# The Back Cover Photos

You know it's your lucky day when a speeding locomotive heading in your direction has those magic numbers on it. Spotted in Wisconsin by **Mike Yuhas**, who was definitely in the right place at the right time.

This is from a hotel in Deerfield Beach, Florida, as discovered by **ateam**. There's another sign in the same complex that says "Guest Parking," but somehow this one tends to draw more of a crowd, who perhaps think this is where the Club Mate shipment comes in.

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 Four
Winter 2010-2011, $6.25 US, $7.15 CAN

# 2600

## The Hacker Quarterly

622 PHREAKS
THE BELL SYSTEM
Let your fingers do the walking...
112,000,000 people find it fast by shopping the Yellow Pages way.
Bell System Yellow Pages
Phreaks
Answer Promptly
Don't make a friend wait or miss a call by not answering your telephone at once
New! CARD DIALER
for fast dialing!
a night on the town?

# Payphones of Foreign Lands

**Cuba? United States?** We honestly don't know. It's that strange bit of reality where the USA somehow has a military base and infamous prison on the land of one of its enemies. And yes, they have payphones there. From the looks of them, they're a lot more American than Cuban. The phones on the left are located in front of the Naval Exchange (the Navy's version of Wal-Mart), while the remnants on the right are in front of a furniture store currently undergoing renovations. We're told the phones will be back.

***Photos by mavrik72***

**Hungary.** Found in Budapest, this old style booth is operated by Magyar Telekom (a subsidiary of Germany's Deutsche Telekom, hence the trademark pink handset) and also serves as an ad for a local cafe.

***Photo by Erwin Goslawski***

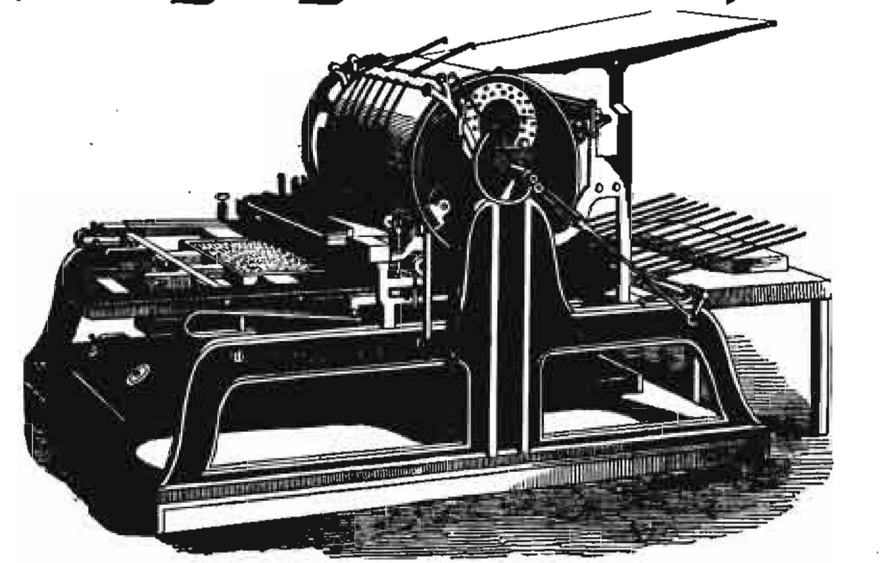
**South Africa.** In Pretoria, this is a fairly common sight. The payphone operator is a human. You pay them and you get to use the phone for a while. The system uses some sort of VoIP over 3G.

***Photo by Breto***

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)

# Revelations

# Changing Landscapes



As we all know, technology has been transforming virtually every aspect of our lives for as long as most of us can remember. In our early days of publishing, we focused primarily on how this affected computers and telephones. And, while these are still two of the primary focal points in our ever-changing technological landscape, the evolution has branched out so substantially that there is really precious little that has not been profoundly altered in one way or another.

Publishing is but one of the realms that will "never be the same." Much like the music and film industries, the rules of yesterday simply don't work in the world of today. New approaches must be tried, new inventions embraced, an entirely new ideology applied. We've seen resistance to these inevitabilities and the ensuing frustration that results when the old ways don't mesh with the new world. And that is another aspect of evolution: the removal of that which cannot adapt.

As hackers, it would be somewhat counterintuitive to shy away from something new and different. We have an obligation to scope out the changing scenery and report back, in addition to figuring out ways of tweaking things and making them more interesting.

This is what we hope to accomplish with some new projects we've gotten involved with in the last part of 2010. We have taken the first steps into the world of electronic publishing with the hope that there will be many more. We intend to keep the world apprised of our progress, so that we can all see the advantages and risks involved with such new developments.

The first thing many people want to know is what took us so long. To answer that, we need to explain that our magazine is rather unique. We operate solely on the support of our readers. That means no advertising dollars to bring down costs, inflate numbers, and dilute material. Major publications risk very little when they splash their content onto the web because along with it are splashed all kinds of flashy ads that most people don't bother to block. Advertising is what brings down the cost of paper publications (ever notice how many free ones are out there?) and makes it desirable to duplicate content, provided the ads are there, too. But this just isn't the case with a publication like ours. We try to keep things cheap and accessible in everything we produce without any sort of commercial sponsorship. And by keeping the support for this within the community, our message and tone won't be subverted by external forces with a completely different agenda. If you don't believe this is a real threat to the hacker world, just have a look at all of the so-called experts out there who claim to understand what our community is all about - and who always have something expensive to peddle, whether it be software, conferences, seminars, or books. Because we face these unique circumstances, we knew things wouldn't be quite as easy for us. But where there is support and a desire to succeed and innovate, there is a way to accomplish what you want to do. We believe we're on that path.

Our first step was to create an ebook version of the Autumn 2010 issue which was readable on devices like Amazon's Kindle and the Barnes and Noble Nook. The technology involved in these devices is quite impressive and has made reading both desirable and easy. One of the best examples of how useful they can be comes from a reader who told us how he was stuck on an airplane that had a long takeoff delay. While sitting on the runway, with a few key clicks, he was able to quickly download an entire issue onto his Kindle and escape the surrounding unpleasantness.

This new edition was met with much enthusiasm and publicity. But we still had hurdles to cross. For one thing, we were forced to sell this first issue as a single ebook, rather than offer a full yearly subscription to the electronic version of the magazine. This was because the terms for magazines were utterly terrible, and clearly designed for huge publications with lots of advertiser support. What a bitter irony that such new and promising technology would somehow manage to penalize the small and independent voices. And, as we promised to do from the outset of this project, we kept our readers in the loop on what we were trying to accomplish and what the challenges were. Miraculously, the terms for magazines changed within a month of our launch, making it much more acceptable for smaller publishers such as ourselves. As of this issue, we should be able to offer annual subscriptions on this new service.

But that was only the first step. We took another, relatively soon after this.

We've always wanted to offer something bigger and more comprehensive. The success of our two recent books (*The Best of 2600* and *Dear Hacker*) demonstrates the need for this as well. So we created a new book out of material from our most recent full volume, comprising issues from Spring 2009 to Winter 2009-2010. The layout was changed, new artwork was added, and *The Hacker Digest: Volume 26* was formed. In addition to having this available in the above formats, we also made a PDF version for sale at our online store. This version was capable of displaying graphics, pictures, and color in ways that would have been prohibitively expensive in actual print. And by not simply reproducing the material that was in these back issues, we wound up with something that was unique and useful - and only available in electronic form.

In addition, it was very important to us to not buy into the industry desire to control the publication through digital rights management or DRM. This is, after all, what we were dragged into court for back in 2000, as the first test case of the Digital Millennium Copyright Act. How hypocritical would it be for us to claim in court that people had the right to watch DVDs on whatever device they chose and then turn around and say they could only read *2600* on the devices *we* authorize? This is something we just couldn't do, despite going against what so many in the publishing industry were strongly advising. It's precisely this sort of narrow thinking that has stymied progress and annoyed the hell out of consumers. Perhaps this is also why such industries are in the downward spirals we've all heard so much about.

Clearly, this is serving as a test for us, and not one without risk. By going DRM-free, we make it easier for people to get our material just by copying it off a friend. As writers and hackers who primarily want the contents of the magazine to be out there, this is a good thing. But in order to sustain what we do (and the work involved simply in putting together the electronic editions was a great deal more than anything we had anticipated), we obviously need people to stand up and support our efforts. And that is how we're going to measure our success or failure in this endeavor and decide whether to expand it in the future and, if so, in what ways.

In a sense, this is a perfect test for the entire publishing world. If consumers are able to come forward and keep a publication like ours going solely through their support, as they have done with the paper version for the past 26 years, then we will have proven something about the value of advertising-free, non-DRM material. We will be saying that it's all about the actual content, and not the *control* of that content. Of course, the opposite could hold true and the industry giants may prove themselves more knowledgeable than we thought. If making our content available in an open manner results in the vast majority of readers simply grabbing it all for free somewhere, then our method of doing things clearly won't work.

Regardless of how it turns out, we're playing with this system and letting everyone know what it is we find out along the way. And isn't that what hacking is all about?

# you@host:~$ # Bash Bash Bash

**by Douglas Berdeaux**
**(Douglas@WeakNetLabs.com)**

I recently read that there is a struggle in the US lately with computer science majors and passion. Getting students excited enough to fuel their imaginations into producing innovative ideas, devices, and code seems to be a hard task. Being inspired isn't something that can be thrust upon students by just anyone. Being an inspirational teacher means that you are capable of showing your own passion for the subject along with sturdy knowledge to back it up.

Hackers, many of whom never even went to college or have a degree, come up with brilliant ideas every day. Is there then something to be said about our teachers today, if this struggle really does exist? I was recently asked if, in the last month, anything on the web really caught my attention or seemed innovative. My answer was, "no." A lot of things have simply repeated themselves, in different colors, shapes, or sizes. I was just hoping that my answer, plus the articles I had read about the struggle, were purely coincidental. Sadly, those fond of mathematics have no real consideration of coincidence. Let me attempt to help, by speaking of something for which I have passion: bash.

I love bash. In fact, in a recent job interview, thanks to my ADD, I was pondering what really fuels my passion for IT and realized that it was bash. Bash was coded in 1987 by Brian Fox, and is the most beautiful thing in the software side of computer science, in my humble opinion. So powerful and lightweight, it makes CMD.EXE look like a game. In fact, CMD.EXE was actually a hidden game I added to versions 1 and 2 of WeakNet Linux Assistant. When I see command line manuals and Linux magazines that talk about "shell commands," I laugh to myself. If you open those magazines, you will most likely find commands that do not come with the shell, like apt-get or awk. Sure, those commands can be invoked by the shell, but they aren't really part of the shell itself. In fact, the shell only comes with a few commands built into it that you can call "shell commands." These are called directly from the current shell, making them super fast. All other commands are spawned as new processes, spawned with a new instance of the shell, or loaded by the shell when called. The Wikipedia entry for "Shell Built-in" states, "usually used for simple, almost trivial, functions, such as text output."[1] I guess real system administrators don't have time to edit Wikipedia pages.

Here is a small list: `:`, `.`, `[`, `alias`, `bg`, `bind`, `break`, `builtin`, `cd`, `command`, `compgen`, `complete`, `continue`, `declare`, `dirs`, `disown`, `echo`, `enable`, `eval`, `exec`, `exit`, `export`, `fc`, `fg`, `getopts`, `hash`, `help`, `history`, `jobs`, `kill`, `let`, `local`, `logout`, `popd`, `printf`, `pushd`, `pwd`, `read`, `readonly`, `return`, `set`, `shift`, `shopt`, `source`, `suspend`, `test`, `times`, `trap`, `type`, `typeset`, `ulimit`, `umask`, `unalias`, `unset`, `wait`

There are tons of great bash references online. The best reference of all, I'd say, would have to be the O'Reilly books on bash.[2] Bash is a language, interface, interpreter, input, and output for errors and non error IO data as "terminals." It's flexible, powerful, resilient, and found almost everywhere you find Linux.

Just the other day, I realized that my system opened a new instance of VLC every time I double-clicked a media file in Nautilus. What a pain in the ass! I clicked around for a few minutes in VLC settings and Nautilus settings and couldn't find any solution. Well, bash to the rescue!

In Linux/Unix, all applications can be run from the command line. If you install something extra, it usually goes into `/usr/local/bin` or, if it's an administrative application, `/usr/local/sbin`. Sometimes you will see extra applications in `/opt`. Any applications that come pre-installed with your OS, or installed by the OS developer's pre-compiled repositories, will usually end up in `/bin` or `/sbin`. If you type `which <command name>`, you can see where the command is located. This is useful for debugging purposes if, say, you forget to uninstall an application before recompiling it and installing it from source.

Anyway, I typed `which vlc` and saw `/usr/bin/vlc`. I then moved the command to `/usr/bin/vlc_start` and used vim to make a new vlc file (`vim /usr/bin/vlc`). I added the lines:

```
#!/bin/bash
MEDIA=`echo $1 | sed -e 's/ /\\
➥ /g' -e 's/\-/\\-/g'`
killall -9 vlc_start
vlc_start "$MEDIA"
```

I then made the command an executable, by issuing `chmod +x /usr/bin/vlc`, and bash! The problem was solved.

Let's review the code. The first line is the "she-bang!" interpreter line. Bash knows that if it sees a file with this line in it, it uses the command to run the rest of the lines in the file that do not begin with a pound (#) symbol. A few interpreters include `#!/usr/bin/perl`, `#!/usr/bin/ruby`, etc. So in our case, it runs each line through a new instance of bash.

The first line it runs through the new bash instance is the line beginning with `MEDIA`. This assigns the first argument to the throw-away environment variable `$MEDIA`, after running the command in the back ticks. If you remember back to your algebra days, you might recall an acronym: PEMDAS. Parentheses, exponents, multiplication, division, addition, and subtraction all happen in that order, no other. It's part of math's "syntax," so to speak. Everything in back ticks will happen first, as if they were in parentheses. The `$1` is the built-in bash variable that represents the first argument given to the command. You can have up to `$9`, but then you have to add more syntax. You can also use `$*` as a glob for all arguments, but I'll show you that later.

The next line forcefully kills all instances of vlc_start which, if you remember, is the actual binary for the VLC media player. The last line starts VLC again, with the new file in quotes. Problem solved.

If you are a programmer, bash is a playground for you and your OS. There are the same looping and logical constructs found in most languages available to you right in bash. Once, at work, I was asked to fix a bad fstab file on an old Solaris 5 machine. This machine dropped me to a single-user mode shell without mounting `/usr`, so I had no access to any commands, besides those built into the shell. This wasn't a bash shell, but this can certainly be done in a bash shell. There was a backup of the old fstab file in `/etc`, but I couldn't use cat or cp to replace the broken fstab file. Thanks to help from an IRC friend, I ended up typing a one line, simple shell program like so:

```
while read foo; do echo $foo;
➥ done < fstab.backup > fstab
```

This code opened my eyes and mind to the the possibilities available with just the shell alone. What this code does is start a while loop and make a variable `$foo` for each line in the input file fstab.backup using the input pipe <. It then redirects the output to the broken fstab file, overwriting anything inside, using the > output redirection pipe. This was my first introduction to shell built-ins. This fixed the boot problem and made me wonder what else could be done with shell built-ins.

Another cool example I use in system administration practices, which I use almost on a daily basis, is creating functions. Just like in a programming language, you can make functions or groups of code and pass data to the code. In this example I will keep it simple and create a l33t translator. You can start typing this out on the command line, as it will not finish the command until you add the ending } followed by a newline character.

```
l33t {
$* 2>/dev/stdout | sed -e 's/E/3/
➥gi' -e 's/L/1/gi' -e 's/A/4/gi'
➥ -e 's/o/0/gi' -e 's/G/9/gi'
}
```

This will change all of your text into cool l33t text! To pass data to it, simply call it with an application. `l33t dhclient eth0`, `l33t aircrack-ng -w /path/to/wordlist -0 capturefile.cap`, etc. Some downfalls are that tab auto completion breaks and some captive applications seem to go slower, but this simple exercise shows you how to group applications to simply change the output. Think of the possibilities for applications that do even more!

One last example I would like to show is one that benefitted me in a time of need. I purchased music from `LegalSounds.com` and was given a txt file detailing where the MP3s were on their servers. I ran wget on each file in a row after creating a shell script that simply added wget to the beginning of each line in the txt file. Then I used chmod and ran the executable. I dumped the songs onto my Android phone and left for the day. When I tried to play one of the songs, I realized that Android was not detecting the files on my SD card! When I browsed the directory tree, I saw them and the problem. Some how an extra "%3D" was added to the end of each file extension! I then thought the best way to handle all of these was to loop through them and rename them, right? Beautiful bash can do this. Here is how I did it on my Android phone using the terminal:

```
while read foo; do bar=`echo $foo
➥ | sed 's/%3D$//g'`; mv $foo
➥ $bar; done < names.txt
```

See how this does more than just output text? Think of the powerful possibilities! This solved my problem rather quickly!

Let's wrap this article up by covering a few bash favorites of mine. Tab auto-completion is number one. A systems administrator isn't lazy, but has too much on his or her mind to be ls'ing or using find to run applications or pass files as arguments. Recently, the matched strings from grep filters have been colorized by default.[3] This is awesome for anyone who is new to regular expression syntax and wants to see exactly what he or she matched. History, found in `~/.bash_history` is also an amazing feature. You can use the up and down arrows to access your recent command history. Sure, this is available in DOS, but does DOS have a CTRL+R command history shortcut that allows you to type strings to match patterns of old commands right from the command line? I don't think so. The terminal emulators that display bash and other shells have also come far since I started using them. Now you have Compiz, and graphics drivers that allow you to have full, true transparency while coding! Who knew 20 years ago, that people would be using Unix shells in X, let alone with beautiful transparent windows and fonts?! DOS can't even maximize properly and it's the year 2010. Environment variables can be made, changed and removed. If you export a variable, it goes away once you exit the shell. These are immensely useful when used in the right places. Sed, awk, and grep also need to be mentioned. These don't come with bash, but exploit the beauty of the bash pipeline. Bash can pipe IO into or from other commands or files using the |, >, <, and >> operators. If you add a 1 or 2 in front of the pipes, you can send STDOUT and STDERR into files and other commands as well! Here is a small example of awk/sed/grep and pipelines with STDERR:

```
cat file.txt 2>/dev/null | awk
➥ '{print $1}' | sed 's/e/3/gi' |
➥ grep -v 'LOL HI'
```

This dumps the contents of file.txt to the screen (STDOUT), but is interrupted by the 2>/dev/null, which sends all errors[4] (binary file matches, no file found, etc) to /dev/null (the UNIX garbage can). It gets interrupted once more by the pipe |, which sends the output to awk, which prints only the first word in each line, delimited by any whitespace character. The output still doesn't quite make it to the screen, as it is once again interrupted by a pipe and sent to sed, which substitutes all "e"s for "3"s. Then one last interrupt sends the parsed data to grep and grep discards all lines that have 'LOL HI' somewhere in them but prints all the lines that don't to the screen in real time.

Everything in Unix is a file. Files have words, and strings and such, which make these utilities powerful and beautiful. There is so much more to bash that I couldn't cover in this article, and if I had, may have interrupted the spark that makes someone interested enough to find out more for him or herself. The spark of passion.

### References

1. http://en.wikipedia.org/wiki/Shell_builtin
2. Learning the bash Shell: Unix Shell Programming (In a Nutshell (O'Reilly)), Bash Cookbook: Solutions and Examples for Bash Users (Cookbooks (O'Reilly)), and Classic Shell Scripting
3. Try changing the environment variable GREP_COLOR!
4. This is left up to the author of the application used. Some simple applications will print errors to STDOUT by default.

# How to Cheat at foursquare™

**by therippa**

In the last couple of months, I've noticed a new trend popping up on my Facebook newsfeed: friends checking into places using Foursquare. Foursquare is a service that allows you to let the world know what restaurant you've been to, what gas station you've filled up at, and what bar you've been frequenting. Each local business has its own page letting you know who's been there, with a special "Mayor" designation for the person who has checked-in there more than anyone else. Frequenting a location multiple times sometimes gives that person special benefits: a free item, preferred seating, etc. Recently, a friend of mine made it his mission to become the Mayor of his favorite cafe, obsessing over it like the high score of an old arcade game. After a month or two of eating there a few times a week, he earned the Mayor badge on his Foursquare page.

Now, personally, I find Foursquare to be the same sort of overshare/masturbatory experience that Twitter has become. I have no interest in demanding that people pay attention to the insignificant details of my daily life. But, after hearing how upset he got when he temporarily lost his Mayor status, I saw an opportunity for a little mischief. I was to become mayor of his cafe, without ever stepping foot in there.

## How Check-ins Work

When you check-in to a place on Foursquare, it is typically done through an application on your phone. Previously, the applications were not location-aware, so you could say you were eating somewhere when in fact you were across town. This caused cheating problems on the service, and the process was changed so that only check-ins including your GPS location would technically add to the running tally you keep. You could still check into an establishment without your location, but it wouldn't count towards your one day becoming the Mayor or receiving any other random badges.

My first thought was to find a GPS location spoofing app for my jailbroken iPhone. I found one and it worked well, allowing me to fake the location and check-in. The downfall, however, was the 10-day trial limit on the app, and the fact that I had a new Android phone being delivered that didn't have an application with these capabilities.

After some searching around, I found a Firefox extension named Foursquarefox that allowed check-ins over the web. I downloaded and installed it, provided my Foursquare login, and it found my location to within three houses of where I live. After poking around in the source code of the extension, I learned that it was using Google's Geolocation API to determine where I was. This API cleverly uses your IP address and a list of nearby WiFi beacons (provided by Firefox) to approximate your location. It returns a JSON string containing your location data, and I knew it would be a cinch to spoof.

After about a half-hour of debugging and tweaking, I had modified the extension to include input boxes that allowed me to enter my latitude and longitude, overriding what was supplied by Google's Geolocation. By doing this, I could check-in to any place I wanted and Foursquare would think I was physically there.

## Method

1. Make sure you are running Firefox 3.5 or greater. Previous version do not support Location Aware browsing.
2. Google search for Foursquarefox and install the extension. Restart Firefox and enter your Foursquare account information into it.
3. Close Firefox, and browse to your extensions folder. On Windows, this can be found in %APPDATA%\Mozilla\
➥Firefox\Profiles\
➥<profile name>\extensions
4. There should be a folder named {8D8755DA-0541-4E4C-818A-
➥99188622BA02}, open this and then open the chrome folder.
5. In this folder will be a file called foursquarefox.jar. Even though the extension is .jar, it is a zip file. Extract all of its contents to a temporary directory.
6. Once you have your .jar file expanded, open the file foursquarefox.xul. This is the file that defines the user interface of the extension. Look for a line that says <toolbaritem id="fsxlogin"> and add this chunk of code directly below it:

```
<bbox>
<checkbox id="fsfx-toolbar-
➥custom-checkbox" label="Use
➥Custom Location" />
<label value="Latitude:"/>
<textbox id="fsfx-toolbar-
➥custom-lat" width="60px" />
<label value="Longitude:"/>
<textbox id="fsfx-toolbar-
➥custom-long" width="60px" />
</bbox>
```

This will create new elements on the extension toolbar that allow you to enter your custom location

7. Open the file /com/chrisfinke/geolocation.js, find the line that says var json = JSON.parse(req.responseText); and this chunk of code directly below it:

```
if (document.getElementById
➥("fsfx-toolbar-custom-
➥checkbox").checked) {
json.location.latitude =
➥ document.getElementById("
➥fsfx-toolbar-custom-lat").
➥value;
json.location.longitude =
➥document.getElementById("
➥fsfx-toolbar-custom-long").
➥value;
json.location.address.street_
➥number = "Custom";
json.location.address.street =
➥"Location";
json.location.address.city =
➥"Lat/Long";
}
```

This code tells the geolocation wrapper that if you checked the checkbox, to ignore the data returned from Google and use the data you entered instead.

8. Using your favorite zip utility, zip all the contents back together (making sure to preserve the directory structure) and name the file foursquarefox.jar.
9. Replace the old .jar file with the new one you just created.

If you did this all correctly, when you re-open Firefox the Foursquarefox bar should now have your checkbox and input fields. You now have the ability to check-in to anywhere from anywhere; all you have to do is use a latitude/longitude map to find the coordinates of where you'd like to be, enter them into the text fields, check the box, and refresh your location. When you click to check-in, you will be presented a list of locations within that proximity. Enjoy!

# The (Obvious?) Dangers of Free WiFi

**by Azazel**

Free public WiFi hotspots are pretty commonly available these days. Libraries, Barnes and Noble, and Starbucks are just a few places where one can go and connect to the Internet for free. Of course, by now everyone knows the dangers of connecting to these hotspots, right? Well, obviously not or I wouldn't be writing this. Here, I'm going to walk you through one of the greatest dangers of connecting to a free, unencrypted wireless access point: the notorious man-in-the-middle attack. Keep in mind, this attack can be perpetrated on any WAP the attacker has access to, whether he legitimately has access or has cracked a key to gain access. The fact that these public access points are open just makes it that much easier. If you try anything demonstrated here, make sure to only do so on a network in which you have permission from the administrator.

First, let's change our MAC address. After all, we're joining a public network, we want some privacy for crying out loud! Open a console and type:

```
ifconfig eth0 down
ifconfig eth0 hw ether
xx:xx:xx:xx:xx:xx
ifconfig eth0 up
```

where eth0 can be replaced with whatever your wireless interface is and the x's are replaced by whatever 48-bit hexadecimal number you choose for your new MAC address.

Now let's join the network. If it's an open network, as free hotspots are, this is easy enough. Once you've joined, type ifconfig in the console to see what IP address you've been assigned. In order to find a target, we'll have to find another host on the network. You can use any scanner for this, but I prefer nmap. For the purposes of this article, we can just do a simple ping sweep by using the command:

```
nmap -sP 192.168.1.0-254
```

Make sure to use the appropriate private IP range and subnet for the network you're connected to. You'll get a list of hosts who are up and on the network. Run a quick check for the default gateway by typing route -nee and make a note of the gateway IP address.

The next step is ARP poisoning the victim and becoming the man-in-the-middle. For this, we'll use Ettercap. Ettercap is a very versatile suite with many useful tools. In fact, had we chosen to, we could've used this for the host scan. It can be used for packet sniffing/logging, data injection, and many other things which we will touch upon later. But we still need to do a little configuring before we can continue. We will first need to enable IP forwarding, so open a console and type:

```
echo 1 > /proc/sys/net/
➥ ipv4/ip_forward
```

Next, open the etter.conf file and under "Linux" remove the comment hashes in the two statements following the if you use iptables line. Ettercap is now ready to go. In a console enter the following:

```
ettercap -i eth0 -Tq -M
➥ arp:remote /gateway_
➥ipaddress/ /victim_ipaddress/
```

Here, -i indicates your interface. The -T switch designates a text only interface. By pressing "h" while in this mode, you will get more options, including the option to activate plug-ins. -M starts your man-in-the-middle attack, where arp:remote is your method:argument. By specifying rap, we are using the ARP poisoning method. ARP poisoning, also known as ARP spoofing, essentially fools the network nodes into associating the attacker's MAC address with that of another client. As such, traffic meant for the victim will go to the attacker, who can then choose to forward that traffic along to the intended recipient (as we will in this case). Alternatively, the attacker could associate a non-existent MAC address with the default gateway which would result in a DoS. And that's it! As an attacker, you now stand between the victim and the gateway and have the ability to intercept and manipulate all the traffic between them.

