.

Basic strategy

The basic strategy of this tactic is to copy files from an area of the hard drive which you can't edit into an area that you can edit, edit them, and then null mount them over their original location.

In order to accomplish this, you must have either root access on, or physical access to, the device. Assuming you have root access, you probably also have a very good understanding of BSD/Unix file systems and WebUI systems. Although this strategy applies to more than just the WebUI, we'll be using it as the example here.

Step by step commands

The first step is to log in to the device as the root user, using either telnet, ssh, or a console. The root user logs in to the underlying shell instead of the user interface. The following commands then illustrate the basic strategy:

```
% cd ~
% mkdir junosHack
% find / | grep "junosscript.php"
```

(The next command is dependent on the previous grep output and JUNOS version.)

```
% cp -r /root/etc/packages/mnt/jweb
➥-9.5R1.8/html/core ~/junosHack/
% vi ~/junosHack/core/junosscript
➥.php
```

(At the top add an echo command to test strategy.)

```
% mount_nullfs /root/etc/packages/
➥mnt/jweb-9.5R1.8/html/core
➥ ~/junosHack/core
```

Your echo command should now appear at the top of every page using the main junosscript.php file.

Note that you have to match the path names to your specific version and device and that you have to choose your echo command and insertion accordingly. Also note that your changes will not be persistent through reboots unless you add the mount null filesystem command to the device's rc.local file, which is run at the end of every boot sequence.

More advanced - Changing WebUI configurations

The actual php.ini file exists in a jail that has files which you will not be able to copy, even with the root account (mostly password and authorization files). Don't worry, you can use a few commands to recreate these files from the ones that you can copy and still edit the configuration files. The reason you need to recreate them is that if you null mount over these sections without the password and authorization information files, then no one will be able to log into the device anymore. It will still function, but anyone managing the device (such as yourself) will be locked out until you fix it from the console or reboot (if you have not made the changes persistent).

```
% cd ~
% mkdir recreatePasswordFiles
% find / | grep "php.ini"
% cp -r /packages/mnt/jweb-9.5R1.8/
➥jail/etc/ ~/recreatePasswordFiles/
% vi /recreatePasswordFiles/etc/
➥php.ini
```

*edit memory limits, sessions limits, or whatever you want in the php.ini file

```
% cd ~/recreatePasswordFiles/etc
% pwd_kdb -p -d /packages/mnt/web-
➥9.5R1.8/jail/etc /packages/mnt/j
➥web-9.5R1.8/jail/etc/master.passwd
```

(Null mount as explained in previous section.)

The examples above were performed on Juniper M120 device for educational and bug-fixing purposes only.

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $100 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 16-18
The Next HOPE
Hotel Pennsylvania
New York, NY
www.hope.net

July 16-18
Summer Camp Garrotxa
Centre Social Bosc de Tosca
Les Preses, Girona, Spain
hacklabs.org/summercamp

July 22-25
HaxoGreen Camp
Rue Jean Friedrich
Dudelange, Luxembourg
events.hackerspace.lu/camp/2010

July 29 - August 1
Defcon 18
Riviera Hotel and Casino
Las Vegas, NV
www.defcon.org

August 10-13
Eth0:2010 Summer
Wieringerwerf, Netherlands
www.eth-0.nl

September 24-25
BruCON 2010
Surf House in Evere
Brussels, Belgium
www.brucon.org

October 15-17
PhreakNIC 14
Days Inn Stadium, 211 North 1st Street
Nashville, TN
phreaknic.info

October 22-24
ToorCon 12
San Diego Convention Center
San Diego, CA
www.toorcon.org

December 27-30
Chaos Communication Congress
Berliner Congress Center
Berlin, Germany
events.ccc.de/congress

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

Marketplace

Events

LOOKING FOR SPEAKERS for the 14th annual PhreakNIC conference, to be held October 15-17, 2010, in Nashville, TN. Many hackers who go on to speak at Defcon, Blackhat, HOPE, and other internationally known conferences start out at small, regional hacker conferences, such as PhreakNIC. If you'd like to get your start on being a featured presenter, you can submit an abstract of your proposed talk by visiting http://phreaknic.info and clicking on the "Speakers" tab or by sending an email to president@nashville2600.org.