Let's go a step further in demonstrating how dangerous free hotspots are. Let's start Ettercap with this command instead:

```
ettercap -i eth0 -Tq -M arp:remote
➥/gateway_ipaddress/ /victim_
➥ipaddress/ -P remote_browser
```

Launch Firefox and watch as your browser seemingly navigates itself. Actually, you're following along with what the victim is browsing. As the victim navigates to Gmail or eBay or other SSL sites, keep an eye on the console where you first opened Ettercap. The victim's credentials will appear as they are supplied. Ettercap passes spoofed certificates to the victim. So all the victim will notice is a certificate as they attempt to sign in. This attack is based on the assumption that people will just accept these blindly. The victim may think that they are receiving this just because they are on a different network or, more likely, they may not care. Either way, there's a good chance it will be accepted and they will then enter their credentials.

If you're having a problem getting the remote_browser plug-in to work, open up etter.conf again. Under [privs] change the values of ec_uid and ec_gid to 0. Then scroll down to the line that reads remote_browser = mozilla -remote openurl(http://%host%url) and change mozilla to firefox.

The attacker has seen the browsing habits of the victim and obtained information to access secure sites at a later time. What this really means is the attacker may now know the victim's interests or place of employment and may have access to the victim's personal information. From here, we hardly have to use our imagination to consider what could happen to the victim. The attacker has enough information off of which to base some clever social engineering attacks and this innocent, though ignorant, WiFi user who just came to have some coffee and check e-mail has become a potential victim for identity theft.

As I said before, Ettercap is a versatile tool. An attacker can ARP poison more than one victim at a time, although if you're following along with them in a browser it can get messy. There are many other things that can be done while acting as man-in-the-middle. I will mention some, and Ettercap can be used for most of them, but I will not go into detail. An attacker can redirect traffic. For instance, if you hate Best Buy, you can redirect all requests for bestbuy.com to anti-Best Buy sites. An attacker can also manipulate data, replacing pictures or snippets of text. Play around with different switches and plug-ins, read the man pages, experiment with it, and have phun! Most importantly, remember how insecure Free WiFi hotspots are.

## Playing "D"

How can we protect ourselves against man-in-the-middle attacks? Obviously, don't use public WiFi spots. But if you have to, do not do anything you wouldn't like anyone else to see, especially typing in usernames or passwords. As an administrator of a small network, you can implement static IP addressing as opposed to DHCP. Also consider implementing static ARP tables. Enabling MAC address filtering on your router may also help prevent unauthorized clients from joining your network. All of these methods will work on larger networks as well, but will become quite cumbersome for the administrator. A program like ARPwatch, or WinARPwatch for Windows, will monitor your ARP cache and let you know if a known association of IP addresses and MAC addresses has changed. Also, don't broadcast your SSID. Make sure to use a complex WPA2 passphrase using a combination of uppercase and lowercase letters, numbers, and non-alphanumeric characters. Don't use words that will be found in a dictionary.

One last thing: the reason we initially spoofed our MAC address was because a vigilant user or admin could easily find the MAC address of an attacker by checking their ARP cache, using the command arp -a -i <device name>, or arp -a in Windows.

# The Buck Stops Here: Inside AT&T's Tier 2 Tech Support

**by kliq**

A recent *2600* article, "How AT&T Data Plans Work (and How to Make Them Stop Working)," inspired me to document my time as a Tier 2 Tech Rep for AT&T Mobility. In the customer service world, Tier 2 tech support is the highest phone support available. Statistically, your chances of getting a college graduate and/or someone who understands the network are extremely low. The majority of Tier 2 reps are generic customer support reps that are moved to a specialty department due to outsourcing. They are given five days of tech support training and then sent to begin taking your calls. At the beginning of training, they are given a brief overview on how a wireless network works, but aren't expected to comprehend or retain the information. AT&T doesn't want to pay them to understand how phones communicate with the network, but just to learn the process of basic troubleshooting steps and how to file a ticket for the engineering team to investigate in the local area. To put it simply, a background in technology is not required to troubleshoot one of the largest wireless networks in the country.

With the combination of systems I was given access to (a more refined coverage map and an Orwellian-sounding program called Snooper that identifies what portions of the network the customer is connected to), I've seen first-hand how truly awful AT&T's network can be. Of course, your personal experiences may vary, but from my eye in the sky, the only places the network consistently worked for 3G-intensive phones (read: iPhone) were bigger cities out west that had the infrastructure without the population density of the east coast. Live in a rural area? 3G coverage is thin, if it exists at all. Live in an urban area? The congestion is so bad that I saw NYC iPhone users whose call histories were seemingly infinite lists of "Network Congestion" errors from Snooper. As tech reps, we were given periodic updates from the president of AT&T mobility, Ralph de la Vega, about how much money AT&T was spending on "upgrading" the network for places like NYC and San Francisco, without ever acknowledging fault for a lack of infrastructure to support the products we were supposed to be selling.

Despite the lack of training, one would assume that all information regarding both phones and the network would be listed within some sort of database for the tech rep to research. This system is called MyCSP, and the information was often incomplete, out of date, or completely missing regarding technical issues. The information regarding billing issues, however, was often updated and very robust. If you were to follow the "decision flow" (a series of Q and As that are used to narrow down a phone's issue) on the iPhone, for example, it would offer to check signal bars, power cycle, soft reset, or change SIM cards. Users familiar with iPhones have known all along that the signal strength on the phone is wildly inaccurate, a fact that Apple finally acknowledged with the release of iOS 4. Nowhere in MyCSP did it show the rep how to perform an iPhone field test, which gives the most accurate signal reading, by pressing *3001#12345#* from the dial pad. Curiously, Apple removed this feature from the iPhone 4, so the actual signal levels you are now receiving is a complete mystery. When customers called in frequently due to reception issues with their iPhone, I would always ask if anyone had performed a field test and the answer was "no" 100% of the time.

The lack of information is not limited simply to Tier 2 reps. I often worked tickets, meaning I reviewed work that had been done in the field and contacted the customer to see if the issues were persisting. I'd get a lot of tickets rejected by the engineering team for "lack of information" when in fact all the information required was submitted with the ticket. If the engineers in the field routinely rejected network tickets due to a lack of reading comprehension or due to a misunderstanding of how the network works was left unanswered. I was always told by supervisors to rephrase what was written and resubmit the ticket. Meanwhile, the customer's service was still out.

Finally, to gauge performance of our jobs, our calls were periodically graded. Whether the issue was fixed or not was often an afterthought (I suspect the graders didn't know that much about how the network worked, either) but how the information was presented determined if a call passed or failed. For example, did the rep say the customer's name enough? Did they sell them something? Did they mention that the customer has an upgrade available, so that they can buy another phone that doesn't work? Despite the fact that the department was called technical support, there was a lot of pressure to sell as many features as possible. The suits looked at each interaction, no matter what the issue, as a sales opportunity. Keep all this in mind the next time your service goes out, but please note I won't be there to take the call.

# TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! Winter in Beijing is bitterly cold and very dry (the Gobi desert is nearby), so it's nice to leave town every once in awhile. I'm writing to you from a sprawling telecommunications complex near the Tokyo suburb of Kawaguchi. Japan was once the world's premier high-tech center but is now a shrinking and aging giant, having recently lost its status as the world's second largest economy to China. Even still, the scale of operations here is amazing compared to the U.S. With Japan's wealthy and tech-savvy population, Japan remains one of the most wired places on the planet.

My first visit to Japan was in 1997, and I was amazed then at how high-tech everything was. While we were still retiring the last of our analog switches, NTT had long been all-digital and was even deploying high-tech ISDN payphones throughout the country. The train and subway systems were computerized throughout (everything from fare collection to signaling) and ran precisely on time. Akihabara was the go-to place for the hottest technologies in the world. And Japan used a strange and wonderful standard called PDC for its mobile phone network. It was fully digital, unique in the world, afforded incredible battery life to handsets, and supported advanced data features like web browsing, picture mail, and QR codes long before these became popular elsewhere.

Vending machines were everywhere, too. You could buy cigarettes, alcohol, condoms and even an alleged schoolgirl's pair of soiled used panties out of a vending machine - along with more conventional items like hot canned milk tea. Some restaurants sold preprinted order tickets out of a vending machine, which you could deliver directly to the kitchen.

All of these things still exist today (including the ISDN payphones, most of which haven't seen data usage since 1999 but are still meticulously maintained - and, yes, vending machine panties). Japan is still an exciting and dynamic place to visit, and remains one of the most important telecommunications hubs in Asia. Still, visiting there feels like a visit to an aging friend's house. You know that friend who was a big gadget freak five years ago, and bought a ton of really cutting edge stuff, but he still has all the same stuff and has never updated it because it all works just fine, so why change anything even though he's falling behind the curve? Well, Japan is like that friend. Everything is still high-tech and it all still works, but it's aging and yellowing and is often much more complicated than it needs to be.

Japanese mobile phones used to blow the world away with their innovation. It was the first country in the world with a working mobile payments system (and even today, leads the world in mobile payments). When we were still using monochrome candy bar style phones, Japanese consumers had flip phones with cameras and color displays. Sure, your phone couldn't roam in Japan, but Japanese phones were so exciting and futuristic that you understood your phone just wasn't worthy of such a magical place.

These days, Japanese mobile phones feel like a step backwards, even though they remain advanced overall. The most popular type of mobile phone in Japan is an aging design: a basic flip camera phone. Sure, the display is gorgeous and the camera is 12.1 megapixels, and the phone has a 700MHz processor and can run highly complicated GPS-based mobile applications (such as a popular dating service that alerts you when you're in the proximity of another subscriber who matches your profile and interests). Still, touch-screen phones that have taken the world by storm (you see them everywhere in China) just haven't caught on in Japan, except for a popular Android-based half-tablet. This is fairly surprising given the popularity of mobile mapping services in Japan.

Android and iPhone are the most popular smartphone platforms, but smartphones seem less popular in Japan than in other places. One reason, of all things, is the lack of native Japanese emoticon support. These are incredibly popular and the lack of support is actually a serious problem. Also, Japanese feature phones are so feature-rich and are capable of running so many applications that smartphones aren't as necessary. Japanese feature phones also make it very easy to send email, which is very popular. Input in the Japanese language can also be a clunky problem with smartphones, most of which aren't designed exclusively for the Japanese market. Local Japanese feature phone brands (Sanyo, Anycall, Sharp, etc.) are the most popular. Samsung and HTC have made some smartphone headway, although very limited, and (of course) the iPhone is popular. Most surprisingly, although Nokia is a huge player in China and much of Asia, their phones are hardly even available in Japan.

There are still some unique characteristics to Japanese mobile phone usage, owing both to the unusual rate plans and to Japanese cultural norms. SMS hasn't caught on because most carrier rate plans allow Japanese consumers free data usage, including email. However, SMS is charged per message, making it less attractive. Japanese people have also become accustomed to sending longer messages, and the 140 character limitation is insufficient for most users. As is the case in many places throughout the world, callers to mobile phones are grossly overcharged but mobile phone subscribers receive their calls for free. This on its own isn't enough to keep people in most countries from making phone calls anyway, but Japan is a hyper-courteous society. It's only socially acceptable to use data services (such as email and Web browsing) on the train. In fact, there are signs posted on trains reminding people not to talk on their mobile phones.

You can subscribe to pre-paid and post-paid mobile phone service. However, signing up is complicated because (in an increasingly popular bureaucratic snarl around the world) the police require linking a Japanese ID card or residence permit with every new phone. Foreign passports aren't legally sufficient to subscribe, so you'll either need to be resident in Japan with the appropriate permit, or will need the help of a Japanese friend to get started. Rate plans are generally higher for pre-paid service; for example, SoftBank's popular service charges the equivalent of nearly $1 per minute for local phone calls. Prepaid phones also cost more, starting at around $50. Visitors tend to either rent phones at the airport or roam in Japan using a phone from their home market, both more expensive but less troublesome alternatives.

Post-paid service provides a subsidized handset (often sold for only one yen), but requires a credit check and two year contract, similar to the way post-paid plans work in the U.S. As in the U.S., handsets are generally locked to the mobile carrier that issued them, and (for a variety of reasons) are almost impossible to use on other networks even if they're unlocked. You need to be a permanent resident in Japan with a Japanese bank account in order to subscribe, and carriers generally require payment via direct debit from your account.

There are three major mobile carriers in Japan. The oldest and most established carrier is NTT DoCoMo, which runs a WCDMA 3G network. The same technology is used by SoftBank, Japan's smallest carrier, whose small, shaky network has been substantially expanded and improved in recent years. SoftBank is the exclusive carrier for the iPhone in Japan. KDDI runs a network called "AU," which uses the same CDMA 1xEV-DO standard as is popular in North America and South Korea. Most WCDMA phones are backwards compatible with GSM and can be taken overseas, but CDMA phones generally are not. To compensate, KDDI sells a number of multi-mode handsets which support CDMA, WCDMA, and GSM, in order to ease international roaming.

Roaming in Japan used to be impossible, but air interface standards and frequencies used are gradually becoming consistent with the rest of the world. This means I'm now able to use my WCDMA-capable HTC Diamond to roam on NTT DoCoMo. This is a basic unlocked GSM world phone, which supports GSM, EDGE, UMTS, and HSDPA on 850, 900, 1800, 1900, and 2100MHz frequency bands. However, even though it's technically possible, roaming is not advisable. On my China Unicom SIM card, data roaming costs about $15 per megabyte and voice calls cost from 75 cents (and up) outbound to $1.50 inbound (oddly enough, receiving calls is more expensive than placing calls).

And with that, it's time to close out another quarter of "The Telecom Informer." Stay safe this winter, and if your travels take you to Japan, don't forget your ISDN modem!

*Shout outs to Bul-lets, Roots Tokyo, and Tokyo Hacker Space - thanks for the friendly hospitality!*

# [redacted]

**by Dufu**

Everything you read here is total fiction. Or at least that is what I am claiming, so that if UPS tries to track me down, I can say it was a work of creativity and not an admission of guilt.

What you do with this information is up to you, but as I always teach those around me, "Keep hacking. Keep it moral. Teach others. Become a leader of the ignorant, not their enemy."

I have debated for a while as to whether I should write this article. Although UPS can, and may very well, fix the issues I bring up here, it will probably translate into higher costs for everyone who uses their service. It may also cause some serious service disruptions as their own employees adjust to the fixes, because their system is highly standardized.

## Shipping Weight and Size Loophole

If you call a UPS representative and ask them what you should do when shipping a package of unknown size and weight, they will generally tell you to make the best guess you can. This is because the conveyor and human inspection system is supposed to catch oversized and overweight packages and automatically reclassify them and back charge the sender accordingly.

Most UPS representatives will tell you that the back charges for a mislabeled package will arrive on your next bill automatically. This is not necessarily true.

Here is my situation and what I have learned. I send a good number of UPS packages on a regular basis. Not Amazon's level of shipping, but generally more than the average business. Often, my customers need to send an item back to me. Sometimes I know what it is, and sometimes I don't. Most of the time, I have no clue how their shipping department or shipping drone will package the items. Will they put a 2 lb. part the size of a soda can into a box that is 18" square with lots of padding? Sometimes they do. At other times, they simply put the part into the large box and let it rattle around in transit. Rarely, they properly package it. In any case, guessing the weight and size are virtually impossible.

### What I Do

Since I never know how the item will be packaged when coming back to me, I never know how much it will weigh or the size of the box. Yet I am willing to pay the return shipping for my wonderful customers. I could provide my UPS account number to the customer and let them simply fill in the details on their UPS shipping screen, but that's no fun and it exposes my account number to an untold number of potential threats. What I choose to do is create a shipping label from me, to me. I'm in the Northeast. My customer may be in California. Regardless, my shipping label says the package is going to travel zero (or very few) miles and not cross any UPS zones other than my own. I also leave the size blank and set the weight to show one pound. This generally translates into roughly a $5 charge for me, per box, on all returns.

### What I Expect

I expect my customer to print the PDF I send to them, stick it on the pre-packaged box and hand it to a driver. I expect that somewhere along the way, UPS will see the error in size, weight, and origin, and bill me appropriately.

### What I Get

In twelve years of shipping things on a daily basis, not a single back charge has ever been applied to my account, until two days ago when they re-rated a package for the very first time to accurately reflect the weight and origin. I'm not sure if this is a new trend for them or just a coincidence, but I thought it worth mentioning since it pretty much makes this portion of my article useless if it is a system-wide, reliable change in their policy.

Somewhere around one package a month is shipped back to me this way. I have shipped 70 or 80 pound packages back to myself, with thousands of dollars in additional insurance coverage, and yet nobody has noticed the extra size, weight, origin, etc. Note that anything over 70 pounds is supposed to come off the conveyors and go into a manually sorted and handled process. I'm not sure if that happens or not with my stuff that is over 70 pounds, since the label indicates a single pound package, but I'm sure the drivers notice! I have shipped numerous packages from the same customer back to myself, all with the same low weight designations.

Do I feel guilty about never having been properly charged for these returns? Only enough to keep me from shipping all my stuff out that way in the first place. Imagine if all my packages were labeled at one pound and no size provided. I'd make a killing on my shipping costs, and I'm sure UPS would either take a very long time to catch on or maybe never catch on. But I'm a non-malicious hacker so I can't do that. It would simply be stealing to me, and I hope to you, too. Malicious hackers have caused more damage to our image over the years than anything else, in my opinion. But I digress.

If I could more properly estimate the weight and size of my returns, I'd do so. Until I can, I'll keep doing what I do. After all, the UPS representative told me it would work out okay that way.

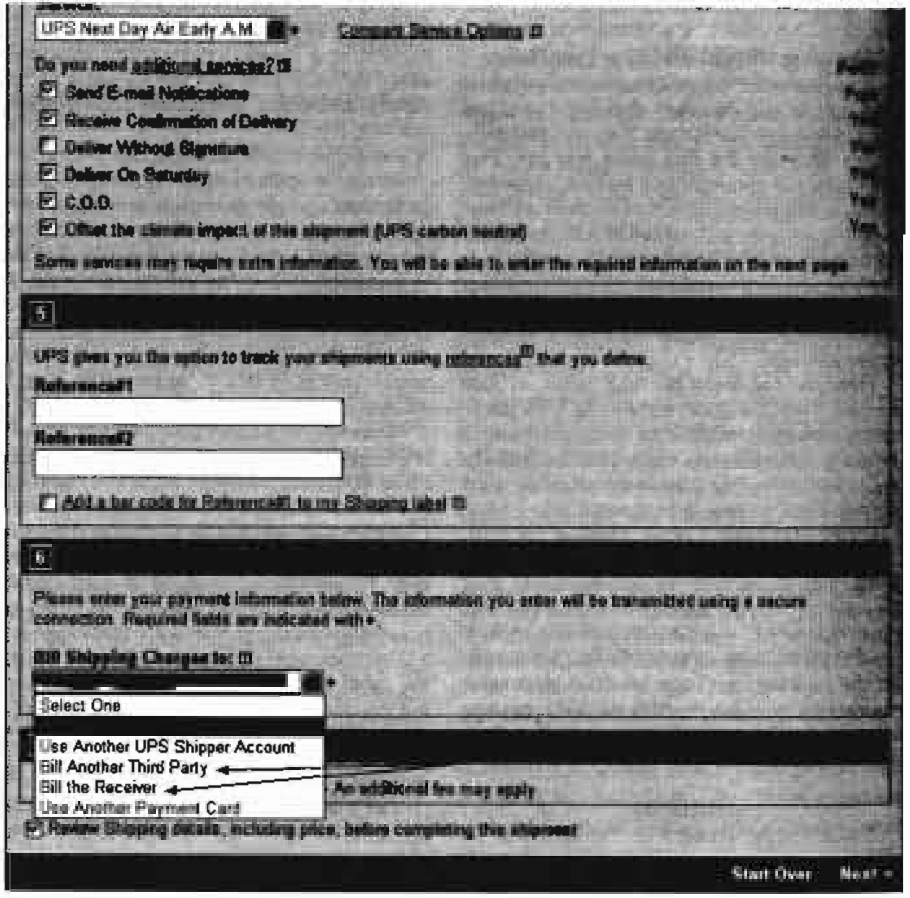
Now, keep in mind that there is yet another potential exploit of the system here. What if you changed your shipping and billing address to one a block away from the destination each and every time you sent a domestic shipment? You could change it back right after processing the shipment and UPS would charge you for a local, one zone shipment, even if you were shipping from Oregon to Florida. I'll let you digest that for a bit. If you can't follow me on that one, then I suggest you start over at the top and re-read what I've already said.

### Tracking Number / Account Number Vulnerability

There have been a few articles written over the years on UPS tracking number structure and all that is related to that. What I have yet to see is an article written about how to exploit the system based on the information provided in the tracking number, at least to a degree that most people can benefit from it.

Every UPS package you receive contains a decently long tracking number. Typically, they start with 1Z. If they are international, they often start with something else. If you ship or receive a lot of packages, or track everything you send or receive, you will notice that UPS has one of the longest tracking numbers in the industry. That's just semi-random information for you and for the folks to discuss in future articles.

Back to your specific package. My best guess is that the first two digits designate the originating location or country. Someone wrote about it once, but I've already forgotten that info because it doesn't serve my curiosity very well.



UPS Next Day Air Early A.M. ▾ Compare Service Options

Do you need additional services?

☑ Send E-mail Notifications
☑ Receive Confirmation of Delivery
☐ Deliver Without Signature
☑ Deliver On Saturday
☑ C.O.D.
☑ Offset the climate impact of this shipment (UPS carbon neutral)

Some services may require extra information. You will be able to enter the required information on the next page

5

UPS gives you the option to track your shipments using references that you define.

Reference#1

Reference#2

☐ Add a bar code for Reference#1 to my Shipping label

6

Please enter your payment information below. The information you enter will be transmitted using a secure connection. Required fields are indicated with •.

Bill Shipping Charges to:

Select One
Use Another UPS Shipper Account
Bill Another Third Party
Bill the Receiver
Use Another Payment Card

An additional fee may apply

☑ Review Shipping details, including price, before completing this shipment

The next six characters of the tracking number are where the treasure is. This is the sender's UPS account number. The digits after that are almost always unique and change from package to package. There are reports that people who keep detailed logs of tracking numbers have shown that old tracking numbers are sometimes recycled.

So, you may be asking yourself, "what good does this do for the average person?" The truth is that the average person can set up a UPS account on the web with a credit card and be "in business" immediately, as far as UPS is concerned. A malicious hacker could easily use stolen or maybe even fake credit card numbers, fake addresses, and various other fake information to set up an account. This would get them nowhere unless they want to hit that fake or stolen credit card with various UPS charges, right? Wrong!

Here is how nowhere can turn into somewhere for someone determined to steal services. Once you have someone else's UPS account number, you are only one step away from using that account number for your own shipments.

All you need to use someone else's UPS account number is the account number and the billing zip code for that account number. When shipping a package, you simply use the pull down box that says, "Bill Shipping Charges to:" to choose "Bill The Receiver" or "Bill Another Third Party"

How you get their zip code is ultimately up to you. You could try the one on their return address (go check the package you originally got the tracking number from) or you could browse their web site. If you want to test your super elite social engineering skills, you can call the target company and ask for their accounts receivable contact and get the zip code from them. UPS has also been known to hand out this information to a corporate employee "working off site at a client" with a need to ship a package late in the afternoon in an emergency situation.

My moral compass and alarm are buzzing, so let's get one thing straight. It's stealing to do what I have just described. However, if bringing this vulnerability to light causes UPS to change their system or implement some controls to limit this vulnerability, then this article will serve its purpose. It will hopefully bring better security procedures into play for people like me who use UPS all the time. I realize that my account number is out there for everyone to see every time I ship a package. I would welcome the change!

While I do not condone stealing service this way, I have actually had legitimate need to make use of this exploit when a customer tells me to ship to them on their account. It comes in handy when they fail to tell me their account number or appropriate zip code.

This vulnerability seems to work for Canadian accounts as well, but I have not had the need to fully document it yet. I have no idea whether it will work in other geographical locations.

### Insurance Scamming

This is where I am most worried that someone will come along and scam UPS out of their hard-earned cash. It is also where I see their largest vulnerability, so it is worth sharing.

In my personal and documented experience, UPS will lose approximately one out of every two envelope-sized packages. In other words, if you take a letter-sized envelope, stick a note or hand drawn picture inside of it and slap a shipping label on it, there is a 50% chance of it disappearing in transit.

$100 of insurance coverage is free, and you can doctor up an invoice for the "product" they lost. Call it a Dufu cleaner or whatever. When they lose it, you are due $100 plus a refund of your shipping costs, and they almost always pay it.

Be creative here and think with me. Insure it for a few thousand dollars and the game changes–for you more than for UPS. If they lose it, they pay you, presuming you provide that most important invoice. Note that they do not cover specialty items like artwork, which could be the subject of a whole different article, I suppose.

At some point, the UPS system probably handles high value packages differently (can you picture hand carried, guard monitored packages?), so if you are an idiot and thinking of stealing from UPS via this vulnerability, expect that the $50,000 insured envelopes you send out, fifty at a time, will all be delivered perfectly.

A final small tip for this exploit: UPS allows you to interrupt the delivery process for a package and have it re-routed. I suppose if you shipped from southern California to northern Maine and then on day three asked that it be sent back to California, you could greatly increase the chances of the package disappearing.

### Packaging Tips and Thoughts

UPS is about as evil as they get when it comes to damaged items and paying claims to their customers. You can do exactly what they tell you as far as packaging goes, and yet they will almost always claim that the box was not brand new, the padding was insufficient, the tape you used was too old, etc. It's probably standard procedure for them to deny a claim before they pay it in the case of merchandise damage.

My advice to all shippers is to overpack your items. When you think it's packaged well enough, go one step further. Take photos of the packaging process, including the box rating.

[redacted]

Anything you can provide to prove that you took care of documenting your process BEFORE they damaged the goods will work in your favor tremendously. To try to clear it up and provide proof later shows that you are not at their level of "damaged package negotiation" ninja fighting and the representative will write you off as a UPS newbie.

The bottom line is that if they damage it, give them hell until you are either out of hope and strength or win your case. They won't hesitate to bleed you dry emotionally while trying to squirm out of paying for the damaged merchandise. Provide them with an overabundance of proof and documentation. Be prepared to appeal their decision at least once.

Another quick tip is to always track your packages. They are often delivered late due to one reason or another. If it is not weather related, and you are not shipping during the Christmas holiday season (and a few other random and unexpected reasons), then you get a full refund of your shipping costs if it shows up late. Insurance costs are not refundable in these circumstances. I always put my initial claim in via the UPS e-mail interface found at `https://www.ups.com/upsemail/➥input?loc=en_US&reqID=WSP`. I do this because, if I ever really have a big mess to clean up with them, there is an electronic record of what I sent.

### Random Thoughts and a Great Tip for Travelers

#### What I Dream About

Sometimes I wonder what would happen if I stuck the same exact shipping label on ten different packages and sent them all off on their merry way to some destination. My guess is that, because the scanning of the label triggers the billing, I would get billed for a single package transit and delivery. However, if they were spread out over a few days so that the delivery of package #1 happened before the pick-up of package #2, then I assume I would be billed for the same package more than once. This could lead to some very interesting discussions with the UPS service representative who receives my e-mail or phone call a few days later asking about duplicate billings. Hypothetically, of course.

A great tip for travelers is to print up a dozen or so shipping labels to you, from you, with a one pound weight designation. That way, if you buy something that you really don't want to carry home on that plane, in that car, or on that motorcycle, you can slap that label on a properly re-packaged box, hand it to the UPS driver or drop off location of your choice, and wait for it to show up at your home or office. There is no need to carry that chrome plated machete on the airplane back from Los Angeles or that vase back from Graceland. Just plop it in the box and packaging of your choice, slap the label on, and pray UPS doesn't lose or damage it in transit! Make sure to insure each and every package for $100 (free), or more if you think you may buy some high value items.

I always wonder if the stuff that I ship crushes other people's holiday gifts or merchandise. I mean, if they can't figure out how to back bill me for a 70 pound box that has a one pound label on it, can they figure out that it needs to be at the bottom of the pile?

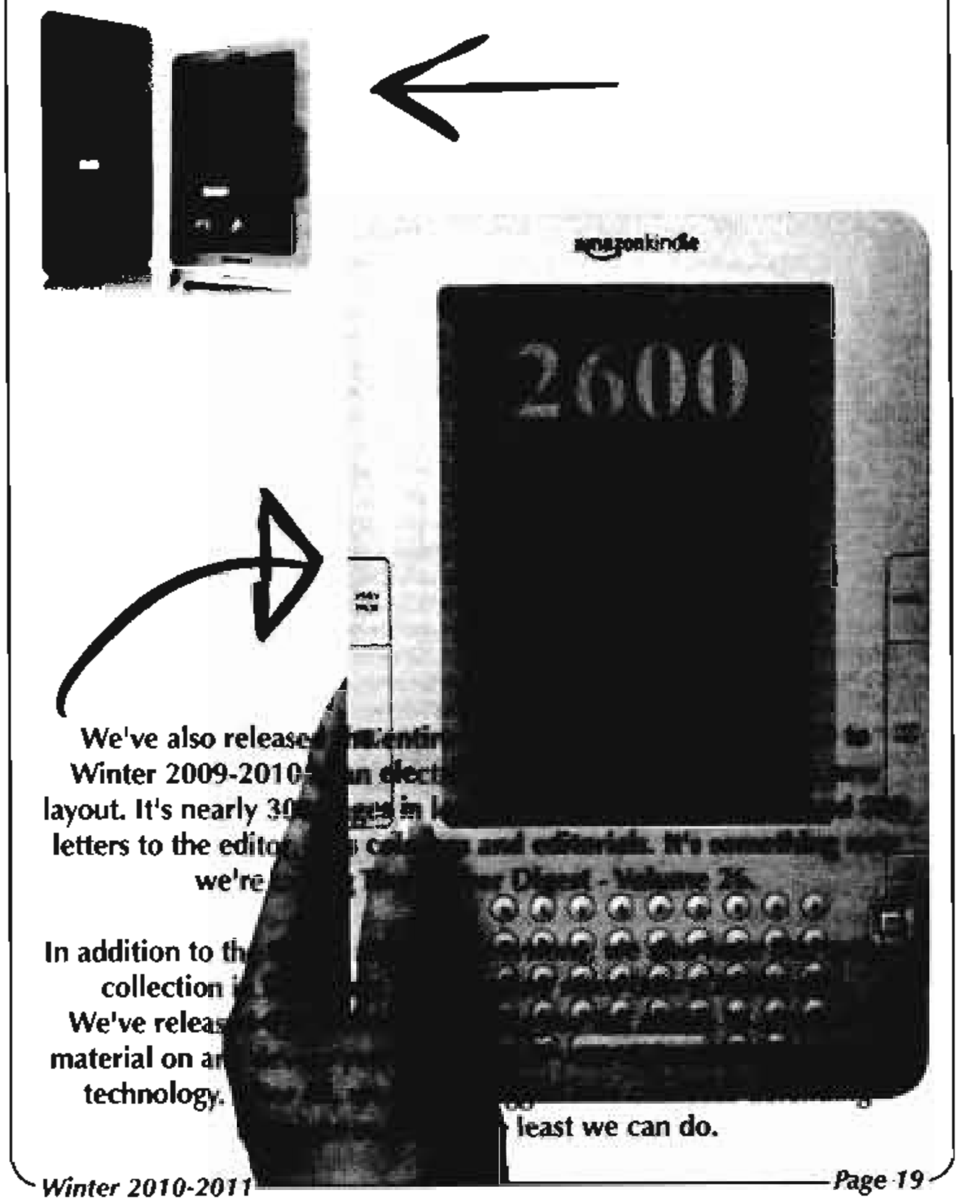
#### Random Observation

I've shipped to and from every state except Hawaii. UPS rules the NYC area and most of the Northeast. They probably rule most of the Chicago area (auto country) and a good part of Canada near that area. It seems that FedEx rules a good part of the rest of the country, including the far west, and DHL is the king of international shipping.

I hope this article is useful for you. Please don't be an idiot or a thief. I'll say it again, "Keep hacking. Keep it moral. Teach others. Become a leader of the Ignorant, not their enemy."

## Did you know there's an electronic version of this issue for the Kindle, the Nook, and various other e-readers? Well, there is.

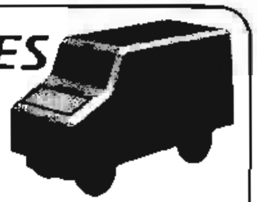
**Just visit our web page at www.2600.com to find the right link to the version you're looking for. And please write to us at ezine@2600.com with your suggestions and feedback.**



**We've also released an entir**
**Winter 2009-2010 an elect**
**layout. It's nearly 30 pages in l**
**letters to the edito s columns and editorials. It's something**
**we're Digest - Volume 26.**

**In addition to th**
**collection**
**We've releas**
**material on a**
**technology.**
**least we can do.**

# ODE TO THE UNITED STATES POSTAL SERVICE, PRIVACY, AND BUREAUCRACY



**by Barrett Brown**

The United States Postal Service (USPS) is a model government service that has sadly been losing the battle against modern times. One of my favorite services that the USPS offers in any city in America is a service called "General Delivery." This is rather like the old fashioned version of `dodgeit.com`, `mailinator.com`, and other one-way e-mail services. The way it works is that you address a letter to whichever name you want and mail it to General Delivery, Any City, Any State. There is generally one post office in each city responsible for General Delivery mail; in San Francisco, the physical address is 101 Hyde Street, San Francisco, California, 94102. So if any of you put some money in an envelope and mail it to Barrett Brown, General Delivery, San Francisco, California, I can then go to 101 Hyde Street, present my ID at the window (this is the only anonymity problem, although since most General Delivery postal workers look at IDs all day long, a good looking fake ID could be used fairly easily, as there is never a magnetic stripe check or anything like that) and pick up my free money. If you think about it, there are many interesting ways that one could use this service. Say you are going on vacation to New York and you don't want to carry something on the plane. You could mail it to yourself c/o General Delivery, New York, New York. I'll let you use your own imagination for further uses. And before you ask, yes, reasonably sized packages are acceptable too.

Now, I'm not the only "Barrett Brown" in the world, so one of my other namesakes (or someone with a fake ID) could pick up my mail or I could get their mail, unless a middle name or initial was used. Like I said, this is a legacy service of the USPS, in all probability left over from the days when everyone in town picked up their mail this way. But some security lies in the fact that there is no way to find out if someone has anything waiting at General Delivery without being told by the sender or showing up at the post office.

I discovered this service several years ago when I was homeless, and I was thrilled. Not just because I had found a way to get mail, but because I had finally found a way to maintain some database anonymity for free! As anyone who does some basic privacy research can find, there are anonymous re-mailer services and anonymous addresses in the Cayman Islands that will forward your mail to you and keep your identity secret, but usually for a hefty fee.

Now I had finally found a dead-end address, an address I could forward all my mail to, an address I could put on my bank account, an address I could put on my driver's license, and no one could use it to track me down and show up at my door! No, not "General Delivery," but "101 Hyde Street," the Physical address of the post office. I did an experiment where I sent a letter to: Barrett Brown, 101 Hyde Street, San Francisco, CA. Then I went to the General Delivery window and, sure enough, I got my letter just the same as if I'd written "General Delivery" instead of the address.

So, quicker than you could say "up yours debt collectors," I put in a request to forward all of my mail there. Next, I went to the DMV to get a new driver's license because I'd "changed my address," and six weeks later I picked it up with my post office address beautifully embossed on it, just like I lived there. Next step was the bank. I hadn't had an account in some time (having been put on ChexSystems for seven years when I was quite young for some "accidental incidents") but my purgatory was up and I was again allowed to open an account. All my paperwork seemed to be in order, but "uh oh!" It seems the bank's computer was smarter than the New Accounts Manger because it said I could not use "101 Hyde" as a valid address, though it thankfully didn't say why. Hmmm, what could I do? I ended up giving them the address of a homeless shelter as my home address, which they accepted, and then "101 Hyde" as my mailing address and that worked out just fine, but I was still worried they might send something to the shelter to check up on me. This was a job for online banking! I logged in to my new account and went to my profile information to change my address. Both my addresses were listed and I simply deleted the homeless shelter, leaving "101 Hyde" as my only address; no problem. I ordered some checks, and two weeks later I was picking them up at the General Delivery window, laughing with joy when I saw the post office as the address on my official checks.

I did some database checking, searching for myself, and sure enough all roads pointed to "101 Hyde." It was a success: everyone had lost my electronic trail. I was happy and proud that I had once again outwitted "The Man." There would be no way to find me unless they put a full surveillance team to watch the post office for a month, and even then it would used by so many people and there were so many disguises I could use. But sadly, this is not the end of my story...

A few years went by and I got tired of going to the General Delivery window every month to pick up my mail, anonymous or not. Especially on the 1st and the 15th of the month the lines can be very long because of all the homeless people who really need to get their mail there. So I filled out a USPS "Change of Address" form to forward my mail from 101 Hyde to my new, swanky apartment. My form came back refused. It seems you aren't allowed to change an address, even for an individual, from 101 Hyde street, because it's filed under some special heading. This again called for the Internet! I went to `www.usps.com` (yes, the United States Postal Service has a .com these days, though it used to be .gov) and tried an online Change of Address but, again, it returned with the error that 101 Hyde was a business address and could not be changed for an individual. A business address? Hmmm... So I filled out the form again, specifying that the Change of Address was for a business; a business named "Barrett Brown." I do business, so I don't think this was fraud. The page charged me $1 and sent me a confirmation. It had worked! What paper would not do, the online form (and money) did!

I waited expectantly for mail to come flooding into my new, swanky apartment, but nothing ever came. I went back to the General Delivery window, showing my ID as usual, and picked up my mail. It hadn't worked after all. The USPS web page had just robbed me of a buck. But as I was picking up my mail, I noticed a new sign taped to the inside of the post office General Delivery window. In fat, black marker it said, "No mail to '101 Hyde Street' accepted. Must be sent to 'General Delivery.' Also, no IDs or checks accepted." Oh no! My first thought was deep sorrow for all the homeless people who didn't have any ID, or any friends whose addresses they could use. What were they supposed to do now? It's legal in California, in these post-9/11 days of terror, for a police officer to take you to jail for not having ID in order to establish your identity and make sure that you're not wanted. I knew of some officers who took away street people's IDs just so they could take them to jail and keep taking them for the six weeks it takes to get an ID from the DMV. This was bad news indeed. San Francisco's war against the poor just keeps getting worse. My second thought was that I would have to keep coming back to the post office month after month for the foreseeable future, but that it was worth the price of keeping my electronic anonymity. At least for the next seven years, I'd have my checks and ID with the address still on it.

Just recently, I started receiving a few letters electronically forwarded to me from 101 Hyde... none of them addressed to me! Were they going to start forwarding ALL the general delivery mail to me?! I gave the first few back to the postman, showing him that the names were different, but this didn't stop the letters from coming. Finally, I walked some of the letters down to the post office myself, to return them and show them the error. I know from firsthand experience how important a timely letter to General Delivery can be to a homeless person, and I didn't want anyone to miss his or her mail because of me.

At the end of this small experiment, I'm saddened and a little confused. I'm saddened that with both the bank and the post office I could do something online that I could not do in person. This shows how blindly companies and corporations are throwing services and power onto the web, without actually knowing how they work. I'm saddened that for $1, and in the interest of "business," I could get the post office to do something that they wouldn't do for an individual for free. Most of all, I'm confused and saddened that someone would remove the ability for a person to get an ID at General Delivery. This is a policy that clearly only hurts the homeless and those with few resources and, for this reason, it's a policy that will probably not be fought by anyone or even noticed.

The only good news I can end with is that, to date, despite the sign that has been posted for four months saying I cannot receive mail addressed to 101 Hyde, I still do on a regular basis. As every good hacker knows, believe none of what you read and only some of what you see.

# Android You Broke My Heart

**by RyOki**

It wasn't Christmas or Arbitrary Day, but there was my new toy impeccably wrapped and waiting: my new Android cell phone! I was so excited and I carefully peeled back the packing and wrapping layers. My fingers tingled with delight to reveal my new HTC Magic. It was gleaming white with sharp graphics and the promise of storing my life in it; my more organized and productive life. I was able to get over the initial fumbling with the OS and the touch screen over a few weeks and I began using my new phone. I filled it with contact information like emails, phone numbers, photos, and I transitioned all my contacts from my old phone to the new super shiny one.

### Introduction

My big troubles with the operating system on my phone began during a job interview, one with the potential for a lot of money, I might add. The interviewer was horrible, so I wasn't really expecting a call back for the job. Although for the money, I might have worked there anyway. I'm in IT. I sold my soul years ago, but I digress.

I discovered the hard way that my phone had been automatically routing all calls to my voice mail, while at the same time shutting off the notifications for new voice mails or missed calls. Maybe it started a couple of days after the interview, but the issue wasn't identified until two weeks after the interview. It must have been a new unannounced feature called "Silence," offering peace of mind by never allowing my phone to ring. To add to the complexity of my issue, my cell phone provider automatically erases unsaved voice mail messages after three days.

I searched through what I thought was everywhere in the phone to re-enable notification of incoming calls, but I couldn't find any setting. So I turned to the Internet. I figured, "Google, I bought your phone; feed me baby." I must mention that under duress, I didn't check with my spouse. But that's another story.

### My Heart Crumbling

Within 30 minutes I found two Android forum posts with similar issues. One said do a hard reset. The other said to install a shortcut program called Any Cut and to re-run the initial phone setup. I chose the "run setup again" route as a couple of people posted that even after the hard reset, the problem came back. The Any Cut solution post said the issue was due to a corrupt configuration file that could only be corrected if you have root or re-ran setup. I didn't have root level access so I re-ran setup. This is where things began to get a little strange.

I went through the setup again, but made a fatal mistake! I entered the wrong password for my Gmail account once. Once, only one little itsy bitsy, teenie weenie problem, I got the Android version of the blue screen of death, "Waiting for Sync. Your email will appear shortly."

Everything with the Android OS is based on your Gmail credentials. You don't need a SIM card for the phone to work, but you must have a Gmail account. Funny thing though... if you run setup again and you enter the wrong credential, you are locked out of a great majority of features on the phone. The only fix per Google; hard reset. Really? Enter your credentials wrong just once and you have to wipe the phone?

### What Worked and Didn't After Invalid Credentials Presented

My contacts were gone. No contacts listed. I was left with a barren message: "You don't have any contacts to display. Go to your menu and Edit Sync Group." I suddenly felt very lonely. My entire call log was fully available, just no names associated with the phone numbers. As I never cleared out my log, all numbers incoming or outgoing were listed with dates, time, call length, call status of missed calls if applicable, and call direction. I guess root has the contacts properties but any user has the call log. No phone numbers were stored on my SIM by default with Android. There is no menu item to force save your contacts to the SIM. The only SIM contacts the Android OS phone was willing to import from my SIM were the cell provider's default contacts.

I am not one to memorize random numbers. I theorize the human brain has a maximum of short and long term memory and there is no use adding useless information. Hence, some contact details I didn't memorize. I went to check if my SMS messages were available, theorizing they may be because I could see my call log. I thought maybe I could rebuild my contact list a little based on the content of the messages.

All of my SMS messages were available but with no names associated with them. I had never cleared my SMS log, so all messages incoming and outgoing were retained and available from the inception of the phone service. My meet up greet up, lovely, or angry, sexy time related flipping SMS messages to said spouse or others were still available. Everything! Frack man.

I could receive Google Talk chats inbound via my regular Gmail account name and could respond only to those Google Talk messages. Yet, I was not logged onto the phone with valid credentials.

I tried the built in Chrome browser. My heart sunk. When I opened my browser, it took me directly to my domain Google mobile page. I could not access my applications like email unless I put in my business domain credentials, luckily. Could this mean that no matter if you are logged into the phone with valid credentials or not, the former person's home page, browsing history (yes, complete from the last time I dumped my cache), and possible credentials for services are still retained somewhere on the phone? That is already a great deal of information about a person to be essentially accessible by anyone logged into the phone or not.

The Android Market was fully accessible. At that point I should have been logged out of the Android Market. I hadn't bought an application. This would allow access to the Google pay system associated with my <same username>@google.com regardless if I were logged in as <same username>@google.com or not. Per the Android release notes for 1.6, access to the market should be restricted if you're not logged into the phone with a valid Gmail account. This would make sense, as this allows full access to the pay system. I guess the release notes need some correcting. The reason the market was accessible is due to one or more of my applications already in the notification bar requiring updates. Going directly from the notifications bar, I could access the market, update my software, and download any software. This appears to override the need for credentials.

About a week went by and I woke up one morning to my phone not really working OS-wise. The Android Market wouldn't let me in and the phone now wanted me to log into Gmail. I used my trusty Any Cut, and I ran the setup wizard again. I tried my credentials again and got the same message: "waiting for sync: this may take up to 5 minutes."

### A Different Tactic

I decided to create another Gmail account. This time it was <same user name>1@gmail.com. I logged into the phone OS and the built-in browser showed via Google search that I was logged in as <same user name>1@gmail.com. I could use the Android Market again. I was happy at this point, until I got an incoming Google Chat from my spouse. I had created the new account not more than 15 minutes prior to the incoming chat so no one knew about it yet. I answered back, "What Gmail account did you send this to?" The response, "<same user name>@gmail.com - the only account I know about."

I was, at this point, logged into the phone but as <same user name>1@gmail.com. I had full access to my <same user name>@gmail.com chats and could talk back and forth with my Gmail chat contacts logged in as someone else. My Chrome home page took me to my <same user name>@gmail.com Google application home page. If I went to a Google search via the built-in browser at the bottom of the page, it showed I was logged in as <same user name>1@gmail.com. No contacts listed still, but my entire call log was available All browsing history since the last dump remained. I could not use the built-in Gmail application, but I could use the Chrome browser to navigate to both email accounts.

### All Was Never What It Seemed

My spouse, a "you should have asked me - I am a master programmer and can fix almost anything," was right. I handed my phone over because it was still unable to receive incoming phone calls. Little did I know this setting is in the "main settings," "call settings," "GSM call settings," "additional GSM only call settings," "call forwarding," then finally "always forward" with my international voice mail phone number built in by default. Otherwise known as an infinite loop of insanity.

### Conclusion

You don't need root, you don't really need to "hack" anything. On any 1.6 (probably beyond too) version of an Android OS cell phone, force a re-run of setup, enter the wrong credentials on purpose, and you have sweet access to the previous settings and plenty of private information to keep you naughty. I have heard the claim "well, not in newer versions." Then I suggest Google force their manufacturers to maintain the OS. If the issue isn't fixed, consumers with version 1.6 are stuck with a huge gaping security hole. "New" Android Tablet PCs are shipped with the 1.6 version to unsuspecting users. All information stored on an insecure phone OS is fair game, including your contact information. I agreed to the terms and conditions, but my contacts weren't given that option.

My journey ends here. An affair with a phone OS that broke my heart, and is willing to leak my data to anyone.

**by Azazel**

I will preface this by saying a few things. First is the usual legal disclaimer: This information is for educational purposes only. What you do with it is your business and I'm not responsible for your actions. Second, the thing I like most about this is that, for the most part, you won't have to talk to a live person to gather tons of useful information. Notice I say "for the most part." Inevitably, depending on how much information you need, at some point you will need to flex those skills.

The methods presented here will work best against a large corporate office building, such as an investment firm or research facility. They can also work against smaller offices, such as real estate brokerages or banks, but I've seen higher success rates with larger firms. Our goal is to gather as much contact information and personal data about as many employees as possible. Essentially, we're going to try to create a dossier on every important person in the company.

Start by going to the company's website. If they have more than one location, find the local phone number for the building you're interested in (not an 800 number). Now and then a company may not publish this information on their site, giving just the phone number for the central location or a toll-free number. Lucky for us, Google has a big mouth and, if that fails, call the number they give and just ask for the local phone number to the building you want. They will probably give it to you.

Sometimes, the main phone number will end in 00 or 000, e.g. 212-555-1000. Usually, if the company is large enough, they'll lease a sizable chunk of the block of line numbers (the last four digits). Before the next time-consuming step, save yourself a little time and look around the website for personnel with their direct numbers or extensions listed. If someone has extension 455, most likely their direct line is 212-555-1455, because of the way direct inward dialing works. Be prepared to spend quite a bit of time on the next step. Wait until after hours. I'd wait until after 10pm, in case people are at the office late. Then call each number in that block until you're no longer calling numbers within the company. Most numbers will have a voicemail

at the other end with the respective employee's name and possibly position in the company. Some numbers may be fax machines or something else, so just keep a note of them. Be creative or old school. Use an autodialer program or write one yourself. Keep in mind, if the company does not use this system you may end up annoying some hapless civilians late at night. So be ready for that.

By the end of the night you should have a list of most of the employees and officers in the company and their direct lines. But don't stop there, our dossier is just getting started. The previous section demonstrated how customer service and the way a company strives to present itself to customers may present a security vulnerability. This section will show how the way individuals present themselves to the world, to their friends, to media, and whomever else may prove to be detrimental to their own personal privacy. Do a Google search on all the names. Things to look for include Myspace and Facebook pages, news or industry articles written about them, bios which may indicate the town they live in or other pertinent information, papers written by them, professional resumes, the college and high school they went to (you can gauge how old they are by graduation dates, too), volunteer organizations they work for, and other business ventures. You may be surprised at how much information you can find. You should also look for an email address, if you couldn't find one on the company website. There is usually a formula for a company's email addresses though. If you find one person's email address, it is easy to deduce the formula for the rest of them. For instance, if you find jsmith@hackerzinc.com, you'll usually be safe in assuming the rest of the email addresses will be first initial and last name at hackerzinc.com.

Next, head over to whitepages.com and look up each name. Remember, not everyone lives in the same town where they work, especially in large, well-paying corporations. Hopefully, your previous searches turned up some indication of at least the town they live in. If not, no worries, here's a simple way to narrow it down. Look at a map of the region. Take New York City as an example. Find the white pages listings for NYC, then start branching out from there. For instance many people commute to NYC from North Jersey, White Plains, Long Island, and Connecticut. Use common sense; if you're looking up the CEO of a top investment firm and you turn up an address in the projects, it's probably not him. If you get more than one instance of a name, you'll have to call and do some social engineering. Calling a home phone number asking something as simple as, "Can I speak to John Smith of Hackerz, Inc?" usually works well because you'll at least get some indication on whether or not it's the right John Smith. The worst thing you can do is inadvertently target the wrong person due to a mix-up with names. So now you can match each person with a home phone number and address.

The next and final step in this article is the social step. This is just one example of social engineering that has worked for me. Everyone is different, so fine tune this for your own personality or to get other information. If you sound like you're 12 years old, this specific method may not work for you. Around 5pm, call the subject's home phone number. Hopefully their spouse will answer. Ask for your subject (hopefully he's not home yet). Their spouse will (hopefully) inform you that he or she is not there. Explain that you were supposed to call him or her about something important regarding work, but you just missed him or her at the office. Further, you're very upset because your boss is leaving at 5:30 and needs the information NOW! The sympathetic spouse (all sexism aside, this usually works better on women) will hopefully then offer your subject's cell phone number.

In the end, you should have a bare minimum of name, direct work phone number, home phone number, home address, and maybe cell phone number for most of the employees of the company. Hopefully you had some good luck with your searches and got much more information as well. This article should have given you some insight on how much research often goes into a well-planned attack and how, if the attacker is good, you won't even know you're being targeted until it's too late. So much information is readily available on the Internet these days and people ARE looking at it. This should also act as a warning: no matter how impenetrable your network is, or how well you and your coworkers have been trained against social engineering, finding alternative methods of gathering data is all too easy in the information age. Be careful what you put out in public and be careful next time you consider giving out seemingly innocent information to a spouse's desperate coworker. It's also a good idea to do searches on yourself from time to time so that you know what information anyone else could have about you. Have fun.

# The Hacker Perspective

## *by John W5EME*

I'm not sure I qualify for the word "hacker" anymore. I'm pushing 70, now, and although I read and enjoy *2600* any time I see it at Barnes and Noble, I hardly ever see anything I would rush out and try. My hacking days started at about age nine or ten, right after World War II. I was interested in anything electrical or mechanical, and I left a trail of disassembled clocks, toys, and other interesting things wherever I was. I smashed mercury batteries with a hammer (state of the art, back then) to collect the tiny droplets of mercury. With pliers, I twisted the lead nose of a bullet out, to get the smidgen of gunpowder inside. Back then, you could go to any chemical supply house and purchase any chemicals you wanted if you had the cash. I once bought a canister of ether to see how much it took to put neighborhood animals to sleep. Yes, the clerk sold a little kid a canister of ether. Those were simpler, more trusting times. I bought gallons of nitric and sulfuric acid to see what they would attack and how long it took. One thing that caught my eye was the fact that nitric acid really attacked copper pennies: first it cleaned them up and made them a reddish color, then it would start eating away at the copper. If you let them soak awhile, they would actually reduce in size down to the approximate size of a silver dime. A light flashed inside my head... for months, I had been rubbing silver coins with mercury to make them bright. The mercury coating made them slippery, too, just like they were greased. Could a coating of mercury be rubbed on the acid-treated pennies to make them look like dimes? The answer was yes, much to my delight. I made a pocketful of "dimes" and proceeded to see if they would pass scrutiny with clerks at stores. Usually, they did. I also found they worked well in many coin-operated machines. Back then, you got three three-cent stamps and a penny change for a dime in a coin-operated postage machine. I could get three-cent stamps and a penny back for one of my trick pennies - *pure* profit. The city buses collected fares in an elaborate gadget in which you dropped your 15-cent fare into a slot and it then fell onto a little platform. The bus driver looked through a little window to make sure you had put in the right amount, flushed them into his coin box, made change if necessary, and you found a seat. Two of my shiny, almost right-sized pennies fooled every bus driver I ever tried it on into thinking I had inserted two dimes, and gave me a nickel change! Coke machines accepted the fake dimes, gave me a nickel Coke, and a nickel change. For weeks, I was the richest kid in school. I even sold my fake dimes to my friends for a nickel, and we both walked away happy. Then, one of my friends had a bad experience at a store when he tried to buy a bicycle. This terrified me so much I got out of the fake dime business for good.