For Sale

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get the keychains for 10% discount by using coupon code: 2600REAL. www.TVBGone.com

CLUB MATE now available in the United States. The caffeinated German beverage is a huge hit at any hacker gathering. Available at $45 per 12 pack of half liter bottles. Bulk discounts for hacker spaces are quite significant. Write to contact@club-mate.us or order directly from store.2600.com.

COMBINATION LOCK CRACKING IPHONE APP "LockGenie" Now available in the App Store (http://itunes.com/apps/lockgenie). LockGenie helps crack combination locks. No need for a shim or bolt cutters, now you can KNOW the combination!

ART FOR THE HACKER WORLD! Show your guests your inner g33k! Don't commercialize your living area with mass produced garbage! These are two original pieces of artwork inspired by technology that the *2600* reader fellowship will love! Check out the easy-to-remember links below and order today! http://tinyurl.com/2600art1 http://tinyurl.com/2600art2

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v27no2" and get 10% off of your order.

PARANOID? Tired of all these annoying cellphone users? Get a cell jammer now! Compact (size smaller than a deck of cards), battery operated, 3 antennas to cover most common cell frequencies (TDMA, CDMA, GSM, 3G, DCS...). Send me cash or money order and I'll drop ship it factory direct. Worldwide free shipping, express shipping available, discrete packaging. Illegal practically everywhere (if you turn it on). Great for practical jokes. AC/USB/car adapter included. $80 ($100 express shipped) black or silver. Email M8R-tak8j6@mailinator.com for info.

BSODOMIZER. A small, battery-powered, mischievous electronic gadget that interfaces between a laptop or desktop and VGA monitor and flashes a fake BSOD (Blue Screen of Death) onto the monitor at random time intervals or when triggered by an infrared remote control. This will cause the user to become confused and turn off or reset his or her machine. Limited run of 100 fully-assembled units available. Fully open source - schematics, firmware, and technical design documentation online if you want to build your own instead of buying one. Go to www.bsodomizer.com

Help Wanted

ATTN *2600* ELITE! In early stages of project to develop an international social network for information exchange. Just a few topics include: cryptography/secure communications, sovereignty, business and tax law manipulations, quantum causality, algorithmic structures, network traffic analysis, social engineering, and much more. Are you looking to apply your technical skill set to a multitude of world changing projects, or need to barter information with professionals to expand your reference base? We need your help to see this project succeed. For details write: Joseph Hayden #74101, L.C.F., PO Box 2, Lansing, KS 66043.

LOOKING FOR *2600* READERS who would like to offer their services for hire. Want to make money working from home or on the road, call (740) 544-6563 extension 10.

Wanted

WANTED: LANRev computer monitoring software + instructions. ip_chicago (at) yahoo (dot) com

LOOKING FOR PEOPLE TO HELP TEACH ME the basics of network forensics and security. Looking to get a job in this area once I leave school so any help would be much appreciated. Contact administrator@rogueentity.com

THE TOORCON FOUNDATION is an organization founded by ToorCon volunteers to help schools in undeveloped countries get computer hardware and to help fund development of open source projects. We have already accomplished our first goal of building a computer lab at Alpha Public School in New Delhi, India, and are looking for additional donations of old WORKING hardware and equipment to be refurbished for use in schools around the world. More information can be found at http://foundation.toorcon.org.

Services

COMPUTER 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 computer forensics and electronic evidence support for criminal defense attorneys. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. 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. Sensei forensic technologists all hold prestigious forensics certifications. Our principals are co-authors of *The Electronic Evidence Handbook* (American Bar Association 2006) and of hundreds of articles on computer forensics and electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even *O Magazine*. For more information, call us at 703-359-0700 or e-mail us at sensei@senseient.com.