I was delighted when I discovered the rotary dial telephones of the day dialed by the very short interruptions to the line which the old rotary dials produced. Dial a three, and the line got interrupted three times. I badly wanted a lineman's handset, but of course had no way to obtain one. I took an old handset, hooked up the earphone, carbon mike, and a normally-closed push button in series and stuffed all that back in the plastic handset shell with a cord equipped with alligator clips. Presto - lineman's handset. You clipped on a live telephone pair, got a dial tone, then dialed your number by mashing that push button switch, quickly, the number of times needed for that digit, then doing the rest of the number the same way. It took some practice, but I got very good at it. Upon reflection today, I think the reason I was so successful in dialing with a push button was that the timing specifications had to be so relaxed to cope with variations in the speed the old rotary dials returned when you dialed a number and let loose of the dial. The line interruptions occurred on the return stroke and some dials were much faster than others.

Our telephone company in those days had climbing pegs on nearly every pole. I guess the age of litigation had not yet arrived and companies didn't have Safety Managers to take the fun out of everything. It was not unusual for me to climb a pole, open the unlocked box at the top, and hunt around for a dial tone with my alligator clips. I learned quickly, though, to respect the ringing voltage that was sent over the pair to ring the bell on an incoming call. Later, I read somewhere it was about 100 volts AC, at 20 cycles per second, generated at the central office by a big motor-generator set. Never got blown off a pole, although I got the peewilly knocked out of me a few times by that big central office generator.

One wonderful hack we learned (we didn't know the word "hack" back then) was that on the payphones, you got a dial tone and could dial out when any part of the microphone circuit was grounded momentarily. I soldered an alligator clip on one end of about a foot of stranded wire, and a safety pin on the other. If you clipped the alligator clip on the finger stop of the rotary dial, you had your ground. Then you poked the sharp end of the safety pin through a hole in the handset, right over the carbon mike. You had to penetrate a little rubber cover (probably there to keep spittle out of the mike) and probe around. Soon your grounded pin would contact the mike circuit, and you would hear a beautiful dial tone. Put away your clip, wire, and probe, and make your free call. Soon I learned exactly where to probe the mike to make contact quickly, and the elapsed time to get a free dial tone was just a few seconds, with no damage to the equipment. A lesson learned the hard way was to be sure to close the safety pin before putting your little jumper cable in your pocket. You didn't forget again.

Later, in high school, being interested in electronics (ham radio operator, etc.), I realized that the hearing aids of the day were very high-gain amplifiers with a mike. My paternal grandmother had one. She was a wonderful old lady, and let me examine hers once. I discovered that there were three subminiature tubes in there, and a big 30V "B" battery, as well as a mercury cell which was the filament supply. My grandmother told me she had to replace the filament battery at least daily, but the "B" battery lasted at least two weeks. The mike was in the big box with the tubes and batteries, and you put it in a pocket with the earphone wire stretching up to your ear. Most users tried to conceal the earphone wire by running it cleverly inside clothing, but I could spot a wire a mile away.

Naturally, after seeing inside the hearing aid that one time, I decided I was an expert. Also, I wanted a couple for myself to experiment with. So after school the next day, I went to every hearing aid store in town, offering my services as an expert hearing aid repairman. Some stores had their own repairman, and some sent the unit back to the factory for repair, but when I hit the Belltone store, I got hired on the spot! It seemed the lady who owned the place was a recent widow and her husband had been the repairman.

She was looking for a new repairman and I happened to drop in at just the right time. She immediately gave me a dozen or so units to fix. She was under time pressure because these hearing aids belonged to customers and she had the policy of loaning out a unit while the customer's was in the shop. She had run out of loaners and was forced to loan out new units! I fixed a few that afternoon (mostly corrosion on the battery contacts and a blown tube or two, as I recall) and she was very pleased. She had a large collection of old units, trade-ins, and junked units which she gave me to take home. She even threw in a few "B" batteries and mercury filament cells of various types. I worked after school every day until all the repairs were cleaned up, then dropped off to a couple of days a week. I fixed up most of the junkers she gave me until I had about 15 or 16 nicely working units.

Like many kids of the day, when I was much younger, I had built several crystal sets. They worked OK, but were not very loud and required a big antenna to work at all. I hooked up a crystal set to the hearing aid mike input, and wow! It was loud in the earphone and a strong station would come in with just a two foot antenna! Perfect for covert listening during boring classes at school! I built a tiny crystal set from a diode and a "loopstick" coil and attached it to the hearing aid. Next day at school, it was a resounding hit. Nobody had ever seen such a small radio, as transistor radios were not yet available. Everyone wanted one. Naturally, I started taking orders, for about $15 each as I recall, and sold out that same day. After filling the orders, I still made money selling batteries for a few weeks until the school officials cracked down and warned students that anyone wearing a "hearing aid" during classes had to bring a note from home.

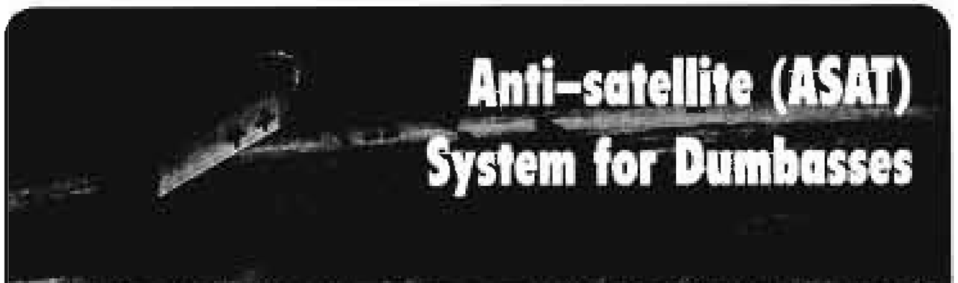
There are probably fewer opportunities today to get into mischief than in the glory days of the 1950s or 1960s, and most likely today would involve computers. I like computers as much as anyone, I guess, and, in fact, built my first one back in 1972 from components, using an Intel 8008 microprocessor with a blazing 50 KHz clock. All software was hand-assembled in the binary machine language of the day. No C++ back then, or even a decent Basic. No mass storage for the average person, unless you had an ASR-33 teletype. The teletype would save data at a whopping 10 CPS speed on paper tape. If you had a decent sized program to load, you inserted the paper tape into the reader, then went out for lunch. When you got back, your program *might* be finished loading. We didn't mess much with online computers back then, but I will admit to playing the game "ADVENT" for hours on a certain Honeywell mainframe computer as an uninvited guest via a 300-baud acoustic modem.

I doubt if you can find a telephone pole today with foot pegs to climb, or find a chemical distributor who would sell a kid nitric acid over the counter, for fear of a lawsuit. But, for those curious folks who are interested in how all things electrical and mechanical work - or can be retasked, there *are* still some fun things to do. Get a subscription to *Make Magazine*. *Make* is full of interesting projects from which you can get ideas. I got my first set of lockpicks from a locksmith years ago, but *Make* sells them for a few bucks if you don't know a locksmith who will order you a set. Look at ordinary everyday things to visualize how they can be hacked into something fun or useful. Here's a simple example: Buy an old or scrapped electric wheelchair at a flea market or tailgate sale. I have seen several for as low as $20. Fix it, then radio remote control it. You can buy a new 2.4 GHz RC transmitter and receiver set today for $100. Imagine the fun as you run your wheelchair down a city street, seemingly out of control, with no one sitting in it. You, of course, are causing it to do wheelies and spinarounds from a concealed location, being careful not to hit anyone (remember the lawsuits). Or build a little handheld programmer for those scrolling signs you see everywhere, plug it into the programming port on the sign, and upload the message of your choice. How about those new billboard-sized displays? Can you imagine one of those monsters showing reruns of *I Love Lucy?* How about hijacking that big video display feed in Times Square during the New Years televised ball-dropping festivities and substituting a "Nuke the Whales!" message. Fun is where you find it!

*John W5EME's early interest in electromechanical devices prepared him well for a long career in electronics and the power generation and distribution industry. He recently retired as a vice president of a high-tech manufacturing company. After retirement, he now has a little time to enjoy his longtime interests in ham radio, robotics, and building microprocessor-based gadgets, with an occasional teaching or consulting gig. Life is good.*

**Hacker Perspective is a column about the true meaning of hacking in the words of our readers. We're interested in stories, opinions, and ideas. We've gotten so many good submissions that we're booked for an entire year! Keep your eyes open for when we'll be accepting submissions again. In the meantime, please send us your articles on specific hacker applications involving any type of technology. If it's interesting, exciting, and detailed, it will show up in our pages.**

**articles@2600.com or**
**2600 articles, pob 99, middle island, ny 11953 usa**



# Anti-satellite (ASAT) System for Dumbasses

by spynuclear@yahoo.com

I have decided to do this as a public service. This is not as fun as a military grade multi-million dollar missile type ASATs but is a workable alternative. As an amateur astronomer, I have had plenty of times where, while trying to lock in on a difficult target with my telescope, a blasted satellite comes into view and spoils my concentration. Since spy satellites can see me, I figured, "why not spoil the view?" They violate my sovereign airspace and so it goes... There are a few high-tech equipment needs for this hack:

- Red and/or green pen-type solid state lasers with fresh batteries.
- Computer controlled GOTO telescope. I use a Meade 12" LX-200 Classic and a Meade ETX-90.
- Starlight night vision scope. Not absolutely required, but it does come in handy for target spotting
- Satellite tracking software. This is used to predict the target orbit and when and where it will come up over the horizon, as well as the orbit path.
- Current and up to date orbital elements of the satellites.

You are going to mount the lasers onto the telescope. The laser beams are bore sighted to where the telescope is pointed. The red laser is used to blank out the infrared (IR) and near infrared cameras. The green laser is a countermeasure against the optical frequencies.

Computer controlled GOTO telescopes have an option to track satellites so that the observer can watch them watching you. You simply select the appropriate bird from the list and proceed with your vast eviltude! It is very important to use up to date orbital elements for proper tracking.

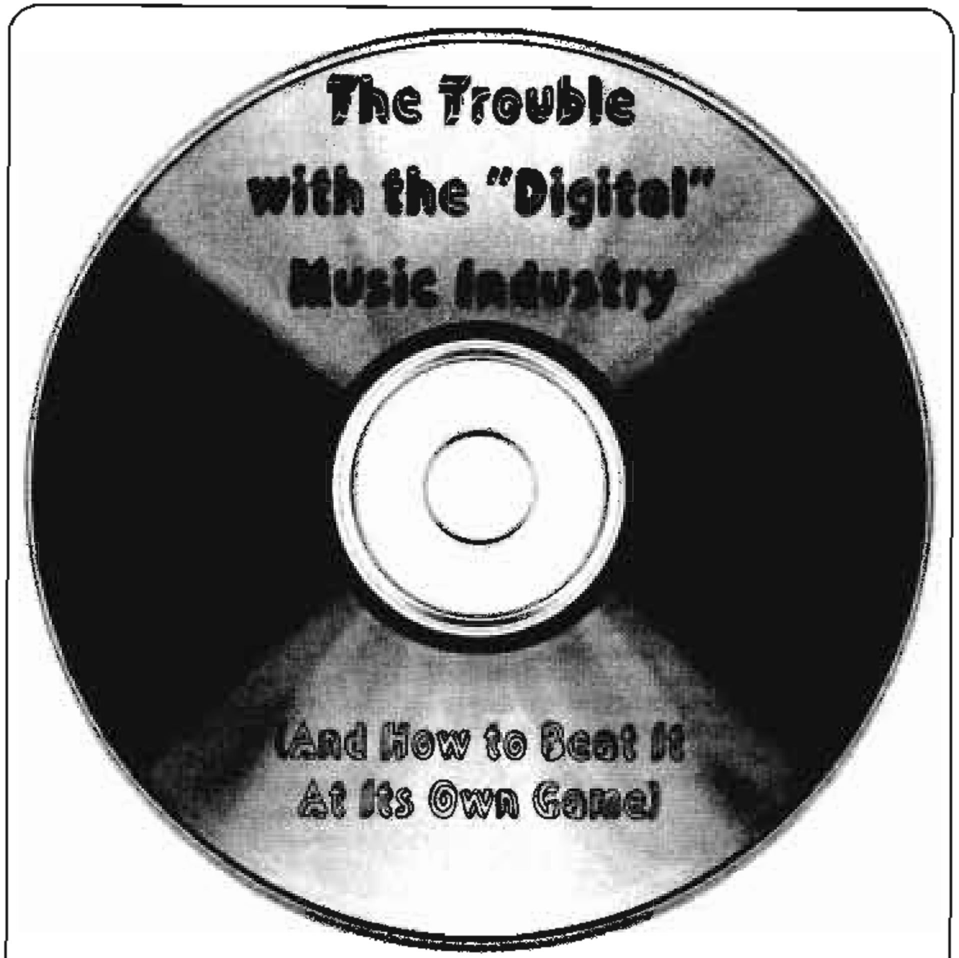
Recon sats can be flying a variety of orbits. The camera birds are usually in low, fast polar orbits that fly over the poles in a north-south or south-north path. These are what we are going after. Electronic ferret birds are in either a geo-synchronous orbit, where they hover over a geographical region, or a Molniya-type orbit, where they move slowly over a target area for a long time before disappearing below the horizon for a short time. Molniya orbits are egg-shaped where the Earth is located at the pointed end. The fat end of the orbit is focused over the target with a long loiter/lag time. This is a great orbit for communications and scanning purposes. These operating characteristics can be useful for picking your "victim." So what if the target is owned by a variety of intel outfits with multi-billion dollar budgets and alphabet soup names such as CIA, NSA, NRO, NGIA, SVR, FSB, GRU, DOD, etc.

The procedure is to lock onto a bird as it comes up over the horizon. The telescope does the target tracking for you and the lasers are used to overload and blank out the cameras on the satellite. Think of this as high-tech geekdom in action! Enough people doing this at random will seem to the sat operators like flying through an enemy territory with very active AAA (flak) and SAM (Surface-to-Air-Missile) defense systems. The laser beams will diverge enough to blanket the cameras as long as you accurately aim at the satellite target.

Another version is to mount a microwave gunnplexer that you can modulate in various modes onto the telescope. This system can be used to mess with the microwave/radar mapping capabilities of the target radar mapper/ferret satellite. Any focused scan of your area on the ground gets overloaded. This is also a GREAT way to attract attention to yourself from the "higher powers." You will need to add some lightweight microwave antenna feedhorns to keep the microwave beam running towards the sat targets. Do NOT expose yourself to the microwave energy, as you would not want to get BBQ'd by your own device.

## References

- Using the Meade ETX: 100 Objects You Can Really See with the Mighty ETX, Mike Weasner
- How to Use a Computerized Telescope, Michael A. Covington
- Weather Satellite Handbook, Ralph Taggart
- ARRL Operating Manual
- ARRL Antenna Handbook
- Observing Earth Satellites, Desmond King-Hele



# The Trouble with the "Digital" Music Industry

## (And How to Beat It At Its Own Game)

**by ScatteredFrog**

The whole "digital" movement irritates me. It's disturbing how CDs and vinyl are endangered while downloadable music is taking off. I like being able to listen to music without having to boot a computer. (Yes, I have an iPod Classic that I'm crazy about, and I guess you can say you don't have to boot a computer to use one, but you do need to boot a computer to get the songs on it in the first place.) And by the way, to those of you who refer to downloadable music as "digital," I have news for you: CDs are digital, too.

For about 13 bucks, you can go into a store and buy an album on CD or vinyl (yes, they still make vinyl), and what do you get? You get a physical medium that contains your music, and you use the appropriate player to listen to it. You get some form of storage with it (e.g. a jewel case or sleeve), and you get artwork, liner notes, and sometimes lyrics or extensive details about how the recording was made. With vinyl records, all those goodies come with a roughly 13" x 13" cover that often is suitable for framing. What really gets me is how the artists get screwed, though. After the sales of vinyl and CDs get divvied up to line the pockets of the record labels' corporate suits, pay for the costs of designing and printing the covers, payola for the radio stations (as a former radio broadcaster, I can assure you that payola is alive and well), etc., there is so little left to pay the artist that the only way most recording artists can earn a decent living is to go out on the road and tour. The only other way the artist can profit is to release the music without the red tape of a label. But unless they do this, the aforementioned 13 bucks of your money doesn't go to those who truly earned it.

For roughly the same price, you can download the same thing on iTunes, Amazon, or other similar online stores – with many catches. First of all, you don't get your music in any tangible form (unless, of course, you burn the music to a CD). You also don't get the liners in any tangible form. But there's one thing that people tend to miss: most, if not all, of this stuff is in MP3 format. Yep, for roughly the same price, you get reduced sound quality. So all those people who think they're keeping up with the times and technology by downloading their music are actually downgrading their music. (And, of course, you gotta wonder how much the artist actually gets from the sale of this product that has virtually no overhead.)

Perhaps one could argue that your average consumer might not be able to tell the difference between a reduced-quality MP3 and an uncompressed source from a CD. Of course, because of bitrate settings, some MP3s can sound better than others: an MP3 encoded at a rate of 128kbps won't sound as crisp as one that's encoded at 192kbps. A friend of mine can identify a song as an MP3 at rates up to 224kbps. I could always tell up to 192kbps, yet most CD ripping programs I've seen inexplicably refer to 128kbps as "CD quality." After listening to the new Beatles reissues in Apple lossless format on my iPod (with studio-quality headphones, not those piece of crap earbuds), I can now tell if it's an MP3 at up to 224kbps. To save space on my iPod, I eventually MP3'ed the new Beatles remasters to said bitrate and now I can even hear that little of a difference.

Many major acts haven't made the leap to iTunes and other online music providers. The only way to hear their music is to actually buy a physical object that you can't download. So anybody who decides to rely solely on downloads for their music will be missing out on some big-time stuff, unless they take the path towards music piracy.

Some of my favorite artists release CDs of previously-released material, but with maybe one or two tracks that have never seen the light of day; either songs that were never released, or new and (presumably) improved mixes of old songs. This is not a new practice, either; it's been going on for decades. Nevertheless, sometimes it's upsetting to have to buy an entire album just to hear one new song. Often, even the download route isn't an option, because you may have to download the entire album to hear the one song! One solution is to check the public library to see if they have the CD, and just check out the CD and rip the track. But what if they don't?

This is where Amazon came in for me. I found a redemption code for Amazon good for $3 in music downloads. There happened to be three songs that I wanted, and in each case it was one of those "buy the whole album to hear one new song" situations. Fortunately, Amazon gave me the option to download these songs individually. Unfortunately, I hadn't used the code properly (let this be a lesson: always read and follow the instructions to the letter!), so the MP3s ended up not being free.

Before I had a chance to remove them from my shopping cart – in fact, there is no shopping cart for MP3s on Amazon – they transferred to my computer, meaning I would be charged for the songs. Oh, well. Lesson learned for only $2.98, no big deal. I still had the code for $3 in free tunes, so I used it to get three other songs.

The next day, I got an e-mail from Amazon saying that my order had been canceled because there was no valid form of payment attached to my Amazon account. (Mind you, this was a day after the MP3s had already transferred to my computer.) Indeed, my Amazon Visa card had been recently stolen and I had to cancel it. I hadn't used Amazon since getting the replacement, and I forgot to update my account with my new card number.

Basically, I got free MP3s from Amazon simply because of an invalid credit card! This could be a boon to music pirates, but a big loss in profit for Amazon. All you'd need to do is make sure your Amazon account has nothing but an invalid credit card number on file, and you're home free.

I don't know if it was the Catholic guilt in me, or if it was that I didn't want to risk eventually being found out, but I confessed to Amazon's customer service, mentioning that I had updated my credit card info so that they could charge me for the amount on the invoice. What really floored me was the e-mail I got in response. In a nutshell, the e-mail said that they couldn't charge the card because it wasn't attached to the invoice! Wow. Whether or not this incident of unintentional free music was enough for the folks at Amazon to rework their MP3 payment system is too early to tell.

While many writers like to put disclaimers in the beginning of the article, I'd rather put mine here as a recap. The purpose of this article is not to encourage anybody to steal, but rather to vent about some of the problems with downloadable music. It was not my intention to rip off Amazon, but I admit I was proud to have exposed a flaw in the system. All someone has to do to get free MP3s from Amazon is to use a canceled or expired credit card number. And who gets hurt in the end, really?

The artist.

# INVISIBLE ASCII: USING AN ASCII GLITCH TO CREATE A POOR PERSON'S STEGANOGRAPHY

**by Strawberry Akhenaten**

I'm not a computer expert. I'm not even a programmer. The most I can do is debug and compile Pascal. I like to play with codes and ciphers, especially the classic pen-and-paper ciphers. I also like to use retro computers. Sometimes I create ASCII art in MS-DOS. This article is a report of a discovery I made while making a "palette" for ASCII art and to describe the encryption I created as a result. I call my ciphers "DEC-160" and "Pseudo-Unary."

### Background information: ASCII

As you already know, computers can work with letters, numbers and other symbols. PCs in particular can type everything a typewriter can, and more, because of ASCII (American Standard Code for International Interchange). This is like an "alphabet" for the PC. ASCII also makes it possible to type symbols that are not on the keyboard, such as programming symbols and foreign characters. This is done with the ALT + command. The ASCII Character Code chart is not hard to find. It can be found in many computer manuals or on the Internet. I myself use this chart to type in foreign languages, because it will let me use accent marks without having to learn different keyboard layouts. Typically, the ASCII code chart shows three things: IBM characters, DEC code, and HEX code. My "stupid keyboard trick" is done with DEC code. (Note: This trick doesn't work very well with laptops. It should be done on a desktop. I suspect this is because of the fact that a desktop's keyboard is an external device. Perhaps, ALT + will work on a laptop with an attached keyboard or keypad. I'm not sure.)

This is where it gets weird: when I made ASCII art using the ALT + number technique, I noticed discrepancies when I looked at my MS-DOS work in Windows. This was not true with the keyboard characters, but it did happen with other characters. In one case–just one–a character that was visible to me in DOS (as an á) did NOT appear in a Windows word processor: ALT + 160.

I doubt that I'm the first to notice this, but I have never heard of anyone exploiting it for cryptography. An invisible symbol, even ONE invisible symbol, can create an invisible message. In cryptography, this is called steganography. The word steganography refers to two things:

1. Traditionally, a message hidden in an image such as a drawing or photograph.
2. In computers, hiding a file within another file.

I used the program "figlet" to create the following image:

```
 ####  # ####  #    # ##### ####  ##### ##### #   # #####
#    # # #   # #    # #     #   #   #   #     #   #   #
#      # #   # #    # #     #   #   #   #      # #    #
#      # ####  ###### ##### ####    #   #####   #     #
#      # #     #    # #     #   #   #   #      # #    #
#      # #     #    # #     #   #   #   #      # #    #
#    # # #     #    # #     #   #   #   #     #   #   #
 ####  # #     #    # ##### #   #   #   ##### #   #   #
```

This is what happened when I tweaked figlet to replace # with ALT + 160 (doing this in MS-DOS, of course):

What happened here is that I created an ASCII image that's invisible in Windows, but perfectly visible in MS-DOS. (Note to self: Be sure to send my modification to the figlet people.)

### Pseudo-Unary

This discovery gave me a challenge. How am I supposed to create invisible text while having only one character at my disposal? Even something as "minimal" as binary code requires TWO characters. I had a EUREKA moment when I was going through my notes in a book on programming in Pascal and saw the word "unary." I immediately understood that, in the end, binary is nothing more than unary code with an indicator for the OFF position.

Based on my knowledge that all IBM characters (on and off the keyboard) have equivalents in DEC Code, I knew that I only needed to create symbols for the ten numbers and to correspond text with DEC. I didn't want to use conventional binary code, because I wanted to abbreviate the typing. Considering the ON/OFF nature of binary, I knew that I only had to use a MAXIMUM of 5 digits for my notation. I also used blank spaces to substitute for the binary 0. Therefore:

```
0
1 á
2 áá
3 ááá
4 áááá
5 ááááá
6     á
7    áá
8   ááá
9  áááá
```

In the following section, I'm only using commas as place markers to keep track of the number of digits I'm using. (Try to imagine this without commas or the DEC code.) I can encrypt the word GROMIT:

Plaintext: GROMIT

```
DEC:    DEC-160:
071     ,     ,   ,   áá,   ,á    ,
082     ,     ,   ,  ááá,   ,áá   ,
079     ,     ,   ,   áá,   , áááá,
077     ,     ,   ,   áá,   ,   áá,
073     ,     ,   ,   áá,   ,ááá  ,
084     ,     ,   ,  ááá,   ,áááá ,
```

This may look clunky, but it's a lot more concise than binary. If I went so far as to type this without my place markers, it would look like a completely blank text file in Windows. If I did this with eight digits, I could create a HEX code notation too. With some simple programming, it would be possible to create an interpreter that would work faster than pen-and-paper.

### Level of Security

In a word: NONE!

Even if you ignore the fact that this can be read by the simple act of opening the text file in MS-DOS, the ciphers "DEC-160" and "Pseudo-Unary" were created with pen and paper. They can be broken in the same way. This knowledge is more useful in ASCII art than in real cryptography. Truth be told, I would classify my ciphers between ROT-13 and Vigenère as far as cryptographic strength is concerned. If I were to use it, I would use it in conjunction with other encryption. By itself, I don't expect this secret writing to be secure, but it can conceivably be used to "hide" other types of encryption and make them invisible in certain circumstances.

I remind you, I wrote this article in MS-DOS. This is NOT high technology.

-EOF

# DISCUSSION TIME

## Query

**Dear *2600*:**

My name is mohsen, I'm a student in software engineering. Write article What worked? I love that I work with your website. Please guide me. To working with you. What should I do? I am very eager to work with you. Please help me.

Thanks.

Best Regards.

**mohsen**

*Kinda vague but if you want to write an article with many sentences, we will be happy to look over it for as long as it takes and determine if we can use it. You should have gotten all of the information in our autoresponder but, in case you didn't, simply send your article to articles@2600.com. Good luck.*

## Spreading the Word

**Dear *2600*:**

First off, thanks for continuing to run this mag. I know it's difficult and costly and it's nice to have you guys around throughout the years. I am not a subscriber, but I do pick a copy up occasionally.

To get to the point, I would like to run a full single page ad in your magazine and am interested in cost. Depending on that factor, I may be interested in a half page ad. The content is pretty simple. I am looking for hacking/phreaking apps from the 8 bit era for machines such as the Atari 800, Ti994a, Amiga, Apple, C64 (though most C64 stuff seems to be easy to find).

I am also searching to find a program that is mentioned in a few places, but nowhere to be found on the Internet. I was in possession of the program before the Sundevil raids so I know it truly existed. It was written by Brew Associates for Phortune 500 and was called TransPhor. TransPhor was a PC version of Apple's AE file transfer program with some differences. It had a crude message base, and also a user account system rather than a "single signon" like AE had.