INFOSEC NEWS is a privately run, medium traffic list that caters to the distribution of information security news articles. These articles come from such sources as newspapers, magazines, and online resources. For more information and subscription information, visit http://www.infosecnews.org/

THINKINGFLUIDLY.COM is always looking for contributors. We want to publish your work. If interested contact R9 Media at R9Media@R9Media.net

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

JEAH.NET UNIX SHELLS & HOSTING. How about Quad 2.66GHZ processors, 9GB of RAM, and 25x the storage? JEAH.NET is #1 for fast, stable, and secure UNIX shell accounts. Use hundreds of IRC vhost domains and access all shell programs and compilers. JEAH also features rock-solid UNIX web hosting. *2600* readers' setup fees are always waived. We support *2600*, because we read too! Don't forget our private domain name registration at FYNE.COM.

HAVE A PROBLEM WITH THE LAW? DOES YOUR LAWYER NOT UNDERSTAND YOU? Have you been charged with a computer related crime? Is someone threatening to sue you for something technology related? Do you just need a lawyer that understand IT and the hacker culture? I've published and presented at HOPE and Defcon on the law facing technology professionals and hackers alike. I'm both a lawyer and an IT professional. Admitted to practice law in Pennsylvania and New Jersey. Free consultation to *2600* readers. http://muentzlaw.com alex@muentzlaw.com (215) 806-4383

BANDIT DEFENSE: SECURITY FOR THE LITTLE GUY. I'll hack into your computer systems and then help you fix all the security holes. I specialize in working with small businesses and organizations, and I give priority to those facing government repression. My services include: hacking your organization from the Internet (comprehensive information gathering and reconnaissance, web application security testing, remote exploits), hacking your organization from your office (physical security, local network audits, and exploitation), wireless network security (slicing through WEP, brute forcing WPA), electronic security culture (evading surveillance, encryption technology, etc.), and other misc. services. More details at www.banditdefense.com, or email info@banditdefense.com.

INCARCERATED *2600* MEMBER NEEDS COMMUNITY HELP to build content in free classified ad and "local business directory" in 50 countries. John Lambros, the founder of www.BrazilBoycott.org, has launched a FREE classified ad, want ad, and local business directory in 50 global markets. The mission is simple: "free help to billions of people locating jobs, housing, goods and services, social activities, a girlfriend or boyfriend, community information, and just about anything else in over one million neighborhoods throughout the world - all for FREE. HELP ME OUT! SPREAD THE WORD! Please visit www.NoPayClassifieds.com and add some content. It will take all of five or ten minutes. Links to "No Pay Classifieds" are also greatly appreciated.

Announcements

JESUS LOVES HACKERS! www.christianhacker.org.

SOCIAL ORGANIZATION OF THE COMPUTER UNDERGROUND. A new 20th anniversary edition of the first sociological study of pirates, phreaks, and hackers is now available. Discover what it was like before the Internet and Operation Sun Devil. Free PDF version, other formats benefit EFF. Download at http://www.g2meyer.com/cu/

BLACK OF HAT BLOG. Covers topics such as cryptography, security, and viruses. Visit http://black-of-hat.blogspot.com.

WE LIVE IN AN INCREASING AGE OF MISINFORMATION, fraud, and dysfunction. We need more people exploring, collecting, and connecting public Intelligence in the public Interest (Cryptome.org, Wikileaks.org). I work as the NYC Director for the nonprofit Earth Intelligence Network. Our Online *Public Intelligence Journal* can be found at http://phibetaiota.net. We seek to reconfigure dysfunction by interconnecting and harmonizing the 12 policy domains with the top 10 global threats and 8 challengers. Related links: twitter.com/earthintelnet, youtube.com/earthintelnet, www.earth-intelligence.net, true-cost.re-configure.org, smart-city.re-configure.org. Contact earthintelnet@gmail.com.

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and Central America at 5110 khz. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2009 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600*, PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

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

Deadline for Autumn issue: 8/25/10.

"Everything that is really great and inspiring is created by the individual who can labor in freedom." - Albert Einstein

STAFF

Editor-In-Chief

Associate Editor

Layout and Design

Cover

Office Manager

Writers:

Telephone Historian:

Webmaster:

Network Operations:

Broadcast Coordinators:

IRC Admins:

Forum Admin:

Inspirational Music:

Shout Outs:

RIP:

2600 *(ISSN 0749-3851, USPS # 003-176); Summer 2010, Volume 27 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. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-2009 at
$25 per year, $34 per year overseas
Individual issues available from 1988 on at
$6.25 each, $8.50 each overseas

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 Line: +1 631 751 2600**
***2600* Fax Line: +1 631 474 2677**

Meetings

ARGENTINA

Buenos Aires: Rivadavia 2022 "La Pocilga."

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

CANADA

Alberta

Calgary: Eau Claire Market food court by the wi-fi hotspot. 6 pm

British Columbia

Kamloops: Old Main Building coffee shop in front of the registrar's office on Student St, TRU Campus.

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

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere near the Dunkin Donuts in the glass paned area with tables.

CHINA

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

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

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

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

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), lowest level. 6:30 pm

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

Norwich: Borders entrance to Chapelfield Mall. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

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

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

Paris: Quick Restaurant, Place de la Republique. 7 pm

Rennes: In front of the store "Blue Box" close to Place de la Republique. 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 phone booths on Wicklow St beside Tower Records. 7 pm

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

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

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

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

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

SOUTH AFRICA

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

SWEDEN

Stockholm: Central Station, second floor, inside the exit to Klarabergsviadukten above main hall.

SWITZERLAND

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

WALES

Ewloe. St. David's Hotel.

UNITED STATES

Alabama

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

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Unlimited Coffee, 741 E. Glendale Ave. 6 pm

Prescott: Method Coffee, 3180 Willow Creek Rd.

Arkansas

Ft. Smith: Sweetbay Coffee, 7908 Rogers Ave. 6 pm

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Mucky Duck, 479 Alvarado St. 5:30 pm

Sacramento: Round Table Pizza at 127 K St.

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

San Francisco: 4 Embarcadero Plaza (inside). 5:30 pm

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

Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm

Lakewood: Barnes and Noble in the Denver West Shopping Center, 14347 W Colfax Ave.

Connecticut

Newington: Panera Bread on the Berlin Turnpike. 6 pm

District of Columbia

Arlington: Champps Pentagon, 1201 S Joyce St (in Pentagon Row on the courtyard). 7 pm

Florida

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

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Orlando: Fashion Square Mall food court, 2nd floor.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court.

Idaho

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

Pocatello: College Market, 604 S 8th St.

Illinois

Chicago: Mercury Cafe, 1505 W Chicago Ave.

Rock Island: Cool Beanz Coffee House.

Indiana

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

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

Iowa

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

Kansas

Kansas City (Overland Park): Oak Park Mall food court near Street Corner News.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown at 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

Marlborough: Solomon Pond Mall food court. 6 pm

Northampton: The Yellow Sofa, 24 Main St. 6 pm

Michigan

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

Minnesota

Minneapolis: Java J's coffee house, 700 N Washington.

Missouri

St. Louis: ArchReactor Hacker Space, 2400 South Jefferson Ave.

Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall southern food court, 100th and Dodge. 7 pm

Nevada

Elko: Micro Binary Digit, 1344 Idaho St.

Las Vegas: Barnes & Noble Starbucks Coffee, 3860 Maryland Pkwy. 7 pm

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

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. 5:30 pm

New York

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

Rochester: Interlock Rochester, 1115 E Main St. 7 pm

North Carolina

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

Raleigh: Royal Bean coffee shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College).

North Dakota

Fargo: West Acres Mall food court by the Taco John's. 6 pm

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm

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

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm

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

Oklahoma

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

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm

Pennsylvania

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

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

Philadelphia: 30th St Station, southeast food court near mini post office.

Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm

State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

Trujillo Alto: The Office Irish Pub.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: J&J's Market & Cafe, 1912 Broadway. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Dallas: Wild Turkey, 2470 Walnut Hill Lane, outside porch near the entrance. 7:30 pm

Houston: Ninfa's Express next to Nordstrom's in the Galleria Mall. 6 pm

San Antonio: Bunsen Burger, 5456 Walzem Rd.