Why? Well, on the front of the old school h/p applications, it's for a project I'm already running called "The 8 Bit Underground," which basically aims to catalog all of that old stuff on the Internet before "bit-rot" kills all of the data on all of those 80s 5.25 inch floppies. If you would like to see what I've done so far and the format, you are welcome to visit http://blog.8bitunderground.com - the software archive I have built so far is a link at the top of the page.

On the front of the TransPhor BBS program, I am also a BBS nut. It was an interesting program and one of the few that I've not been able to put my hands on because it was so lightly released, and because the current "scene" of that time was disrupted by Operation Sundevil. I realize that the BBS will be next to worthless in today's computing environment, but I still want to immortalize it if I can find it, and I am willing to place a bounty on this particular piece of software for anyone who can find it for me.

Anyway, I may take a stab at writing an article that would outline all of this and more for your publication, but thought, if it was inexpensive enough, that a full or partial page ad would be more effective at reaching people. Maybe I'm wrong.

Regardless, thanks for taking the time for reading through this and I look forward to your response.

**Maynard**

*Least expensive of all is simply sharing what you've written here with our readers, who may very well be able to help you out. As for further advertising, please consider a marketplace ad, which is free for any subscriber. Finally, you would do well to join forces with textfiles.com, a site/project also dedicated to preserving the history of our community.*

**Dear *2600*:**

I have been working on my own network recon tool(s), as I wrote about a few issues ago. Those interested in trying it, requesting creature feep, stealing it, improving it, or just griping about it should feel free to check it out at http://systhread.net/coding. It is free, just like my site, just like my writing, just like my coding... you get the idea. Currently, it sports the following: very fast LAN scan, decent long hop single port scans, experimental IPv6 (single host and port), experimental passive scanning, a mini tcpdump utility, and ARP sniffing. There is still a lot to do but the goals of it are to be fast and small.

**j**

**Dear *2600*:**

I got a bit sick of Myspace and its hypocrites blocking people's site links. Myspace has more escorts, agencies, pimps, and drug dealers than any other site in the world hands down. But they block other sites for their content. So, when I pointed this out to them, they kicked my account off. In return, I created the code displayed now on my site at http://www.grhmedia.com. That will detect their servers and prevent them from seeing the actual destinations server, yet allow regular users through. They can defeat it, but it would require testing every link manually.

No actual hacking or anything illegal involved. At worst, they can say I am preventing their servers from being snoops.

**George**

*We'll just add this to the list of things that Myspace has to worry about.*

**Dear *2600*:**

Greetings to all fellow hackers! I know that a lot of us are concerned (maybe paranoid) about our data being available on remote computers in order to have access to them from everywhere. (I even encrypt my data before sending them to DropBox, even though they say it already is.)

I already read in this magazine that some of us created a local web server to have access to their files from everywhere instead of sending them to a third party. I like that idea, but why not democratize that web server?

I already took a look at the Tonido personal cloud and that was exactly what I wanted. The only problem was that when I checked the documentation to create my own application, I faced a nonstandard way of doing web apps. It was so weird that I just gave up. I guess I am not the only one since no one other than Tonido's crew are doing apps, even though they did a contest with nice prices.

That's why I started my own personal cloud with Tomcat, a small library that handles configuration and users, and some basic web apps to manage it. You can find it on http://cumulus-cloud.cc.

I am sharing that in this magazine because it is still an Alpha release and I am asking for help. You can contribute by checking the code for security issues, continuing the development, or just creating some nice web apps. Thanks to everyone.

**Pro Virus**

**Dear *2600*:**

Apologies if you feel that this mail is not addressed to the right audience.

I would like to introduce you to Null - the open security community, a registered nonprofit society in India. The community has members ranging from security researchers, law enforcement officials, and defense personnel, to business executives. Our focus is primarily on security research, awareness, and helping government and institutions with security related issues. We currently have six active chapters in India (Pune, Bangalore, Delhi, Mumbai, Hyderabad, and Bhopal). You can find more details about Null in our website at http://www.null.co.in.

Nullcon, the international security conference, an annual event, is held in Goa in the month of February. Null is the biggest open security and hacking community in India with around 1200+ members. This year's conference will be held on the 25th and 26th of February. Visit http://www.nullcon.net/ for more details.

We are looking for your support and association with Null and Nullcon. I request you to kindly see if your organization would be interested in collaborating with us for the event and our future initiatives.

**Prashant**

*India has a lot to offer for hackers and we're eager to see what the future will bring. We'll let our audience decide if this conference and organization are right for them. Either way, we wish you luck.*

## Coincidences?

**Dear *2600*:**

Here's a link to a news story I just came across on yahoo.com. I wonder if Doc Rivers is a hacker.

**The Asseater**

*We doubt it. The story is basically about the NBA coach for the Boston Celtics who hid $2600 in the ceiling of the Staples Center in Los Angeles to somehow entice his team into winning. He demanded $100 from each of the players, coaches, and even the manager, and told them they would only get their money back if they returned to that particular arena in the playoffs, which they later did. The interesting thing is that the envelope filled with money remained undisturbed behind a ceiling tile all year long. If we consider the facts that there are 28 other arenas, that NBA players tend to carry lots of money, and that this guy is a little nuts, it probably wouldn't be a bad idea to check out the ceiling tiles of some of these other locations. But, as for it having anything to do with hackers, it seems we can instead point the finger at simple arithmetic here.*

**Dear *2600*:**

I was reading 27:2 on a flight the other day. The flight attendant came by, and, instead of handing me one of those little tiny cups of soda, handed me the entire can. I can't help but wonder if it was because he saw me reading *2600*.

Granted, I shouldn't get excited about my 12 ounce gift after paying some-hundred dollars for the flight itself. But still, um, thanks?

**Drykath**

*Get used to a life of privilege that comes from proudly displaying our pages. Now imagine what might have happened had you been wearing one of our shirts.*

**Dear *2600*:**

I was in Silverdale, Washington a couple of weeks ago visiting a friend, and, after leaving my friend's house, I headed to the SeaTac airport to pick up my grandmother. Her plane was delayed, so I decided to leave the car at the airport and take the train into downtown Seattle to waste some hours. During the trip to and from downtown Seattle, I was reading the latest issue of *2600!* On the way back to the airport, the train suddenly slammed to a stop. Everyone in the train looked worried. Outside, I saw people from the neighborhood running toward the front of the train. A couple of minutes later the doors opened, and we saw/heard a lady screaming/under the train. It was, to say the least, tragic, and very painful to watch. The girl lived after being run over by the train, which is a miracle, but whether or not she kept her arm I don't know. Before, during, and after the ordeal I was holding onto my reading material (*2600*), and sometimes glancing at it to take my mind off the horrific scene. The transit ops chief wouldn't let us back on the train and instead made us wait for a bus. After waiting for two hours for the bus to finally arrive, I was pleasantly surprised by the number of the bus. Bus 2600 to save the day. I have attached two pictures.

**Micheal**

*While we weren't able to run the pictures in this issue, we felt the world needed to hear that story. No matter how crazy things get, it's good to know our readers are constantly thinking about us.*

## Exciting Offers

**Dear *2600:***

The New Age. Come one come all for the new age of technology. The digital download and the always abundant digital storefront.

We give you freedom. Freedom from porn. Freedom from free speech. Freedom to hear and see what we want you to.

Paying is easier than ever. Just hand over your credit card and we'll take care of the rest.

Sharing is not a right. Ownership is not a right. We dictate what you can and cannot do with the product, it's the only way to be safe.

Your digital rights are now our digital rights. Your liberty is now our liberty.

For your convenience we have removed unnecessary features. For your safety our stores will provide you with all the content you'll ever need. Thinking is now optional.

Your books, your movies, your music remains our property. We have liberated you from ownership.

We own the deed and dollar and download.

**cl0ckw0rk**

*The only thing you didn't tell us is how to sign up.*

**Dear *2600:***

I'm working on my third "Minto wheel" style heat engine, and would enjoy writing up what I have figured out during my journey, which begins with a conversation in a truck stop, contemplating the dippy birds for sale, with a fellow who claimed that he had heard a story about some engineers at a nuclear power plant who set up a wheel in the cooling pond and were able to pull substantial wattage from it until management made them take it down, and who informed me that instead of carbon tetrachloride, the fluid inside their wheel was nothing more exotic than club soda. (Which, on research, is one of the recommendations made by Mr. Minto in his 1973 pamphlet, and is what my sun mills use. Actually, cheap diet cola, or for higher pressure, sugar water plus yeast and a week.)

I imagine a handwritten article with amateurish freehand illustrations - back-of-envelope kinds of things - sprawling over five or six pages. If you would like to consider this for publication, would writing on letter-sized paper for reduction make sense, and how much margin should I leave blank around the edges?

**David**

*This might be a bit too mainstream for us, but, by all means, send it in. If we wound up using it, we'd likely wind up transcribing your handwriting into regular printed pages and we're not sure about the "amateurish freehand illustrations," just so all our cards are on the table.*

## Another Query or Two

**Dear *2600:***

Hello. I send email for *2600* but I did not get an answer. If possible, please answer me. :( Thanks.

Best regards.

**mohsen**

*This is where it gets a bit tricky. If you sent us an email, we sent you an email back. But now you've sent us a second email saying you didn't get a response to your first email. We can tell you for sure you won't get a response to the second email since it was sent so close to the first one. That's the way our system is set up. If we sent an autoresponse to every subsequent email, all sorts of mail loops would begin with other autoresponders. We also don't send personal replies to every piece of mail as there aren't enough hours in the universe for that. So we hope you'll see our reply here in the magazine and will act accordingly. It was our pleasure answering your question.*

**Dear *2600:***

"By the early 1970s, hacker 'Cap'n Crunch' (a.k.a. John Draper) had used a toy whistle to match the 2,600 hertz tone used by AT&T's long-distance switching system. This gave him access to call routing (and brief access to jail)." Is this the mystery behind the mag's title noobs like me have been trying to solve?

**Ben**

*It's not really a secret that this is what "2600" means and it's pretty easy to find that out by looking up our history online or at any FBI office. Still, we're glad you now know the truth.*

## Policy

**Dear *2600:***

I have written an article concerning the cable modem termination system and internal network security that is currently being used by a company that I am intimately familiar with. I am concerned about my anonymity should this article get published. I feel that the activities of the network management staff are putting the customers at risk on a day-to-day basis, and this information should be made public. I would like *2600* to be the voice by which it is carried. The tradition of the magazine has inspired me in so many ways and I want to give back to the community by adding to the collective knowledge base inspired by freedom of information. Please let me know what the policy is regarding author anonymity. I want this information out there, but not at the cost of my career.

**Handle Deleted**

*Well, to start with, we even eliminated the handle that you signed, since it's possible that you used something that could get traced back to you, thinking this letter might not get published and that instead you'd get a personal reply. So we do take your privacy seriously. We do not hand such information over nor do we leave it lying around for others to find. We do stress, however, that many times a writer will include some personal detail that will help certain people find out who they really are, such as a geographical location, personal anecdote, or even an email address that can be cross-referenced with ease. Writers need to keep these things in mind if they want to remain anonymous. We agree that getting the information out there is a priority. Keeping yourself safe from retribution is also a priority, but one that you have much more control over than we do. We look forward to seeing your submission.*

**Dear *2600:***

I'm glad to hear you've selected my article for publication. Thank you! I'm writing to inquire about your request in the latest *2600 Magazine* for the next generation of "The Hacker Perspective," which I only just read about yesterday. Had I known about this a bit earlier, I would have requested that my submission be considered for "The Hacker Perspective."

Can you tell me if my submissions meet the criteria for "The Hacker Perspective," and, if not, why? Note that I would consider altering my submissions to meet your requirements if necessary. Hey, when $500 is on the line, that's some pretty powerful incentive.

**K**

*This column is quite specialized in what it contains and, while there were elements of that in your article, it wouldn't have been enough to qualify. Had there been, we would have let you know. That said, there's nothing stopping you from submitting such a column for future consideration. Right now, though, we're full for at least the next year, so please wait until we make a new request in a future issue so that it doesn't get lost in a pile. We are thrilled with the amount and quality of submissions we've received for "The Hacker Perspective" since opening this up. We hope to see "regular" article submissions also continue to pour in, as they are key to the information that gets disseminated here.*

**Dear *2600:***

I have an article that I would like to send in for consideration. Do you accept articles sent in Word format? If not, what format do you prefer?

**Jody**

*We accept all formats, but if it's something that we wind up having significant trouble converting to ASCII for whatever reason, we usually get impatient and move on to the next one. Life is too short. This is also a reason why we tend to discourage encrypted submissions. While we love encryption, more than half of the articles submitted in this fashion have some issue where a bad key is used, some kind of version conflict occurs, or there's some other sort of problem that we just don't have time to go back and forth to resolve. We're certain that many good articles have never seen the light of day as a result of this. Hopefully, one day these conflicts won't be such a barrier to so many users. Unfortunately, that day has not yet arrived. Until it does, there are other (and more effective) safeguards you can employ. For instance, if you work for the Department of Defense and you want to send us an article about a specific security gaffe, sending an encrypted message to articles@2600.com from your dod.gov account really isn't going to do much to cover your ass. Your superiors will be jumping to all sorts of conclusions in very short order and you'll likely be invited to a number of rather contentious hearings. If, however, you send us your article from a civilian email account that you've only set up for this purpose, provided you're not already under surveillance from your home, you should be fine sending it to us that way unencrypted. Obviously, supersensitive material gets more complicated and in such cases we take the time to work something out. Oftentimes, though, more attention is drawn because of the extra precautions being taken and not because of the actual content, crazy as that may sound.*

*We apologize for answering your simple question with a mostly off-topic essay.*

**Dear *2600:***

I recently wrote an article on turning an iDevice into a complete mobile penetration testing device and would like to offer it up as an article for the next *2600 Magazine*. It can be found at blog.nickmpetty.com/. If you have any questions, please contact me via this email address.

**Nick Petty**

*Unfortunately, the moment you put your article on a blog (no matter how small it may be or how few people may read it there), it became ineligible to be printed in the magazine. As consolation, we're letting people know how they can read it. The reason for this policy is so that the material printed in our pages is not something our readers may have already seen. They get extremely enraged when that happens. Trust us. We do look for evidence of every article we print already being online in some form. We've even had cases of writers posting their submissions online right after we've notified them that they were going to be published, presumably to let other people know it'll be showing up in an issue. It's unfortunate, but we're forced to pull the article at that point for the above reasons. Of course, you are free to post your article online after it's been printed. But to be published here, the material has to be new.*

**Dear *2600:***

So it looks like the *2600* group in Chicago has been dormant/dead for over a year now. The meeting place that was listed on the *2600* site, and chicago2600.net is closed down, and the last post on chicago2600.net is now over a year old.

In the wake of not having a *2600* group in Chicago, the Chicago Hacker's Union (CHU) was formed. The idea was proposed that CHU should talk to *2600* about having/hosting *2600* meetings. CHU has a monthly public meeting on the last Thursday of every month from 6:30 pm to 9:00 pm. The format of the meeting is a presentation by one of the members followed by group discussion. After the presentation, the meeting follows the pattern of most *2600* meetings I have been to. People talk with each other and show off their new cool tricks.

There are some things to be aware of. The Chicago Hacker's Union is affiliated with a labor union, the IWW. There are dues to be a member of the union, but our monthly meetings are free and open to the public.

Let me know what your thoughts, concerns, and ideas are.

**Steve**

*This sounds like a good gathering place for hackers to go and we certainly support that. However, it's not a 2600 meeting for two reasons. First, meetings aren't sponsored or affiliated with any other existing organization. Second, meetings are held on the first Friday of the month. The first rule is so that the meetings remain independent and not subject to anyone else's agenda, regardless of how much they may appear to be in line with what we're all about. The second is simply a matter of logistics. If you look at the tiny print on our meetings page, imagine what that would look like if we had to add different days for different meetings. We would also quickly lose track of when the meetings actually take place. While we know that there will always be people who can't make it on Friday evening, the same will hold true for any day at any time and the first Friday has become a tradition over the past 23 years. We hope to see a 2600 meeting return to Chicago but until and even beyond then, we will help to spread the word about what you guys are doing.*

**Dear *2600*:**

I recently got into the *2600* hacking quarterly magazine. It's awesome. I'd love to communicate with other hackers, but sadly there is no *2600* forum.

Keep up the good work!

**Bobby**

*Yes, we've shied away from this as it requires a lot of work and maintenance, not to mention the fact that forums tend to be dominated by people with the loudest voices and most shocking/offensive stances. We have to focus primarily on getting the magazine out. If such a thing becomes doable for us in the future, we'll be there.*

## *Critique*

**Dear *2600*:**

I was disappointed by two things in 27.2.

First, in Poacher's article on how to steal from grocery stores using faked UPC barcodes, he claims "there will be no way of knowing how and when the items left the store." Of course they can detect this. If they notice a large number of incorrect weights on a transaction, plus a large number of "baked beans" in the same transaction that doesn't match inventory, it'd be trivial to detect and match with CCTV and your payment method.

Likewise, any store security will notice if you go around putting UPC stickers on "a large number of products." In addition, all checkout scanners beep, have a brief lockout, and display the purchases on every single item scanned - including loyalty cards. This, again, would be noticed very quickly... and coming back to cash it in would lead to a detour through jail.

If you're going to be a thief, at least don't be an idiot too by dismissing the ways that you'll get caught, and don't recommend hypothetical techniques you clearly haven't tried yourself.

Second, the editors' response to Jsnake asking about the reason for the layout of letters was rude and inappropriate. The same dismissive tone when asked about some detail of someone's else's actions is what you have railed against in the opening editorial many times. Why condemn curiosity for its own sake when it's aimed at you? I thought we're supposed to encourage and support it.

On the positive side: Brian's article on Bayesian Craigslist classification was interesting, and I'd like to see it happen. A more powerful technique that he didn't cover might involve a support vector machine (SVM) - but it's impressive how good the results are from even a simple Naive Bayes classifier. Of similar interest is OKCupid's statistics blog - http://blog.okcupid.com - which has direct access to a fairly massive dataset, analyzed well.

People interested in p4nt05's article on darknets may like to investigate cross-hackerspace VPNs, some of which are set up for CTF hacking games. Visit hackerspaces.org to find your local hackerspace and ask them about what's available or how they could join existing networks.

Happy hacking.

**saizai**

*Concerning our response which you cite, this was to a reader's eight paragraph long letter theorizing as to what we were thinking when we continued a previous letters column onto another page. Perhaps you're strong enough to resist turning to sarcasm in such a case, but we have a very hard time doing that. If, however, our remark to that letter writer was indeed "rude and inappropriate," we're fully prepared to step forward and do the right thing, whether that be covering any resulting therapy sessions, punitive damages, and the like. If, however, your remark was simply to try and get us to resort to sarcasm yet again, you have played the game well.*

**Dear *2600*:**

I recently read the article "How I Scored the Avaya PBX Init Password" in the Summer 2010 issue and, coming from an Avaya background (I'm actually a certified Avaya tech), I found the article poorly written. It provided no real information, nor did it shed any light on what it meant when the individual actually got the "init" password. I can tell you that the "challenge" response this person got was part of a program that every Avaya technician has which takes the "challenge" and pairs it with a code within the Avaya program.

A little background on the Avaya platform: Today's Avaya PBX runs on a Linux OS. If you know even a little bit about Linux, then you can pretty much guess what I'm going to say next. The "root" password is always going to be default. So, if you find yourself in front of one, chances are you will be able to get into one. Business partners and Avaya installation technicians are supposed to change these, but they rarely do. The "craft" passwords work like the "init" passwords. You're given a challenge and the Avaya program pairs it with a code so you can get into the system. So the chances of you getting into the "init" or "craft" logins are pretty slim, but if you feel froggy, figure it out! Just make sure you tell us how you did it. haha.

Most business partners use the "dadmin" login which is used to program stations, trunking, etc., but now Avaya has added a PIN component, so nowadays it's hard to crack these logins. However, the dadmin logins are usually defaulted as well, but if you can figure out the root default login, then you can probably figure this one out too.

Anyway, that's all I had to say about this. Avaya is doing as much as they can to secure their systems and are now pushing for a "SAL" solution which goes through VPN, then you have to put in an "admin" login, then a "dadmin" login, and finally the PIN. You think they're worried about security?

Thanks for the time and information. Love your magazine!!

**anonymous**

**Dear *2600*:**

The article in 27:2 ("I'm Not a Number" by Poacher) has some erroneous information that is worthy of sharing. The simple version of one of his exploits is to create a canned beans barcode and stick it on any item you want (be it a TV, a DVD, a laptop, or whatever). While he is smart enough to make clear that this is illegal and should not be done, he is not smart enough to know why this won't work. Programmed into each of the scanners is a scale to see that every item is scanned. This prevents people from just passing items through without scanning them, because the weight shouldn't change between barcode scans. However, the system is more sophisticated than that. Each item has a weight range as a double check. That is why you can't get away with scanning one can and putting six in your bag. It is also why you can't scan cans and expect to get a laptop to ring through correctly.

There is some slop in this (the scale isn't very precise), so it isn't guaranteed to work against the hacker who would try this. Further, for all I know, this feature isn't implemented in every installation. However, I remember this being discussed when barcode scanners first came out (yes, I'm that old).

**The Piano Guy**

## *Still More Grammar*

**Dear *2600*:**

t0sspint writes: "Words like extricable, abeyant and truculent flooded my email and peaked my interest." t0sspint means to say "piqued my interest."

It is surprising that in this day and age of such powerful computers with spell and grammar checkers one still sees howlers like this.

**Robert Lynch**

*We do occasionally miss things, as we did in the example you sited. For all intensive purposes, most people could care less if their was perfect grammar on our pages and perhaps discussing it is a mute point in this day and age. It could also be a blessing in the skies, though, since it makes those who do pay attention ostensively more intelligent. We're certainly not adverse to doing a better job on this, especially if it'll effect our readers abilities to try and write good.*

**Dear *2600*:**

Debating grammar is approximately as stimulating as washing dishes. Unfortunately for Adam, et al., the rules of grammar are rules, not vague guidelines. There is precisely one correct parsing of the sentence. A rebuttal of Adam's analysis in 26:4 can be found at: http://www.chompchomp.com/terms/prepositionalphrase.htm

The basic rule requiring agreement in number of the subject and verb of a sentence, or of a pronoun and its antecedent noun, is taught in the fourth grade. More complex grammatical analysis is taught in the seventh grade. Adam, et al., are, simply and embarrassingly, wrong.

There is a jpeg facsimile of an eighth grade graduation examination administered by Kansas public schools, circa 1890, floating around the web. Adam, et al., would, in all likelihood, flunk the exam.

We, who learn our language colloquially, frequently make mistakes which would not be made by foreigners who learn English in school, as a second language. (Unless, of course, we have actually paid attention in our elementary school English classes.) It can be disconcerting to converse intelligently with a foreigner over an extended period of time and then produce utter consternation by saying something like: "Hang a U and park here."

As New Yorkers, the *2600* staff are probably aware that the *New Yorker* magazine had exceptionally high grammatical standards continuously from its inception until the paranoid schizophrenic Australian bought it. If there were an online archive of the text files of *New Yorker* articles, Adam could search it in vain. There is undoubtedly not a single instance of the erroneous construction that he urges upon us in support of his erroneous opinion.

Grammatical purity has not been the strength of *2600* during the many years that I have been reading the magazine, but the grammar in editorials has improved steadily over the years and is now quite good, in my opinion.

**RWM**

*At last, we have arrived.*

## *Infiltration*

**Dear *2600*:**

I just thought I'd share a little story with you. I was at my sister's horse reining competition a couple of days ago, and was bored out of my mind. At one point during the contest, my family and I walked up to the tent where the scores and awards were given out, and I noticed something kind of odd. The tent was really a huge awning kind of thing, and photocopies of original judges' score sheets for each horse rider were kept in three ring binders, sloppily thrown all over several tables. As I watched the contestants coming up to the tables, I stood back as they frantically would skim through a binder, even if it wasn't labeled for their class, throw it aside, and continue on their search for their scores. Taking this disorganization into account, I decided to try a little experiment.

During a lull in the search frenzies, I collected all the binders, stacked them up, placed them in orderly columns, and sat down with them. As people came to check their scores, I would ask them what their class was, and hand them the appropriate binder.

Eventually, people began asking me questions. These ranged from why I thought they received the scores they did to directions to various things at the competition grounds. People even began complimenting the job "you guys" did with the contest. Now keep in mind, I am an 18-year-old in board shorts and a t-shirt. My lack of Wrangler jeans or a cowboy hat made me stand out, not only from the employees of the grounds, but from just about every person there. Also, I know basically nothing about horses or horse riding, let alone competitions and scoring procedures. But my experiment was working; people were assuming I was an employee at the reining competition.

Within 45 minutes, a real employee, with the word "Contest Manager" embroidered into her blue polo shirt, came up to me and told me I wasn't "needed at the table anymore." She suggested I follow her, and realizing she actually believed I was one of her employees, I continued to play my role. Leaving the scores behind, I walked behind her as we walked through a building near the awning. We continued behind a desk where all the contest's prizes were stored (interestingly enough, where my family was at the time. They did not notice me whisk past them.), out a back door, behind the main arena's riding area (I do not even know what its official name is. If horse riding was similar to football, you would call it the "field." But maybe not since I don't follow football either.), up a series of stairs, and into the judge's booth.

The manager asked the two men inside if they needed any assistance, and one said, "Nah, not right now. You could take these scores to the photocopy room though," and handed me a new binder. I opened it up and was surprised to see scores from recent riders, written in pencil, from both judges. The manager told me to go ahead, and she began a conversation with one of the judges. I left the booth and continued back to the previous building, assuming that was where the copy room was.

As I was walking back, I was awestruck by how easy it was to gain access to the judge's booth, and how their original scores were written in pencil. At any point from leaving the booth to entering the building, I could have easily changed any of the scores before they were photocopied and manually submitted to the contest ground's computers.

Entering through the back door, I walked past the stacked prizes. Dozens of belt buckles, even more ribbons, and several expensive saddles, were neatly set on shelves, and I could have taken any of those without any question (maybe the saddle would have been too obvious). Incidentally, I didn't need to take any, even if I wanted to. My sister won a first ribbon and a third ribbon, as well as a Top Five belt buckle.

As I reached the desk, another employee asked me if I needed anything, with an odd look on her face. "No, they just wanted me to bring you this," I replied nonchalantly. At this point I was getting a little bored, so I gave her the binder, she thanked me, and I walked out the front door, and headed back to our family's trailer across the grounds.

My experiment granted me access to official scores and official prizes, in less than an hour. I was consorting with contest officials like I was one of them, and they trusted me without question. I can only imagine the security on these people's home computers.

**Jeff**

*You basically earned these people's trust, albeit not through the normal channels. There really shouldn't be anything wrong with this, as life is filled with such stories. Isn't this how Steven Spielberg got his start? (Actually, it's not, but it's still a great story.) While you certainly could have messed things up if you had the desire, too often we're left with the assumption that this is what an individual will do in their default state. In actuality, people are more often honest than dishonest, yet society's lowered expectation may well turn out to be a self-fulfilling prophecy. If people are treated like criminals, then they will behave like criminals. You weren't treated that way, and you didn't act that way, so if you really wanted to become involved in such horse activities, this would be a classic way to make your debut. As for the computer analogy here, these people may well have all sorts of security issues. But if they have everything locked down tight because they're afraid of hackers, they've taken care of one problem while buying into something else that's equally problematic. Communication, mutual respect, and, yes, trust, are all key ingredients in being both secure and open at the same time.*

**Dear *2600*:**

It's been almost 15 years since I first walked up to the front door of the Berkeley, California Pacific Bell central office on Bancroft Street in downtown Berkeley. I walked up to the large black phone box to the right of the locked glass doors, opened the metal door on it, picked up the phone receiver inside, and heard a tone. I dialed "9" on the keypad, then a local (510 area code) phone number. It worked! Then I tried long distance. It also worked! I laughed and laughed and laughed. Right outside the front door of the Pac Bell CO, using their own phone that was meant to only call the switchroom and such, one could make free outgoing calls just by pressing "9" first. It was one of my very first hacks and I passed it around to many homeless people who needed to make the occasional free call.

You can imagine my surprise and ensuing stomach-hurting laughter when I tried it again tonight, October 1st, 2010: I could still make free local calls by pressing "9" first. Will they never learn? Shouts out to Ma Bell!

**Barrett D. Brown**

*They must figure that few people would have the audacity to stand directly outside the central office making free calls on their phone. Perhaps they just want to compile a photo album of all of the people who do.*

## *Fighting the Power*

**Dear *2600*:**

I was watching a documentary about the corporations responsible for creating the software used on electronic voting machines and I took note that the source code to the software was kept under lock and key. Even election officials and some government bodies were prevented from reviewing the code. When the inevitable security holes came to surface, it got me thinking about how they could be avoided and it reminded me of an open source encryption program with which you are most likely familiar: TrueCrypt. The fact that it's open source means the code is under the scrutiny of the public eye and this ensures there are no backdoors or other weaknesses, and in a recent example it's been shown that a drive encrypted with TrueCrypt was uncrackable by both the Brazilian government and the U.S. FBI after 18 months of trying.

My idea was that if the voting machine software was developed as an open source project, or at least if the code was released for review and changes, there would be no possibility of foul play. After hearing you guys discuss ways to better secure voting at the physical voting place on your last radio show, I was wondering what you thought about the software element. Would open source voting machine software be a more secure alternative? What other measures would you suggest or like to see in voting machine software, in addition to the physical measures you discussed on the radio?

**Samuel**

*This should not even be a negotiation. The only possible system that could begin to be trusted would be something that people are able to, and in fact are encouraged to, examine and look for weaknesses on. The existing "black box" technology does nothing but foster mistrust. Any system must have a paper trail, be easy for voters to understand and use, allow for sufficient privacy, be prepared for voter error or confusion, protect the secrecy of the ballot, have the ability to be run during a power outage, and more. So many existing systems have failed in several of these categories. It can be done right. But, just like with any software application, when it's done wrong, it can be a real nightmare. As the ultimate end users, we have the obligation to point out where it's fallible and to demand a better product. As hackers, we have the additional obligation of figuring out the weak points and sharing this information. This is the foundation of our democratic system, after all.*

**Dear *2600*:**

With regards to proprietary formats, CSS, closed source etc... If a beer company made a beer that you could only open with their bottle opener, which cost an outrageous amount, would you still buy that beer? Would you try to circumvent the opening mechanism? What if it were illegal to circumvent the opening mechanism? The only problem is that with DVDs, software, etc., a lot of times there aren't as many choices as with beer. Are you tired of these stupid analogies? Heh.

As for me and my house, we will continue to open our beer, and our open source software the old fashioned way.

**drlecter**

*The only reason such an analogy doesn't actually exist in real life is because they haven't figured out a way to make it happen. Yet.*

**Dear *2600*:**

I'm a new reader and am currently looking at 26:2. There is a reader's letter about hacking OBD-2 systems (current engine management systems required in cars sold in the U.S.) and how doing so would help consumers and independent repair shops compete with dealerships. This message is consistent with hacking and the theme of the magazine.

The letter also mentions a small group of tool makers who are petitioning the government to make a law requiring auto manufacturers to share more information and tools with the consumer and independent repair industry. In the editor's response to the letter, in italics, is a link to the right to repair group's web page, which seems to indicate support for this group and its movement.

To me, supporting the right to repair crowd is support for big government. This is a case of the consumer (and the independent repair shop) versus the manufacturer. The free market provides a mechanism for us to deal with this, which is don't buy cars unless they have the features you require. In a free market environment, the last thing we need is more government interference.

And, it sounds countercultural for *2600* to support such a move anyway. The hacker culture is about independence and freedom of knowledge and, is largely, anti-government. Those values do not coexist well with calls for more government regulation.

There is also a letter about privacy issues in Alamo and other online car rental companies. The call for action in the letter is for additional government regulation in the form of privacy laws. A better call to action would be for customers to discontinue using these rental car services until they fix their service.

I see a common theme in several letters to *2600* where the call to action is for government regulation to fix security vulnerabilities. What a joke! *2600* should lean on the free market and educated consumers to affect such changes. Government has never been a good way to improve market conditions.

I would expect the editors of *2600* to agree with this perspective. I'd hope you would correct your readers when they request more government interference in the free market, instead of supporting (even if silently) such requests.

**Brian in Leawood**

*We hear this view frequently but can't help to conclude that it's overly idealistic. Confusing over-regulation with consumer protection is exactly the thought process desired by those who want to have things their way without any opposition. If the people who spoke out so fiercely against "big government" also viewed "big business" with the same suspicion and hostility, the possibility might exist for some sort of populist movement that would actually protect individuals from abuse. Sadly, this is rarely the case. The huge corporations are simply "trusted" to do the right thing with the misguided belief that the free market will somehow even the playing field. That just doesn't happen. Individuals cannot just stand up and defeat entities that have more power than many countries, not without an awful lot of support. Where would this support come from? Other people, obviously. But this would be rather hard without a good deal of publicity, and the media is another one of those entities that is in the hands of the most powerful, not the most populous. The fact is that governments are supposed to be the tools of the people. That means when you need them to help you, they should do precisely that. The people decide if they want to elect those who will protect their interests. And if that means getting people in power who will stand up for their rights in demanding certain things from these corporations, that is precisely how the power structure should be used. Ultimately, the purpose of government is to take care of the people it serves. A corporation has no such obligation inherent in its own structure. And individuals have precious little chance of altering such an entity's direction on their own. It's only through political pressure that real change can be made and we shouldn't be discouraging that kind of approach. The examples cited are perfect examples of corporate abuse and show what direction we'll be heading in if there is no oversight and no means of preventing such injustice. If all cars are locked so that only car dealers have the access to repair them, it's not enough to say that we can simply stop buying them. Obviously, that won't be an option unless there's a viable alternative. An unimpeded industry has absolutely no motivation to make such an alternative happen and civilians have no power on their own to turn things around. Not without massive anti-corporate revolution in the streets. And we suspect that's not what you're suggesting.*

## Yet Another Couple of Queries

**Dear *2600*:**

Hello. I send an email for you but you not answer me. i want write an article for your magazine, i want need some information about your magazine, What kind of article can be write for magazine?

Thank you.

Best Regards.

**mohsen**

*We're not sure what kind of article you're interested in writing, but, as you can see, our standards for letters are pretty liberal. If you continue to have trouble getting an autoresponse from us, why not simply visit our website, which will address all of your questions? We must say, there is visible excitement at the office as to just what this article might be about when it finally gets here.*

**Dear *2600*:**

Last week my PR department sent you a press release about our latest product and I wanted to follow up and make sure you got it.

If you have any questions or would like to receive additional information about our products and our company, I will by happy to handle that for you.

*2600*, if I've reached you by mistake I apologize and would appreciate it if you could pass this note to an employee I can talk to.

Thank you for your assistance.

**Denis Gladysh**
**Senior Project Manager**

*This note has indeed been passed on to someone in the appropriate department who you can talk to. Expect to hear from a "4chan" representative soon. And frequently.*

## Addendum

**Dear *2600*:**

I would like to offer a minor correction to my article you published in 27:2 entitled "Roll-your-own Automated System Restore Discs." In the "Final Thoughts" section, I mentioned that PING overwrites your "partition's MBR," which is, of course, incorrect. Partitions don't have MBRs. I meant to say that PING overwrites your partition *table* (and everything else) in your MBR. Either way, back it up if you change it after creating discs (even better: create a new set of discs after modfying the table). Thank you for a great publication!

**ternarybit**

**Dear *2600*:**

I remember reading in the past that it's hard to keep track of distribution or whatever if the barcode doesn't scan so I thought I would just let you know that when I bought a copy of the mag, they had to manually enter the number. On the receipt, it just shows periodical and the barcode number.

**Jason**

*Thanks for letting us know. If the number showed up on the receipt, then the sale was, in fact, credited to us. When that doesn't happen, it's quite possible that we won't get anything at all, depending on how the store in question operates.*

## Advice Sought

**Dear *2600*:**

I am endeavoring to become CEH certified (ethical hacking). My problem is I'm an intellectual hacker. I understand and can converse intelligently about hacking having never done any *real* hacking. My question is where should I start to have a credible body of knowledge to take on, what would be a new career path for me? The end result I'm going for is being employable as a penetration tester and being flexible enough to understand more of the skills needed so I can progress successfully Any advice you can provide would help immensely.

**Salih**

*We're not really big on career counseling, nor on terminology, especially the bogus kind with words like "ethical hacking," "black hat hackers," and the like. These are phrases created by the security industry to try and compartmentalize the hacker community into neat little packages that can be easily defined and manipulated. It's all a load of crap. If you're truly passionate about the world of hacking, then dive into the culture, read what's available about it online, look at the kinds of articles we print, start playing around with technology. Don't fixate on how it's going to pay off or what you're going to call yourself. If you truly have the interest, pursue that and figure out where your strengths lie. It takes years, it's not easy, and most people will think you're completely wasting your time. But if you're truly into it, you will enjoy the process and meet a whole lot of really interesting people. It's a journey that simply can't be rushed. And if this isn't you, that's fine, too. You should be able to find what you're looking for through corporate conferences, expensive seminars, and security training. You'll have lots of company.*

**Dear *2600*:**

PayPal has discontinued the single-use generated credit card for purchases, which seemed to me to be a very cheap and useful alternative for those who either didn't want or couldn't get a credit card. Some want to order items with the protection from automatic charges that require the consumer to dispute. Is there anyone else out there who does the same thing?

**John**

*There are services offered by Discover (Secure Online Account Number), Citibank (Virtual Account Number), Bank of America (ShopSafe), and more which allow you to give a "special" card number to a particular merchant that's not your actual credit card number. You can set the expiration date so that it can only be used once or use it for recurring charges that only that merchant can use. However, this doesn't work if you don't already have a credit card with one of these credit card companies. We're curious if there are other services out there that people without credit cards can use.*

**Dear *2600*:**

I am a 14-year-old hacker/programmer/Linux devotee. I have enjoyed your magazine for a few years now. Sadly, I cannot subscribe because my parents would freak out if they found a copy of your mag in the mail! I am stuck reading *2600* at bookstores, and occasionally buying a copy when my parents are not looking (which is rare). Is there any way for me to subscribe to *2600* and receive them *not* in my mailbox at home? (I have the money). The answer is probably no. I would like to write an article for *2600*, perhaps on modifying and using Medusa.

**Cm0nster**

*If you have enough money to buy a Kindle or a Nook, you can now get a copy of our magazine in that format. Assuming your parents don't peruse these devices to see what you're reading, you should be safe. There are also applications that will allow you to access this content through* *an iPad or equivalent.*

**Dear *2600:***

Some friends of mine have recently decided to put together a local magazine and are debating formats. I have always loved the *2600* digest size and the lo-fi style and want to show them a copy, along with info on costs and a quote from a printer. Who do you guys use to print up the magazine?

**nate**

*Who you use depends on so many factors, including frequency, size, distribution, and more. If you're just starting out and you're fairly small, we suggest going local. If your run is in the tens of thousands, then a larger company in another part of the country would be more economical (they are quite easy to find). The most important thing we can tell you at this point is to know your audience and work with that. You don't want to overdo it before knowing what your demand will be or you will burn out quickly. Once you have a sense as to how big your readership will be and what it is they want, you can focus on growing within those parameters. It's a tough business but that's all the more reason for there to be more people trying to make it work.*

## *Challenges*

**Dear *2600:***

Here is my experience with Doctor Antivirus. This is how I fought a malware infection and what I did to solve the problem. I hope this will help someone else fix their problem and inspire others to not take the easy way out by reinstalling their OS, but fight against the producers of such malicious shit. By all means, try this at home. Post your results. Help others to fight these greedy bastards.

Let me start by saying I keep my anti-virus up to date and running. Same goes for my OS. I should have created a limited user account to surf with, but I always seem to forget. Learn from my mistakes. Don't let this happen to you.

After a long day of reading Linux manuals, I had decided to relax with a little web surfing. Suddenly, *thar she blows.* An annoying ad, as big as a snow hill, saying I've got a virus. Shit. I've been down this road before. WinPatrol caught it before it could get all the way installed. So this gave me a fighting chance.

I closed down my browser and did a search of "My Computer" to ID any files that had changed. Locating them, I tried to delete them to no avail. Finally, I changed the properties to read only and went to the command line and did "del /f" to get rid of the POS things. So far, so good. Pop-up's dead. Next, run virus scan. It came back clean. Spyware removal next. Strange, my spyware removal doesn't work. It *was* working. Oh well. I'll just download another one.

Thinking I was in the clear, I went back to browsing, did a web search, and noticed my window for what I had searched for looked strange. The text was only showing half height. My browser had been jacked. (Internet Explorer as well as Firefox. This told me it was not just the browser, but something on the system.) Every search for anti-virus or spyware removal would not display. I tried getting around it with mixed results.

OK, into safe mode virus scan. It was clean, also. Back to normal mode. Update my anti-virus (it was almost 24 hours old). No luck. I couldn't connect to the server. This had occasionally happened before, but I thought something else was up. Back to the command line. A quick ping of www.avg.com showed an IP address of 127.0.0.1 (same with www.grisoft.com and www.trendmicro.com). Yahoo and others came out correctly. Web search for an online ping to get IP addressees for these sites showed I could ping them with their IP address and get a correct response. DOS time. Ipconfig/flushdns, no luck. Ipconfig/displaydns also yielded no clues.

I was in a little deep. I needed help. I called my bro Shean. No sweat, he would get some recovery tools from the net and get me going. Well, the tools didn't work. Web searches turned up info I had already tried. Online anti-virus and spyware scans wouldn't connect. Searches through other help sites turned up nothing. Shean was doing this because I was unable to get to these sites myself. I also took the advice of turning off system restore until I had everything under control. He got the tools on CD or emailed them to me. Some required registration or updating online before use. How are you supposed to do this when you can't connect to the site?

The CDs used some version of Linux to boot. I've had mixed results getting Linux to recognize some of my hardware on my laptop, therefore I was not surprised when they didn't work on my system. They worked great on Shean's desktop, but not for me. The emailed programs would install but not display (Task Manager showed them as running).

Going through my browser's settings, I had to change its behavior (connect in same window). I remembered my A+ instructor talking about spyware and saying if he could not find it in 15 minutes, he just reimaged the drive. I understand that from an economic standpoint in the business world. Just get it up and running. On the other hand, without the fight, there is no learning. I thought about giving up several times, even to the point of booting from my DVD to get to the recovery console. Alas, the Gateway factory DVD is not standard Windows and has no recovery console, only reinstall to factory new. Although I regularly backup my downloads and could restore all my programs, this was not acceptable. I became more determined than ever to kick these greedy bastards' asses.

Next up: Wireshark. This showed my pings to anti-virus sites not even leaving my computer. Consulting Harvey's book I found the key for browser helper objects (HKLM\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects). Regedit, here I come. I checked the keys and found a couple of suspicious entries (wormradar.comIEsiteblocker.navfilter and linkscannerIEnav.filter). The search was on through the registry jungle. Using the CLSID, I searched and deleted all keys related to these. This was enough to enable me to get to some sites. They were still blocked if I hit "open in new tab" but by copying and pasting the DNS in the URL bar and using the enter key instead of the goto arrow I was able to get to some sites. Most kept on saying things I already knew (get anti-virus, etc.). All responses Shean and I found showed people were still having problems with this and the fixes did not work. As a downside, it really seemed to do a number on laptops. They only seemed to address the pop-ups and not the browser hijacking. The search for browser hijacking started.

Finally, I had help in the name of "UnHackMe" (from http:greatis.com/unhackme). Got it, ran it, *bingo.* "Hidden program running TDSSserv.sys." A quick registry search turned up the key. Investigating it showed a key labeled disallow. This had the names of the executables of the anti-spyware I had been trying to run but would not display. Recommended action: reboot and it would be deleted on startup. Did and bye bye hijacker. Ping confirmed success as well as browser behavior back to normal.

Now to finish the job. Three scans of one antispyware tool later showed I was clean. Next on the list: "SuperAntispyware" (http://www.SuperAntispyware.com) free edition. This picked up even more crap. Scanned until clean. Update anti-virus scan until clean. Safe mode and repeat. I win.

Quick extras for dealing with malware I picked up from an unremembered source on the net: When closing down a suspected piece of malware, use alt+F4, not the close button. Some malware use this as an install area. Also, when trying to connect to a site, use enter instead of the connect button. This helped me as the button appeared to be hijacked and would send me off to never never land. After all that, I felt good about not giving up. I've won a skirmish, not the battle, and far from the war. It's a constant struggle to try and keep up. We must fight - there is no other option. It took me about 20 hours over four days to fix this problem and I would do it all over again if I had to. I could use this time to slam Microsoft or the anti-virus and anti-spyware manufacturers, but I refuse. In general, they do a very good job. I got infected through a little carelessness on my own part. It was my fault, plain and simple. That does not mean I will let the adware people and their greed off the hook. These people are assholes.

Well, that's all I have for now. Keep the faith and keep up the fight. I didn't do everything by myself; I had some help. I'm not going to take credit for other people's work, and don't like when people take credit for mine. That being said, props to Harlan Carvey for *Windows Forensic Analysis* from Syngress Publishing, Inc. (http://www.syngress.com), Frederique B. for her contribution (and reminder that editing the registry can have disastrous results), and my brother Shean T. for pointing out it was a challenge (the gauntlet had been thrown down) and without whose help I could not have fought the evil. Special props go to my wife Sonya for putting up with my temper tantrums when the going got rough.

**BBWolf**

*And to think that all of this came simply from browsing to a hostile website. We think your letter may have just scared the hell out of people who don't have your determination, technical prowess, or support network. Most of this crap can be avoided by never opening unknown email attachments, only running programs whose point of origin you know and trust, and never ever clicking on pop-ups, especially the kind that tell you you have a virus. If you set up your system properly and use a decent browser, you should at least get warned before something potentially risky takes place.*

**Dear *2600:***

I recently transferred to a new college. They had claimed to have a very open "anti-censorship" policy in the school's library. Supposedly. As the librarian explained (on Internet access), "we aren't trying to keep you from viewing any material online." There was an exception for pornography, which would almost certainly get you kicked out of the library. Naturally, the first site I attempted was 2600.com. Three windows came up from Trend Microsystems letting me know that this site was blocked due to it being labeled a "Malicious Site." Curious. (On a side note, the IT admin had *not* bothered to block 207.99.30.226. *Lazy.*)

There was a form to submit incorrectly blocked sites, but it consisted of nothing more than a form used to report more sites as "threats." I decided to get IT's contact information and deal with them directly. I honestly didn't see it turning out too well, and having my cover blown as a hacker was not high on my list, but blocking 2600.com in the library was wrong and someone had to do something about it.

I thought it through and came up with a list of *2600's* good points. That at its heart is raw education. I gave reasons why *2600* should be available to students, and also how it is not a malicious site or organization. I kept it to the point and professional. The next morning (very quickly), I got a reply. His response: 2600.com had been labeled as malicious by mistake. This problem was to be fixed immediately. The URL should now work in the school's library. True to his word, it came up without having to type in the IP address.

I guess my reason for writing in was to say that we cannot always accept defeat. But retaliation is not generally the best option, either. Asking questions will often get you much further than some more direct approaches. And sometimes, often, that is all it takes. 2600.com is banned for some reason at many higher learning institutions. And it still would be here too, if facts and logic were not inserted into the equation, and a simple question asked. *Why?*

So I will not need to post the name of my college now, as the problem has been fixed. And before you write to *2600*, angry that you can't log onto the website, take a few minutes and talk to the people in charge. It's amazing how sometimes all it takes is a little education as to what *2600* is. The term "hacker" can be a powerful word and certainly work against you when dealing with the wrong people (especially IT people).

**ghost**

*Thanks for asking the question and hopefully inspiring many more to do the same.*

## *The Last of the Queries*

**Dear 2600:**

This is totally off the wall, but is the name of the magazine typically said "twenty six hundred" or "two thousand six hundred?"

**Feathered Serpent**

*We find that people in the U.K. tend to say "two thousand six hundred" while the rest of the world says it the way we do. We don't pretend to understand this.*

**Dear 2600:**

I recently purchased a copy of *The Best of 2600: Collectors Edition* from Amazon. My question is, is there a difference between the *Collectors Edition* and the regular edition? I was sent the wrong copy by the seller. Is there anything else to the *Collectors Edition* besides the CD and the different cover? My attempt is to contact the seller and obtain what I had paid for, hopefully.

**Wes**

*In addition to what you've mentioned, there's also a special fold-out page with every one of our covers from the beginning to when this book was published, which is a pretty neat thing to have. Each of the collectors books is also individually numbered, in case that sort of thing is appealing to you. You definitely should get the version you ordered, so please pursue that.*

**Dear 2600:**

What is your PayPal address? I picked up a copy of *2600* without paying and I would like to pay for it.

**Jack**

*That's quite considerate of you. Simply send it over to orders@2600.com.*

**Dear 2600:**

Before I submit, I was wondering if you have published Tahiti payphones before?

**m**

*Even if we have, it doesn't mean we can't do it again. Please submit.*

**Dear 2600:**

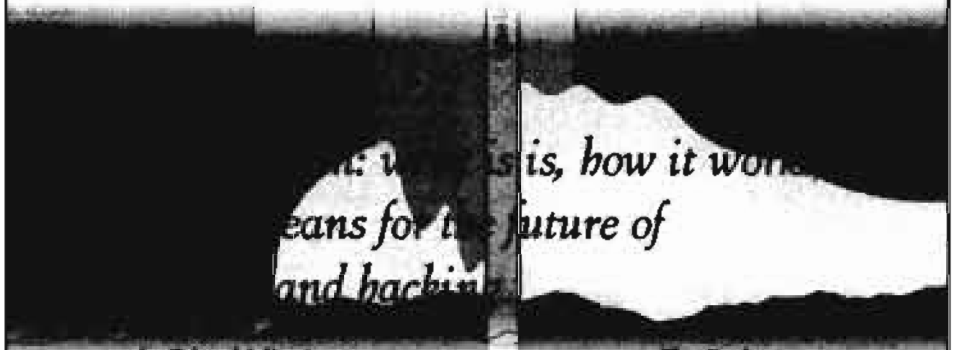
Hello. My name is mohsen, I'm a student in software engineering, I want write an article for *2600 Magazine*, what should I do? Please guide me.

Thanks.

Best Regards.

**mohsen**

*Every few days, like clockwork, you send us one of these queries. You have, in fact, mastered the true art of hacking, which involves persistently trying something over and over again until it works. You might be trying this for a long time, though. We hope you'll just send us the damn article already.*



**by Triscal Islington**

As a bit of a preamble, I'd like to say a few things. Firstly, I'm not an expert on the subject of electromagnetic radiation interception, just a curious mind and a hobbyist. Secondly, there is not a lot of easily available information on enacting an EMR interception breach, and so you'll find the article below to be primarily based in theory.

### The Basics

Known by many names–Electromagnetic Emanation Interception, Van Eck phreaking, TEMPEST–the concept of electromagnetic (EM) radiation interception is relatively simple. When an electrical signal is passed down a cable or through circuitry, it gives off a weak electromagnetic wave. Normally this is so weak as to be negligible. If it wasn't, you'd get all sorts of interference and cross-talk. However, just like any wave, you can pick it up with the right antenna (a big one) and decode/display it with the right equipment.

This type of intrusion can be especially dangerous because it targets weak points that can be especially revealing. By monitoring the EM waves of a monitor, one could see, in real-time, everything that monitor is being sent. Perhaps you want keystrokes? Just analyze the waves coming from the USB or PS/2 cable of the keyboard. The more complex the system, the harder it is to decode. A VGA display uses a fairly simple form of transmission compared to a twisted pair Ethernet cable, but that doesn't make decoding the ethemet impossible. It might be difficult or impossible for you to do in your own home, but the US government is already doing it and I'm sure others, like my own Canadian government, are doing so as well.

What's worse is that this form of monitoring is completely passive, and therefore nearly undetectable (unless, perhaps, if you were using the same technique to sniff out any would-be attackers). You see, EM interception is just that, interception. They're simply pulling waves out of the air that are already there. They are not broadcasting anything, nor interfering in any way with the target equipment.

### What can I do to stop it?

The most effective way would be to put your computer into a lead-lined bunker hundreds of feet underground, but adding EMR shielding to your computer's weak spots is much easier. Anything that gives off EM waves is a potential leak, but cables are the easiest to exploit and the easiest to protect.

There are plenty of options out there, and anyone who has had experience defeating electromagnetic interference will be in familiar territory. Otherwise, just look up EMI shielding. Normally this is used to prevent one device's EMR from causing undesirable effects on nearby devices, but it works just the same in keeping those waves from being spied on.

While doing this, you may also want to look at other potential forms of nonstandard data leakage. I've heard that it is sometimes possible to derive rudimentary data from your computer's grounding. Meaning that, for example, someone could detect keystrokes from anywhere on the same circuit by analyzing the ground wire.

Regardless, I'm sure there are many ways of remotely monitoring a computer's emissions, but it's likely that some good shielding on your weakest points will do the job. You could also give Tinfoil Hat Linux a try.

### I want to do it myself!

The technology involved is not altogether complex, so some types of EM interceptors are possible to build on a hobby budget and the software to use them is starting to appear online. The Eckbox project offers specs on building the hardware as well as a nice open source program to analyze those results. The project is simple enough to build and I hope that the open source software will yield some interesting modifications to the project over the coming months and years. Just head over to their site for the software and for specs on the hardware: `http://eckbox.sourceforge.net/`

If you're the type of person who is interested in building this stuff for yourself, I'd recommend reading up on more regular forms of transmission first. Learn how radio waves work, then build a rig that will let you pick up radio transmissions on your computer. That type of setup is not far off from what you'd need to intercept other forms of transmission. Perhaps trying picking up TV signals and, when you're familiar with how that works, move to an old VGA monitor (older is often better, as they have less shielding).

### The Future

As a longtime fan of hardware hacking, radio technology, and computer programming, I feel that EMR hacking is a great way of fusing "old" hacking and "new" hacking. It's also a great excuse for software hackers to get together with some of the awesome people involved in the transmission hobby world and start pioneering some really neat tools.