Vermont

Burlington: Borders Books at Church St and Cherry St on the second floor of the cafe.

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

Virginia Beach: Pembroke Mall food court. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

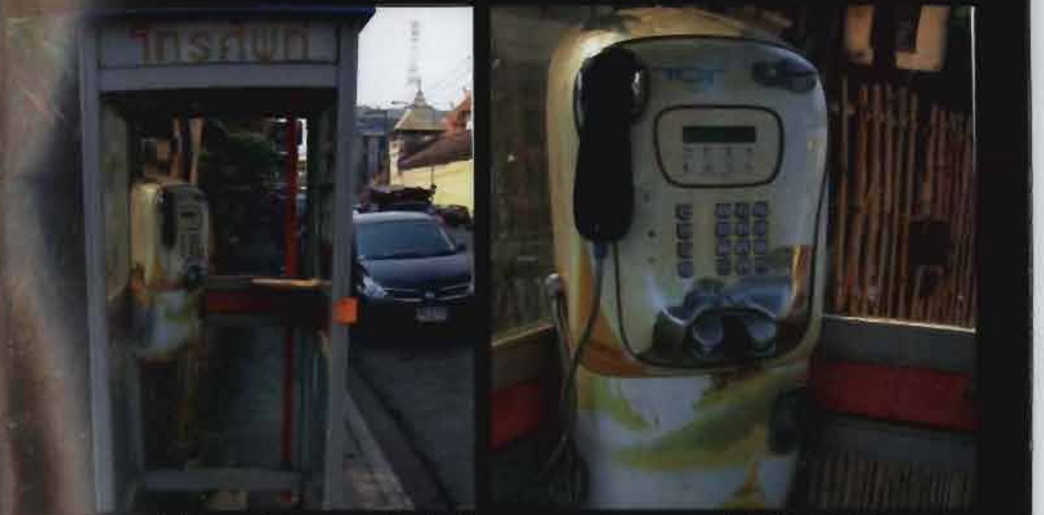
Spokane: The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

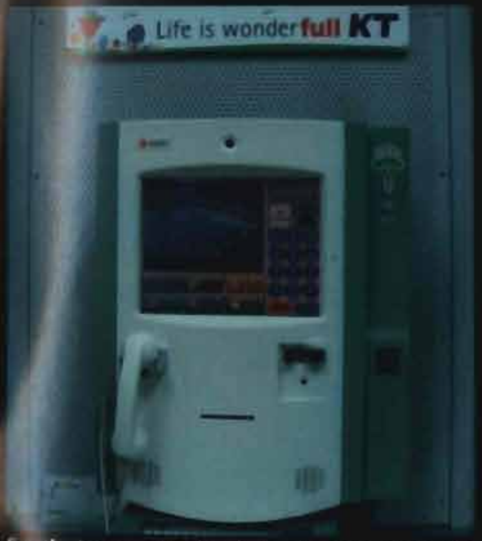
All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Mostly Asian Payphones



Thailand. Definitely one of the more alien-looking setups we've seen and the Thai alphabet on the booth only adds to that feel. Found in Chiang Mai near a Buddhist temple, we're not entirely sure if the color scheme on the phone is just a really neat design or the remnants of something truly disgusting that got all over it.

Photos by Martin



South Korea. It's hard to disagree with the sentiment expressed above this model when you realize that this phone is prepared to cheerily take on any task under the sun. Discovered at the Seoul airport, it's ready to surf the net for either coins or cards.

Photo by John Hilger

United States. Oh how the mighty have fallen. In this issue's only non-Asian contribution, we see the continued disrespect that payphones and former payphone kiosks are treated with. Spotted at the Tri-Cities Regional Airport in Blountville, Tennessee, it's apparently become necessary to remind people not to throw their trash into the space where the phone once was.

Photo by Peter Knauer

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
Email your submissions to payphones@2600.com.
Do not send us links as photos must be previously unpublished.