Looking to the future? The field of emanation analysis is one that is relatively new for the hobbyist, but I'm sure that the wonderful readers of *2600* will continue to explore this interesting form of computer breach. Personally, I'm really quite interested and I'd love to see how this field can be made more publicly accessible and advance beyond the basics that we can currently achieve.

Thanks to IW4, Arisuki and jefftheworld for their support in my research.

### Further Reading

If you want a quick and dirty way to see the results of EMR, check out this neat app that intentionally causes your computer to emit radiation that can be picked up with an AM radio: `http://www.erikyyy.de/tempest/`

Wim Van Eck, considered an early expert on the subject, has a good paper on the topic that I recommend you read if you're interested: `http://jya.com/emr.pdf`

# THE JOY OF IPv6

**by Sam Bowne**

I am a mad IPv6 advocate. I teach computer networking at City College San Francisco (CCSF), and I am adding it to all my classes next semester. If you want to understand computer networking, you need to learn IPv6. And I recommend that you start soon.

This article introduces IPv6, explains why you need it, and how to get started with it quickly and easily. And, of course, a few tips on hacking it.

### What's Wrong with IPv4?

Most Internet-connected devices are still using the older IPv4 addressing scheme, which assigns each device an address like 147.144.1.212. This translates to a 32-bit binary number, so there are a total of $2^{32}$ possible IPv4 addresses–approximately 4 billion. And that is simply not enough. We have almost 7 billion people on Earth now, and they all need cell phones, iPads, RFID tags in their shoes, and, soon, WiFi-enabled Google brain implants. Various tricks like Network Address Translation have been used to stretch the inadequate IPv4 address space, but they are not sufficient to allow the Internet to grow as it must.

The IPv4 address space is almost completely full. At the time of this writing, only 16 "/8" address blocks remain of the original 256, and they are expected to be all allocated during 2011 or 2012[1]. After that, no more fresh addresses will be available, and people will be reduced to buying used addresses from other, smarter, companies who already switched to IPv6. CCSF has an entire class B allocation, by the way, and my current asking price is $1 million. Call me.

### IPv6: The New Frontier

So IPv6 was created. IPv6 addresses are longer and written in hexadecimal notation, like this: `2607:f128:0042:00aa:0000:0000:0000:0002`

Omitting unnecessary zeroes makes the address easier to write: `2607:f128:42:aa::2`

This address has 128 bits, so there are $2^{128}$ of them, which is more than 256 billion billion billion billion. That is a lot more sensible–an addressing scheme that has enough room to accommodate all the devices we expect to create for centuries, even if Moore's Law continues that long.

### Is This Just Hype?

Until a few months ago, I thought we could safely ignore IPv6, because we could continue to stretch IPv4 with NAT and also re-purpose the reserved class D and E addresses for general use. But I was wrong. ARIN, the organization that controls IP addresses, has announced that they will not use class D and E addresses to prolong the life of IPv4—when the addresses run out in 2011 or 2012, it's GAME OVER. Imagine inventing some awesome new gizmo like heads-up Internet sunglasses or a holographic game people play with tattoo-implanted OLED displays, manufacturing 50 million of them, and finding out that you cannot connect them to the Internet because the Internet is full.

The Dept. of Defense converted to IPv6 in 2008, after years of planning and preparation[3]. The rest of the US government will complete their conversion in 2012[4]. Google is on IPv6 at `http://ipv6.google.com/`, and Facebook is at `http://www.v6.facebook.com/`. IPv6 is mandatory. Ignoring it will only make you obsolete. You might as well stick to your 300 baud acoustic coupler.

### How to Get Started with IPv6

Most ISPs don't offer IPv6 for home customers yet. So you are probably limited to IPv4 right now. But just because your ISP is not ready yet, that's no reason for you to wait. You can use IPv6 immediately over any network with a tunnel–sending IPv6 packets inside IPv4 packets.

I have used three free tunnel brokers for this purpose. The simplest and easiest for Windows users is `gogo6.com`. If you want to try other services, these tips may help:

- `Sixxs.net` has a package called AICCU available for OS X, Linux, and Unix, but the Windows GUI version does not work with Windows 7–you have to use the older CLI version.
- `Tunnelbroker.net` provides tunnels, but they use protocol 41, which is neither TCP nor UDP and is blocked by most home routers.

### Fun and Games: IPv6 Certification

Hurricane Electric has a series of certification tests to show proficiency with IPv6. These are fascinating, challenging, and fun! You get a badge (see figure 1) and even a T-shirt if you make it to Guru level. Here are the levels:

*Newbie:* Knows basic facts about IPv6.

*Explorer:* Has the ability to connect to servers via IPv6.

*Enthusiast:* Has a Web server delivering pages over IPv6.

*Administrator:* Has an SMTP server that accepts mail over IPv6.

*Professional:* Has reverse DNS correctly configured for the IPv6 address of your SMTP server.

*Guru:* Nameservers have AAAA records and can be queried over IPv6.

*Sage:* Has IPv6 Glue.

Certificate of Completion

[illegible]

hereby attains the rank of

Sage

Hurricane Electric
IPv6 Certification

Every company will need to perform these tasks within the next few years. I learned a lot getting these certifications–I had not even heard of "Glue" records before.

### Privacy Risks in IPv6

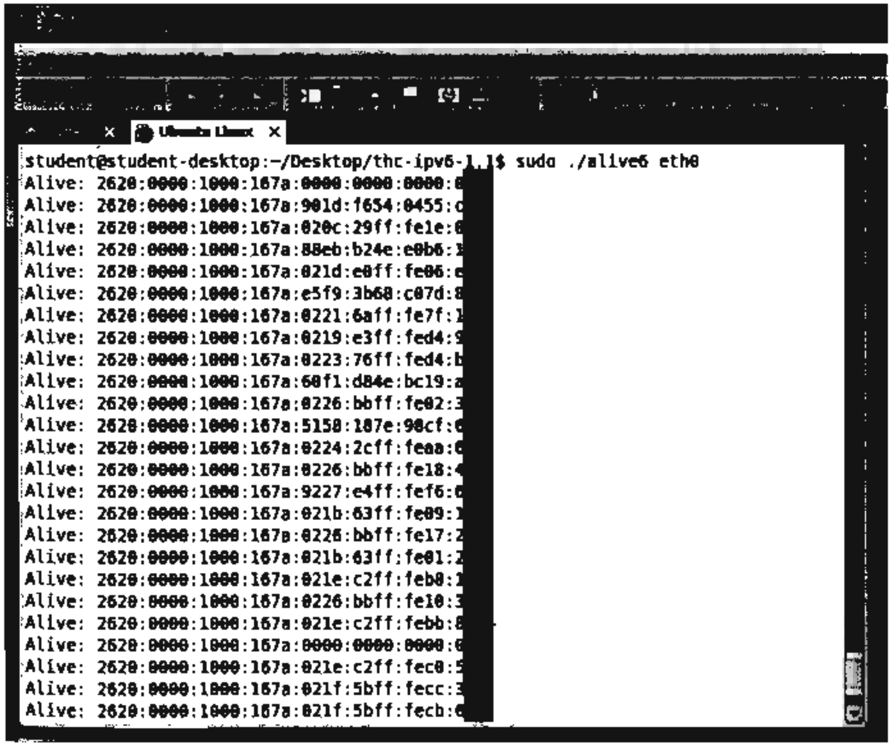
In IPv4, most people use private IP addresses which are translated to public addresses shared by many people. So if you do something naughty, like download copyrighted music, it's not easy to prove who did it. But in IPv6, the MAC address of your interface is included in your IPv6 address, unless you implement "Privacy Extensions". Windows, however, uses "Privacy Extensions" by default[5].

### Hacker's Toolkit

THC-IPv6 is available from `http://freeworld.thc.org/thc-ipv6`, and includes a nice suite of hacking tools for IPv6. I went to a conference where they provided a native IPv6 wireless LAN, and scanned it. I found 30 hosts, as shown in figure 2. For instructions to help you install THC-IPv6 on Ubuntu Linux, see ref. 6.

### Other IPv6 Hacks

Most security devices are not yet IPv6-capable. That makes it open season for people who are ready to use it. You can run bittorrent over IPv6, which will probably bypass any traffic shaping, Deep Packet Inspection, or security devices in your way[7].



```
student@student-desktop:~/Desktop/thc-ipv6-1.1$ sudo ./alive6 eth0
Alive: 2620:0000:1000:167a:0000:0000:0000: [redacted]
Alive: 2620:0000:1000:167a:901d:f654:0455:
Alive: 2620:0000:1000:167a:020c:29ff:fe1e:
Alive: 2620:0000:1000:167a:88eb:b24e:e0b6:
Alive: 2620:0000:1000:167a:021d:e0ff:fe06:
Alive: 2620:0000:1000:167a:e5f9:3b68:c07d:
Alive: 2620:0000:1000:167a:0221:6aff:fe7f:
Alive: 2620:0000:1000:167a:0219:e3ff:fed4:
Alive: 2620:0000:1000:167a:0223:76ff:fed4:
Alive: 2620:0000:1000:167a:60f1:d84e:bc19:
Alive: 2620:0000:1000:167a:0226:bbff:fe02:
Alive: 2620:0000:1000:167a:5150:187e:98cf:
Alive: 2620:0000:1000:167a:0224:2cff:feaa:
Alive: 2620:0000:1000:167a:0226:bbff:fe18:
Alive: 2620:0000:1000:167a:9227:e4ff:fef6:
Alive: 2620:0000:1000:167a:021b:63ff:fe09:
Alive: 2620:0000:1000:167a:0226:bbff:fe17:
Alive: 2620:0000:1000:167a:021b:63ff:fe01:
Alive: 2620:0000:1000:167a:021e:c2ff:feb0:
Alive: 2620:0000:1000:167a:0226:bbff:fe10:
Alive: 2620:0000:1000:167a:021e:c2ff:febb:
Alive: 2620:0000:1000:167a:0000:0000:0000:
Alive: 2620:0000:1000:167a:021e:c2ff:fec0:
Alive: 2620:0000:1000:167a:021f:5bff:fecc:
Alive: 2620:0000:1000:167a:021f:5bff:fecb:
```

Rogue Router Advertisements or DHCPv6 servers can be used to deny service to clients, or to perform a Man-in-the-Middle attack[8]. A single malicious packet sent into a point-to-point link can flood it with echoing "destination unreachable" responses[8]. And "Routing Header Zero" IPv6 packets can be used to create loops and amplify traffic to perform a Denial of Service attack[9]. Patches exist for these known attacks, but there will be many more found as IPv6 deployment progresses.

### Altar Call

The End Is Near! Don't bury your head in the sand–get on board the IPv6 train now! There's a lot to learn, especially since we will all need to use both IPv4 and IPv6 for at least a decade. And the boundary between the two systems will be a natural weak spot, where exploits will be found and defeated. You may choose to ignore IPv6, but your enemies won't. People who start now can become experienced professionals, ready to help others when the chaos of rushed transitions begins.

### For More Information

An excellent source for starting out with IPv6 is "IPv6: What, Why, How" at `http://➥www.openwall.com/presentations➥/IPv6`. The book "IPv6 Security" by Scott Hogg and Eric Vyncke is highly recommended by experts–I haven't received my copy yet, so I can't give you my opinion.

If you want to reach me, use Twitter @sambowne, or email `sbowne@ccsf.edu`. Have fun with IPv6!

### References

1. "IPv4 Address Report" `http://www.➥potaroo.net/tools/ipv4/`
2. "Beware the black market rising for IP addresses" `http://www.infoworld.➥com/print/121729`
3. "IPv6 in the Department of Defense" `http://www.usipv6.com/ppt/IPv6Summit➥PresentationFinalCaptDixon.pdf`
4. "Federal IPv6 Transition Timeline" `http://➥www.cisco.com/web/strategy➥/docs/gov/DGI-IPv6_WP.pdf`
5. "IPv6 Deployment on Production Networks" `http://tinyurl.com/37m2cc2`
6. "Scanning for Hosts on IPv6" `http://sams➥class.info/ipv6/scan-google➥.html`
7. "utorrent app now supports IPv6/teredo directly" `http://www.gossamer-➥threads.com/lists/nsp/ipv6/➥15173`
8. "The ping-pong phenomenon with p2p links" `http://www.ietf.org/mail-➥archive/web/ipv6/current/msg➥09661.html`
9. "RFC 5095: Deprecation of RH0" `http://www.rfc-editor.org/rfc/➥rfc5095.txt`

## DORMITORY PHISHING

I work as a student staff member in the dormitories of a large university, and one of my female coworkers was recently threatened by a resident. She got a nasty Facebook message with gender, racial, and personal slurs along with some "watch your back" type stuff. Housing (our employer) hung her out to dry: they weren't willing to do anything for her safety. I decided to step in and offer my computer skills to help trace the culprit. In the end, he wasn't found and she quit for her own safety, but I'm saving the tool for any future incidents.

The threat came in the form of a Facebook message from a newly created account. Facebook doesn't divulge information about accounts, so I had to trick the culprit into giving himself away. I decided to phish him out.

To begin, I installed the Tomcat server on my laptop, and set up a new folder called html to hold the JSP and servlet files. My university has a central authentication service that all students use to log in to various network resources. I copied the source code of the login page and made a duplicate on my server. CAS has a "digital thumbprint" on the login page that, on close inspection, is missing on my version of the page, but the difference is not obvious to the casual user.

I wrote a Java servlet to take the login data and record it to a text file. It also records the IP address of anybody who even accesses the page, just in case the culprit chickens out before logging in. We could have tracked the computer with just the IP address, but with the login information we could do all sorts of malicious "administrative" tasks, like drop the user from all their classes or order them 100 transcripts. Or turn them in.

The way that the dormitory network is set up is such that only somebody in the local physical area could access my server, since I can't access the network routers and set up port forwarding. This meant that the culprit would have to be in his room to reach the fake login page, and that any authorities searching for the server (from their offices) couldn't find it. Neat.

The general plan was to reply to the Facebook message with a link to the fake login page, and entice the culprit to click on it and hopefully "log in." The Facebook message was the weak link in the plan. I had heard about the problem three days later, and it took me another three days to develop the solution and test it. By the time I could deploy the server, the Facebook account was deactivated, and we couldn't send him the message.

I'm saving the files for the next time something like this happens. If Housing won't take care of us, then the least we can do is to look out for one another. I've got your back.

# How to Find Information on People Using the Internet

by DarX

Have you ever tried finding information on someone through the Internet? Whether it be for revenge (cyber attack on a personal webspace of some sort), or to see how much information YOU are putting out on the Internet, knowing your way around is very important.

First, let's analyze who can be easily (and I mean very easily) found on the Internet. Information on someone will be abundant if the person:

- Uses their real, full name on the Internet to identify themselves.
- Publishes documents and/or scientific papers under their name.
- Posts their information on several different sites (forums, blogs, etc).
- They're famous–duh.

If you have a name:

- Look for a Facebook or MySpace page. If they have one, create a dummy account as the opposite sex with a good looking picture and attempt to get them to add you as a friend. Use excuses like, "I was just profile jumping and thought you were cute." Use your imagination, because being an accepted friend can lead to a TON of information. If you can't get to them directly, see if you can add one of their friends. They are more likely to accept you with a common friend.
- Google the name and see if they have posted in any forums/blogs under their own name. From here, you might be able to get an e-mail address and, if you integrate yourself into the forum/blog, you'll be able to post a little, gain some reputation, and maybe add them on an instant messaging application or begin exchanging e-mails.
- Do a whitepages search online. This will turn up an address and usually a telephone number.
- If the person has committed an offense, you might be able to find them through `http://www.➥familywatchdog.us/Show➥NameList.asp`

If you have a phone number:

- Doing a reverse phone lookup online, you'll be able to get the location of the person and which cell phone provider they use. Most cell phone companies will not release the name or any other information on the person in question, so this will only give you the location.
- You can also simply try Googling their phone number to see if it comes up in any cell phone directories. There are services that charge a fee, but that will pull a significant amount of information from private databases. This might be an option if you want to spend the cash.
- Call it! If you can find a reason to call (random city survey, etc), and they decide to talk, you can get a lot of information out of them.

If they have a website or blog:

- Any domain name must be registered to a person or company. Some people are smart and register anonymously, others, however, use their full contact information. Try a whois (`http://www.whois.net/`) and see if their information is listed.
- If they have a personal blog, chances are they mention their name and some other contact info as well.

If you have their e-mail address:

- An AMAZING e-mail lookup service is Spokeo (`http://www.spokeo➥.com/email`). Simply enter their e-mail and you can find a ton of information on them, including IP addresses.

Using combinations of these, and your own intelligence, I'm sure you'll be able to make a full portfolio about anyone you can think of. I'm thinking of making another article on how to leave absolutely NO traces of who you are on the Internet. That will come soon. Until then, have fun and don't forget to visit my blog at `f33r.com`. Out.

# Transmissions

by Dragorn

## The Great Firewall of... Dot-com?

A government institution determines that a website contains unacceptable material, and blocks access to it from within that country. Smells like censorship, but for the sake of argument, let's (briefly) say that controlling what is acceptable is the government's job, and not just for Big Red. Australia does it, and "first-world" countries around the world are working on doing it.

Now consider: A government institution determines that a website contains unacceptable material, and blocks access to it from the Internet at large by hijacking the DNS records. But even this, maybe, has an explanation. Obviously a government ultimately controls what is considered valid within its assigned domain name space. Libya is welcome to enforce whatever standards of conduct it feels like, holding domain shortener vb.ly in violation of Islamic law by shortening URLs that may contain offensive material.

But what if the domain was a dot-com address, one of the great three top-level domain trees, registered outside of the nation in question, and was seized without notification by an organization chartered with defending the nation against underwear bombers?

That's right; the Department of Homeland Security, or more specifically, the ICE (Immigrations and Customs Enforcement), the people responsible for policing the borders, or (from the ICE website) "ICE's primary mission is to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration," apparently now has the power to override registrations in the dot-com (and one might assume other top-level DNS) trees hosted in the United States.

The ICE is responsible, among other things, for preventing the import of counterfeit goods. In a recent takedown of 75 domains, the ICE shut down what would appear to be 71 websites hawking counterfeit handbags, golf equipment, and sports jerseys - and four sites about sharing links to rap music and torrents.

And, of course, it gets even better: The torrent site doesn't even *run* a tracker, *and* doesn't host torrent files. It's a torrent search aggregator, which loads results in iframes. It's *not even scraping results*. The only action it's taking is replicating a FORM POST action.

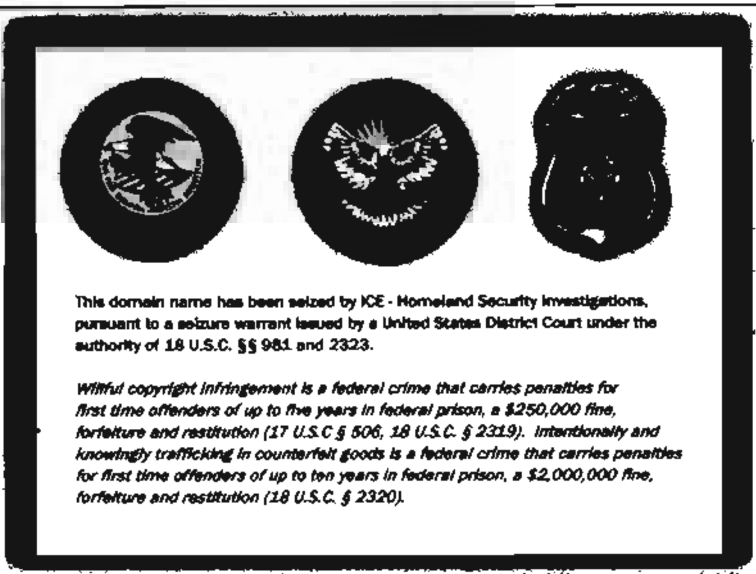
We're not just looking at the slippery slope, we're tobogganing down it trying to dodge pine trees and plastic Santa decorations. With no prior notification, the ICE is taking down websites which arguably do not fall under its jurisdiction, and which do not contain infringing material, or even, arguably, links to infringing material. Of course, it *is* still a site which most people would label a bad citizen, reducing public outcry and complaints, truly the best of all slippery slopes.

Assuming that the website distributed copyrighted material (it didn't) or encouraged it by linking it (it doesn't), it may fall under the purview of the ICE under some odd interpretation of "import" or "counterfeit," but really it just feels like the MPAA has their hands in Uncle Sam's pockets again. The whole thing seems even more suspect in light of Senate Bill 3804, the Combating Online Infringement and Counterfeits Act.

The COICA would call for redirecting DNS records, banning ad services, and preventing any financial transactions (i.e., credit card payments) originating from U.S. addresses, to any site the government declares supports piracy (literally, "no demonstrable, commercially significant purpose other than sharing copyrighted files").

The COICA does not provide any obligation for killing the domain name records outside of the United States, but for domains registered under ICANN (i.e., dot-com), it would seem unlikely that they'd be allowed to persist. Domains squashed by ICE have been redirected worldwide, regardless of the legalities of the site in the owner's or operator's home country, and, bizarrely, regardless of where the server is located: As of the time of writing, torrent-finder.info still functions, and resolves to a server hosted in Texas. The seizure affected the DNS entry only, not the actual server, despite the server (apparently) being located within the jurisdiction of the United States.

So far, the COICA has passed unanimously through the Senate Judiciary Committee, however, at least one senator has pledged to block the bill through the end of the current session, after which the new senate takes over. But if the ICE has the ability to blacklist sites worldwide, why do we even need the COICA?



This domain name has been seized by ICE - Homeland Security Investigations, pursuant to a seizure warrant issued by a United States District Court under the authority of 18 U.S.C. §§ 981 and 2323.

*Willful copyright infringement is a federal crime that carries penalties for first time offenders of up to five years in federal prison, a $250,000 fine, forfeiture and restitution (17 U.S.C § 506, 18 U.S.C. § 2319). Intentionally and knowingly trafficking in counterfeit goods is a federal crime that carries penalties for first time offenders of up to ten years in federal prison, a $2,000,000 fine, forfeiture and restitution (18 U.S.C. § 2320).*

The problem is not that the ICE isn't acting within its charter. Let's say that it is, at least, for the context of websites selling counterfeit products. The problem is that the ICE is also targeting websites which technically have no infringing aspects, and there is no (or at least, none that I could find) publicly known method for redressing mistakes, recovering domains, or even pleading the case in court to present the other side of the argument. Armed with an indisputable court order, the ICE can, in theory, seize any website in dot-com, no matter where in the world it is registered or hosted.

The ICE is able to enact these restrictions on the top-level domains because the U.S. still retains sole control of ICANN, the Internet Corporation for Assigned Names and Numbers. The ICANN is responsible for defining the top-level domains worldwide, dispensing IP address blocks, and controlling the main root DNS servers. ICANN is a relatively new organization (1998) and takes direction from public meetings held around the world, but is still fundamentally a United States construction: It retains ties to the U.S. government, and operates from within the United States. The top-level domains like dot-com and dot-net are handled entirely by U.S.-based corporations (Verisign).

In 2009, the European Union repeated a call for ICANN to cut ties with the U.S. government, and become an international entity under control of the G-12 (the twelve most economically powerful countries). This doesn't seem like much of a solution, either. What better way to paralyze the Internet at large than submitting it to the control of representatives of a dozen countries, with different laws and different interpretations of copyright. Unfortunately, there doesn't seem to be much of a solution: Leave control of the core Internet services under one country, subject to the whims of that government in the name of "preventing piracy," or give control to a dozen competing nations and hope they fight each other enough to prevent any significant harm from being done. Or, of course, they could all adopt ACTA, the secret closed-door trade agreement with just about every poorly planned reactionary policy about Internet use, and we'll all be screwed.

The real questions at the end of the day are: When will the United States exercise this top-level kill against websites again, what recourse do international (or even domestic) site operators have, and how can we prevent "stopping piracy" from turning further into "stopping any technology which might have dual-use?" We've already lost unencrypted cable and unencrypted video and audio between components, forcing independent technologies like Tivo to license with specific providers and leaving customers of some providers with no choice at all. We've already lost streaming video between arbitrary devices and, if the content providers behind the "stopping piracy" bandwagon have their way, we'll lose the ability to play one copy of a video on multiple devices - because obviously, playing it on a TV and a laptop means we should buy it twice, right?

Blocking content is censorship, and once it becomes easy for a government to censor some content, it becomes easier to censor more and more content. Wax up the skis, make some hot chocolate, and get ready to dodge some pine trees. The slippery slope awaits.

# Fun with FOIA

by BY3M@N

Any fans of the general concept of freedom within the government should thank their lucky stars that there were some forward thinking individuals in the U.S. government a few decades ago. Those guys came up with the concept and implementation of the Freedom of Information Act (FOIA, pronounced "FOY-A"), in 1966. While a disheveled President Johnson would have killed the act if he had a snowball's chance in hell, Congress shoved it through the political process like a ramrod. And it has stuck out of the government's rear-end ever since, modified and jiggled around a bit with every presidential administration since.

## The History

If the U.S. government has created information, you have a right to see it (with certain exceptions... nine to be exact). Records can be ambiguously construed as audio files from certain government agencies (air traffic control and NORAD voice recordings from September 11, 2001), graphic illustration training aids (pack of playing cards with Soviet-era tanks for recognition), warning stickers for biohazard materials (on VX nerve gas rockets), and police blotter reports (physical attacks and arrests at any forward-operating bases in Iraq). While proponents of the law give the impression that every loyal American is using FOIA to search out the "truth," the truth is very few red-blooded Americans are actually using it (just like the percentage of voters in local elections–always LOW). Some common users:

- Companies trying to get a leg up on competitive contracts.
- Legal agencies representing commercial companies, trying to do the same.
- Authors, looking for sweet nuggets of cover-up truths (Roswell, anyone?)
- Old fogies, searching for info on their war service.
- Nutcases, looking for UFO and Area 51 information.

While some of the above had minor successes (or major successes, with enough lawyers), FOIA can be used to uncover bits and pieces that government drones would rather keep locked up. A few of the pieces freed up:

- Acknowledgement of Project Moon Dust, U.S. Air Force plan for retrieval of objects of unknown origin (reading between the lines: UFO parts).
- Specifics on a post-nuclear communication system called GWEN. Cancelled in the 1990s, the system was designed to use antennas from AM radio stations (DJs being long dead, of course) to broadcast emergency action messages to whatever forces were still alive. It was also rumored to be used for some mind control experiments. But I have no idea what they were talking about... `MIND:> Del *.*`
- Class syllabi for the next-generation U.S. government cyberwarriors. Apparently their first "step" in the training is to be Security+ certified. Makes you feel safe about the state of the Internet, huh?

## Starting Point

It seems simple to write a FOIA request, but in actuality it's even EASIER than that.

1. Have an idea of what you want to request. Simple or complex, start with an idea. One of the funnier requests I've seen is the cafeteria menu from the National Security Agency. Actually, it was one menu, from the 11 eating establishments at Fort Meade. Plenty of good hacker grub available, if you can avoid the salad bars and low-cal drinks... and the 20,000 government employees and agents.
2. Write the request down. Extend your carpal tunnel syndrome and write up a request. Computer, paper, napkin, matchbook cover–it doesn't matter. Just make sure it mentions FOIA and whatever you're looking for (see sample FOIA letter below).
3. Send it. This used to mean paying for those Postal Service "stickers" and waiting months for a reply. Now, most agencies have electronic FOIA submission, and can reply by email if they have what you're looking for. Using a "vanilla" email account and anonymizing web browser is level 3 privacy protection. But if you're really paranoid (and who isn't nowadays?), get someone else to place the request. (Little brothers and sisters everywhere: unite and charge a fee!)

## Pitfalls (and not the Atari version)

According to the government, freedom isn't free. It will cost you, but, depending on each agency's interpretation, you might get something for nothing. The Department of Defense has a fee floor of $15, meaning if the cost of your request is less than $15, they don't charge. There is no ceiling, however. So if you ask for "ANY records concerning ELIGIBLE RECEIVER" (Google it... you won't be disappointed), they could give you every scrap of paper, at the cost of $0.15 a page, creating a huge FOIA fee.

Also, most FOIA agencies will try to bully you for an e-mail address and phone number. You do not HAVE to provide these. And usually, when you do, they actually call and ask questions. Questions are bad, so don't give them the opportunity to ask them. Most are happy to correspond through the postal service, so be sure to have that "mail drop" ready. If you want to provide a number, for some crazy reason, buy a TracPhone for $10 and provide that throwaway number.

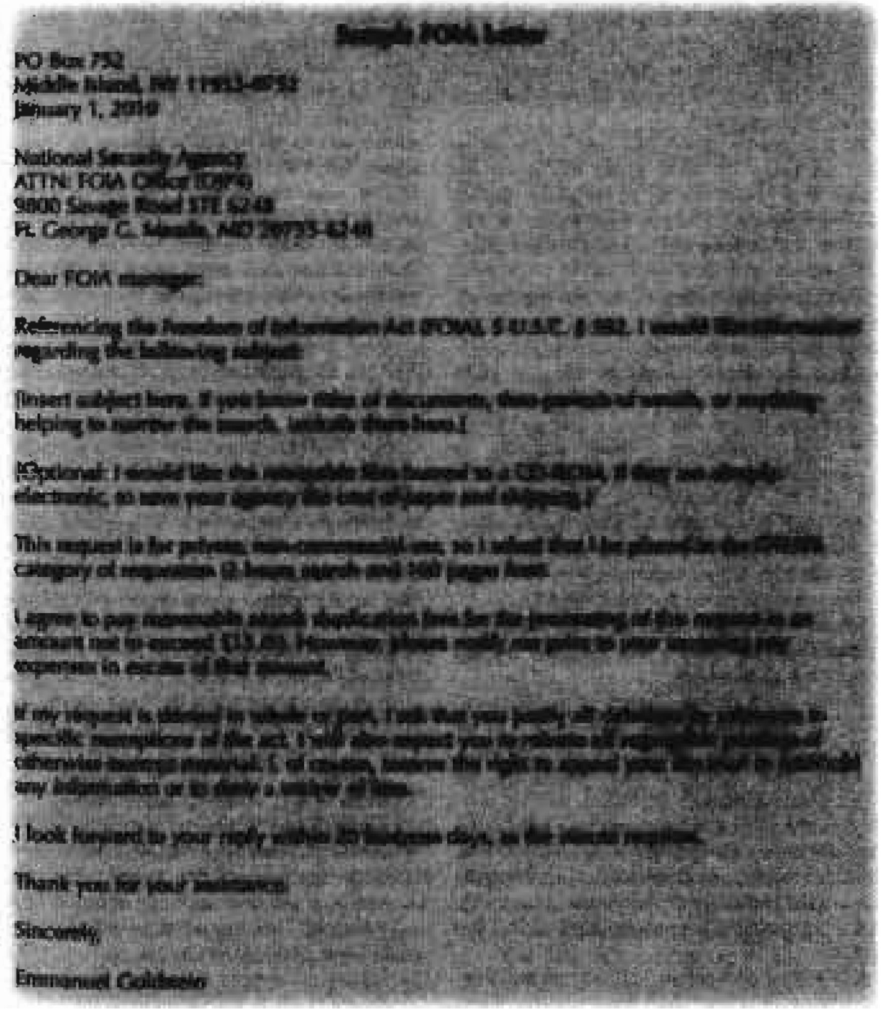
Finally, privacy being what it is in today's world, your name and address will be attached to a FOIA log kept at each agency. You can use FOIA to request these logs, and the agencies are supposed to redact (cross out) your information (Privacy Act or some nonsense like that). But it's a big machine, and some drones just don't get the memo. That's why the mail drop is a good idea. Grandparents, old neighbors, and crazy people in the neighborhood who will prostitute their address for a couple of bucks are priceless.

## Bottom Line

You pay taxes (at least, most of us do). The government does its work (No work? Little work?) with that money. Find out where it goes. You should be able to see what they do with it. There's a mechanism to view the inner workings of the machine, if you know how to navigate the system.

FOIA is a system. Hackers hack systems. Try, and you'll be surprised what you find.

Examples of successful FOIAs are at `http://www.theblackvault.com/`, `http://www.thememoryhole.org/`, and `http://www.governmentattic.org/`



Sample FOIA Letter

PO Box 752
Middle Island, NY 11953-0752
January 1, 2010

National Security Agency
ATTN: FOIA Office (DJP4)
9800 Savage Road STE 6248
Ft. George G. Meade, MD 20755-6248

Dear FOIA manager:

Referencing the Freedom of Information Act (FOIA), 5 U.S.C. § 552, I would like information regarding the following subject:

[Insert subject here. If you know titles of documents, time periods of records, or anything helping to narrow the search, include them here.]

[Optional: I would like the releasable files burned to a CD-ROM, if they are already electronic, to save your agency the cost of paper and shipping.]

This request is for private, non-commercial use, so I asked that I be placed in the OTHER category of requestors (2 hours search and 100 pages free).

I agree to pay reasonable search/duplication fees for the processing of this request in an amount not to exceed $15.00. However, please notify me prior to your incurring any expenses in excess of that amount.

If my request is denied in whole or part, I ask that you justify all deletions by reference to specific exemptions of the act. I will also expect you to release all segregable portions of otherwise exempt material. I, of course, reserve the right to appeal your decision to withhold any information or to deny a waiver of fees.

I look forward to your reply within 20 business days, as the statute requires.

Thank you for your assistance.

Sincerely,

Emmanuel Goldstein

# Hotel iBAHN SiteKiosks and How to Pwn One

**by Sandwich**

The company iBAHN produces hotel computer kiosks that provide travelers with public computer access while abroad. These kiosks allow you to access various applications (Word, Excel, etc.), Internet (via their custom browser), Skype, and Pinball/Solitaire, for a nominal fee. Why someone would pay to play Solitaire on one of these things is beyond me. This article is about one such kiosk, found at a Best Western in the UK.

The one I visited was locked down a la Alcatraz. Thanks to software called SiteKiosk, context menus were banned, system dialog boxes were banned, and Ctrl+Alt+Del was banned. Of course, unpaid access to domains outside their internal whitelist were also not allowed, resulting in a prompt to pay for access to what you requested.

At first glance, it felt like one of the more solid interfaces I'd seen, given the flexibility of apps that could run on it. However, there's always a loophole. You just have to find it. On that note, let's browse around on the hard drive, shall we?

There are a few ways to do this, but there's something elegant about doing it via the company's own website:

1. Click the IBAHN logo in the top right (or type in the URL box of an Internet window) to get the `http://www.ibahn ➥.com/` webpage. Their website is whitelisted (free), so you can browse to it.
2. Go to their "Resources" section and choose any PDF. It will load inline in the browser, thanks to the Adobe Acrobat plug-in.
3. In Adobe's PDF plug-in viewer, click the Document icon on the left ("Pages").
4. Click the Options button and click "Print Pages." This pops up Adobe's print dialog, which isn't blocked.
5. In the print dialog, choose the Microsoft XPS Document Writer, then click OK. A "Save the file as" dialog will be presented. Again, this dialog is not closed by the SiteKiosk software.

You can now browse around the hard drive using the filename text box! Use "C:\*.*" to reveal the contents of C drive. You cannot right-click to get a context menu for running anything, but it's interesting to see what's deployed on the machine.

A brief tour around the HD reveals that they are running Windows and have various third-party apps installed, like PC Anywhere (for remote monitoring/control), Altiris (for asset management), SiteKiosk, and iBAHN. Some of these apps have "logs" directories, with curious ones under folders names "CreditCardPayment" and "Revenue." I could not immediately find a way to open and view these files through this interface, but the exploration has just begun.

After a whirlwind tour through the hard drive of an Internet kiosk, sometimes one just needs to just sit back, relax, put their feet up, and get some free Internet access.

In any Internet window, you can enter the URL of the site you wish to access in the address bar. Interestingly enough, the logic used to check if you're visiting one of their whitelisted websites is string based, not IP based. The software scans from the left of the URL for a match. This means that typing a URL of `http://www.ibahn.com@<enter website here>` allows you to get to any webpage, as the logic allows for URLs starting with `http://www.ibahn.com`. However, if you try to access a link on subsequent pages, you will be blocked, unless you manually type the URL of the link in the address bar, using the URL prefix. This quickly becomes a real pain. There's got to be a way around this.

Well, there is! If you can bury a URL in an IFRAME, the parent frame's URL doesn't change, so the SiteKiosk software doesn't pick up on it and block you. So, use the "free" trick to get to Google and do a search for "IFRAME example" sites that show you how to build an IFRAME in HTML, with accompanying samples embedded in the page. Choose your poison and you can navigate freely within the IFRAME! With this in mind, a prepared boy scout would ensure that they set up such a webpage on a free hosting site with an IFRAME that fills the whole screen BEFORE traveling to such a hotel, to give the greatest flexibility at one of these kiosks.

Now to answer a few final questions:

1. *Is there a more comfortable way to browse around through Windows Explorer?* Download a large ZIP file off of the Internet and, while it's downloading, uncheck the "Close this dialog box when download completes" checkbox. Then click "Open" or "Open Folder." An error message will pop up, but a stripped-down Windows Explorer window will open, allowing you to browse around.
2. *How can I open a text file on the hard drive?* Through Windows Explorer via answer #1, find a text file and double-click it. Notepad will open, but SiteKiosk will pick-up on this and immediately try to close it. So, as soon as Notepad opens, quickly press Space to modify the document. SiteKiosk will try to close Notepad on you but, because you modified the document, the "Do you want to save your changes" dialog will keep Notepad open long enough for you to read the contents of the text file.
3. *How can I force a reboot of the system?* Once you've located the Credit Card Payment application on the hard drive, attempt to run the application and the system will reboot. Safe Mode is also protected by the SiteKiosk software with a password, but you can boot off of a USB stick to get around this if you wish to pwn the box.

When I was doing the above, the machine started rebooting any time I started browsing the hard drive. It was quite clear that an administrator was monitoring the box and was issuing reboots via PC Anywhere. An angry admin makes for a bad experience if you happen to meet him or her in person. Just keep that in mind.

So, without further ado, explore these machines, enjoy your free Internet, and don't do anything I wouldn't do!

# RAM Dumping

**by Metalx1000**
**http://www.FilmsByKris.com/**

As soon as your operating system starts to load, the RAM in your computer is already in use. It's storing all the data you see and a whole lot you don't see. You may think, as I used to, that when you close a program, the program and its data are removed from RAM. What you may not realize is that data and information from programs you have long since closed may still be hanging out there.

There are many reasons why someone might want to acquire memory dumps from a system's RAM and use forensic software tools to examine them. A programmer might be checking for bugs in a program, an anti-virus programmer might be trying to dissect what a virus does once it is loaded, or someone might just be curious as to what is going on in his or her computer, to learn about the technologies in use and maybe find ways to improve them.

Whatever the reason for your curiosity on the subject of acquiring memory dumps, I hope that this little article will help you on your way. The steps and tools outlined will hopefully answer some of your questions about what is going on in the part of your computer that you don't normally get to see.

When a program is compiled, many times other files, such as image and sound files, are compiled into it or compressed into package files that are distributed with the program. When the program is started, not only is the program loaded into RAM, but so are the extra files. Remember, everything you see on your screen is stored in your RAM, including the icons on toolbars and drop down menus.

What we need to do is pull all the information from your RAM and put it back on your hard drive, where we can look at it and pick it apart. I'll be describing how to do this on a Windows machine. The tool I like to use to do this is called "Win32dd." Win32dd is a free kernel land tool to acquire physical memory. Win32dd has some similarities to the "dd" command many of you Unix and Linux users are already familiar with. This tool will copy your RAM to one dump file. A dump file is like a complete image of the contents of your RAM. If you are familiar with the image files that dd creates from hard drives, then you should feel pretty much at home with this concept.

I would like to point out that Win32dd is open source and free as in freedom, but the project has been dropped by the creator Matthieu Suiche. Suiche is now working on a similar tool called MoonSols. I do not believe MoonSols is open source, so I have not used it myself. You should be able to obtain a copy of Win32dd with some Google searching.

The way we are going to use Win32dd is simple. After going to the Win32dd site and downloading the zip file, extract the contents to a folder where you would like to keep the data you grab from RAM. There should be four files in the zip file: HELP.txt, README.txt, win32dd.exe and win32dd.sys. Obviously, the first two files are for your reading pleasure. The last two are needed for Win32dd to work.

Once extracted from the zip file, open your command line and move to the directory where you have placed Win32dd. Then run Win32dd as follows:

```
win32dd -d myfile.dmp
```

You can name the dump file anything you would like. Since most new computers have large capacities of RAM, on average ranging from 2GB to 4GB, it could take awhile to download all the data from your RAM to your dump file. So be patient. As they used to say in the old Heinz Ketchup commercials, "The best things come to those who wait."

After you have gotten up and got a cup of coffee, watched some TV, and went to the mail box to check for a new issue of 2600, you can now come back to your computer. When you do, you will find yourself a large dump file that in most cases will be a few Gigs.

What do you do with this file? Well, you run it through a good forensic tool called Foremost to get all the goodies out. Foremost will scan through the dump file and look for files based on their headers, footers, and internal data structures. This is basically what data recovery tools such as "PhotoRec" do when searching for deleted files on your hard drive. This process is called data carving. Foremost can find many common file types. Some, but not all, include: exe, jpeg, html, doc, xls, wave, avi, mpeg, mov, and mp3 files. According to the website, Formost will not only work on dmp files created by Win32dd, but it will also work on standard image files that are created with dd from a device such as a hard drive or flash drive.

Foremost is also free and Open-Source. If you want you can download the Foremost source code from http://foremost.sourceforge.net/. If you do you will need to compile it yourself. If you are a Linux user such as myself, Foremost is most likely already in your repositories and can be installed with a simple "sudo aptitude install foremost" at the command line. At this point either copy the dump file to a flash drive or boot into Linux on the same machine with liveCD or using a duel-booted system.

Foremost is a command line tool. Open up your terminal of choice and navigate to the folder where you stored the dump file. Foremost has a few switches that do different things. Today we are going to look at the "-t" switch. This switch will specify to Foremost what file type you are looking for in the dump file. For example, "foremost -t jpeg myfile.dmp", will search through the dump file and save anything that it thinks might be a JPEG file to a sub folder labeled "output/jpeg". If you want Foremost to dump every file it sees use the command, "foremost -t all myfile.dmp". Foremost will make a folder for each file type it finds.

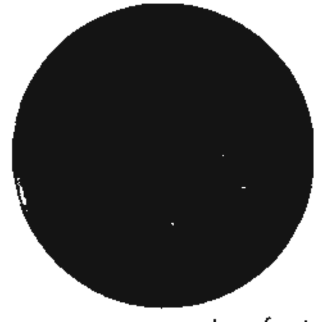
As you look through the files Foremost creates keep in mind that some files may not be complete. Just as when you are saving files to your hard drive you are writing over data that is not being used. You load data to RAM by opening a program, but when you close the program that data may stay in RAM until it is overwritten or the power is cut for a period of time. Some files may get partially written over leaving half a JPEG image or a corrupt MPEG file. This is the same thing that happens to some files that you may recover with PhotoRec.

There will be a lot to go through. Much of it may not be interesting. But, if you take the time to go through it you will find that you could learn a lot about your computer and how it works. You will also have access to media such as videos, icons, images, and sounds that may become useful to you in projects you may be working on.

Proprietary software designers also work really hard to hide things from the end user. They zip things up in proprietary files formats while they are on your hard drive. But, many of these things they hide from the end user have to be unzipped at some point for the program to access them. Many times these items can be found while the program is loaded into RAM. I don't know about you, but I feel that if it's my computer, no one should be hiding anything from me. The only way you can truly have control over your computer is to know the ins and outs of what makes it work.

So, dig and search. Information was meant to be free. The only way we can grow and technology can move forward is to learn and understand how things work now, so we can improve them for the future.

Thanks to Canola for your help.

# WHO'S GOT YOUR  ?

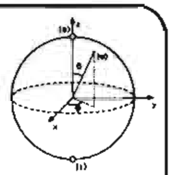
**by windpunk**

Have you ever been asked to petition for something? Someone comes up to you, talks about what they're trying to get passed or stopped, and then they try to get your information. While out shopping one day, some guy came up to me and asked me to petition to get his father into the election coming up. I didn't know if the guy was for real or just looking for information so, to be safe, I did what anyone would do: signed my name and wrote down a second address I use for spam. Of course, my girlfriend signed the petition with the same address. A month or two passed and I found two letters in my mailbox which said "Voter Registration Card Enclosed." I freaked out. How could they know about this address? I opened the envelope, and there sat a new voter registration card for the state of Maryland with the address it was sent to printed on the card as my home address. My real home is outside the city limits, whereas my spam mailbox is in the city. I looked at the bottom of the page and in bold it said "you have been issued a new card because of change of information." I didn't change any information, I hadn't moved, I hadn't gotten one of these cards since I first registered. So I called the number for the voter registration in my area. They asked for my information and told me, "It seems you filled out a petition at the listed address... Would you like to change it?" I was furious. Since when could they take the name from a petition, line it up with a name in the system, and change the address without any authorization, contact, or signature? I told them I wanted it changed back and then they told me that I would have to come to the office to change the address back to what it was, and sign. So my girlfriend and I went down to the office to fill out the form to get our addresses changed back.

I confronted the two people in the office about my problem. I asked one of them, "what would happen if someone put my name down on a random petition with a random address?" She thought for a second and told me that it would be mailed to the address listed. Then she caught herself, and asked if someone had done this to me. Of course I wanted to cover up what I was thinking, (everyone has enemies) so I smiled and told her, "Some people out there may be more devious than others, what keeps them from screwing with peoples' right to vote?" The only thing she could come up with was that they compare signatures to verify a person's identity between a petition and their past voter registration card.

I do not condone any malicious/devious plans, but... it would be possible to add friends, enemies, teachers you didn't like, etc. to a petition (if you can find one going on) and change their voting addresses. The person whose name you write down doesn't get any information about the change at their real address because voter registration thinks they have moved. If you've ever seen how a teacher signs your paperwork, or a friend signs a check, you can get try to get close to what their signature looks like and, with a little playing along with the petitioner, he will think you're legit. Your target, however, will not find out that their address has been changed until they go to their assigned polling place on election day and find that they are not on file. Even worse, they could be signed up with an address in another district, which would mean that the people at the polling place wouldn't even see that person in their systems for the district. Of course this is illegal, so don't do it! This is a flaw in the voter registration system which takes the signature of the voter over any contact with them (phone calls, emails, and letters) for a change of information. This worked here in the state of Maryland, so it may work for you.

# Vulnerabilities in Quantum Computers



**by Purkey**

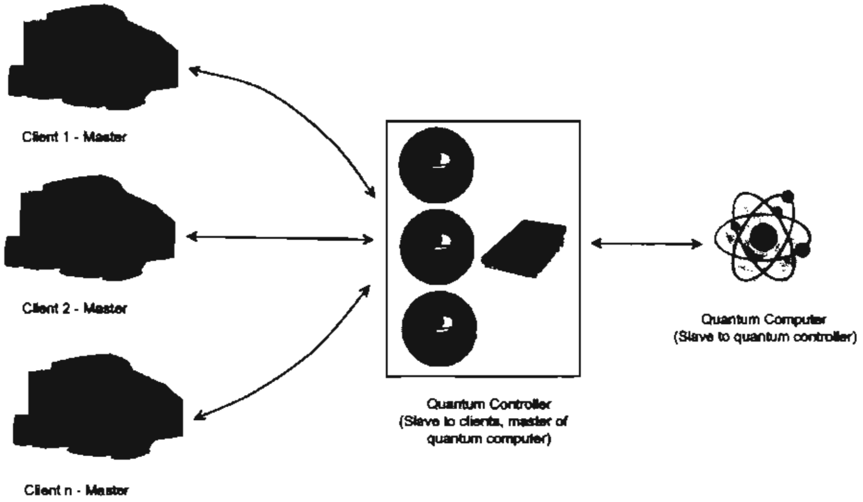
First of all, what is a quantum computer and how is it different from current computers? Current computers operate on bits, as everyone knows. You can think of bits as a bunch of light switches that are either on or off. A quantum computer is different in that the light switches can be on and off at the same time. Furthermore, the toggling of one switch may change another–this is known as entanglement. So a quantum computer has a bunch of these switches, which are called qubits, and each qubit can be in multiple states at once until it is measured. At that point it becomes a specific value, just like a regular computer, but this value is randomly selected from the possibilities.

So why are quantum computers useful? The big reason is that quantum computers can efficiently factor. Given three and five it is easy to know they multiply together to be 15, but given 15 it is much harder to know that it is the product of three and five. This "one way" problem forms the basis of many modern encryption systems, SSL included. But because the result of the quantum computation is random, you may have to try a couple of times to get the right answer. So if you have a quantum computer, you can decrypt most of the encrypted communications over the Internet. Obviously, this is something that most governments would want to get their hands on.

While this all sounds great, quantum computers are still a number of years off–the best guess is 2021, plus or minus five years. There are some that exist in labs, but only with a handful of qubits. So building quantum computers is a very hard problem. When they finally do arrive, it will be much like computers were in the early days–expensive and shared by many users.

The currently proposed architecture is called a quantum random access machine, or QRAM for short. In this architecture, an existing computer communicates with the quantum computer, sending commands and receiving results. This can easily be shared, even over the Internet perhaps.

As one can imagine, there are a number of ways this architecture can be exploited. The most apparent way would be a man-in-the-middle attack. Since the results are random, you could consistently give the wrong answer. Or, if you wanted to see the results, perhaps of decrypted communications, you could just watch the traffic. If the quantum computer is shared over the Internet, you could also break in and utilize it for your own purposes. Since the first quantum computers will likely be owned by governments or large corporations, this may be the only way we'll get to play with them...



# 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.

January 28-30
**ShmooCon**
Washington Hilton Hotel
Washington DC
www.shmoocon.org

February 25-26
**Nullcon**
Goa, India
nullcon.net/

April 7-9
**Hackito Ergo Sum 2010**
Paris, France
hackitoergosum.org

April 14-17
**Notacon**
Hilton Garden Inn
Cleveland, OH
www.notacon.org

April 15
**THOTCON 0x2**
Chicago, IL
www.thotcon.org

April 22-25
**Easterhegg2011**
Eidelstedter Mansion Association
Hamburg, Germany
wiki.hamburg.ccc.de/index.php/Easterhegg2011

June 18-19
**ToorCon Seattle**
Last Supper Club
Seattle, WA
www.toorcon.org

August 10-14
**Chaos Communication Camp**
Finowfurt, Germany
events.ccc.de/category/camp-2011

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

# Marketplace

## *For Sale*

**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.

**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

**ANONYMOUS VPN.** Send $5.00 per month to IP Anonymous, PO Box 83, Port Hadlock, WA 98339. Include a very unique user name, password and the date you would like service to start. Simply point your PPTP client at ipanonymous.dontexist.net. IPSec account also available for an additional $5.00 setup fee. Include an email address so we can send your configuration. For technical assistance, email ipanonymous@yahoo.com or call 614-285-4574. TOS: The exploitation of minors will not be tolerated.

**GAMBLING MACHINE JACKPOTTERS,** portable magnetic stripe readers & writers, RFID reader writers, lockpicks, vending machine jackpotters, concealable blackjack card counting computers, computer devices, odometer programmers, and much more. To purchase, visit www.hackershomepage.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

**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.

**ET PHONE HOME FOB:** Subminiature, tiny (7/10 ounce), programmable/reprogrammable touch-tone multi-frequency (DTMF) dialer with key ring/clip which can store up to 15 touch-tone digits and, at the push of the "HOME" button (when held next to a telephone receiver), will output the pre-programmed telephone number which can be heard at the same time from the unit's internal speaker. Ideal for E.T.'s, children, Alzheimer victims, significant others, hackers, and computer wizards. It can be given to that guy or gal you might meet at a party, supermarket, or social gathering when you want him/her to be able to call your "unlisted" local or long distance telephone number, but want to keep the actual telephone number confidential and undisclosed. Only you have the special programming tool to change the stored number. Limited quantity available. Money order only: $24.95. $23 each if you order two or more. Add $4 S/H per order. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas, Box 410802, Crc, Missouri 63141.

## *Help Wanted*

**NO COMPROMISE PROVIDER** of open architecture-based network privacy & security services is actively searching for exceptional technologists (of all hat colors) with extensive experience in network topology/design, VPN architectures, and general *nix sysadmin - we recently survived a massive federal effort to shut us down via extralegal harassment & imprisonment of our founding CTO on political grounds; company is now bouncing back & expanding our service offerings (telecom included). Must have strong loyalty to principles of free expression, anti-censorship, genuine cultural diversity. Tribal-based management philosophy - strong financial performance, strong community involvement. Details, compensation info, & longtime community credentials available via: wrinko@hushmail.com. Namaste.

**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*

**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*

**"TALK GEEK TO ME" NOW A NEWSCAST.** The tech audiocast "talk geek to me" is now a news format audiocast, seeking to bring a weekly dose of news that the mainstream media doesn't care to cover. We also seek to cover hacker projects, so if you'd like an interview done to help get your message out, let me know. Email: dg@deepgeek.us Web: www.talkgeektome.us

**HACKERS/PHREAKERS REJOICE** and join us on ClientX, a PBX that has been set up and designed for the telephone, radio, VoIP and technology enthusiasts all across the world! To reach the PBX at anytime, dial 425-906-5656. Or use the SIP extension *010912940 from your favorite hard/soft phone or SIP client! Conferences, voicemail, tech news and more!

**PHONE PHUN.** Blog listing interesting phone numbers and telephone services. Share your finds! www.phonephun.us

**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/

**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 forensics 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.

## *Announcements*

**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* (*loaded* with resources) can be found at http://phibetaiota.net. We seek to identify dysfunction and energize creative solutions by interconnecting and harmonizing the 12 policy domains with the top 10 global threats and 8 challengers - http://is.gd/d0FOj Related links: twitter.com/earthintelnet, youtube.com/earthintelnet, www.earth-intelligence.net, true-cost.re-configure.org, smart-city.re-configure.org. Free books: Intelligence for Earth - http://is.gd/b4519 & Collective Intelligence - http://tr.im/jo9S Contact earthintelnet@gmail.com.

**JESUS LOVES HACKERS!** www.christianhacker.org.

**BLACK OF HAT BLOG.** Covers topics such as cryptography, security, and viruses. Visit http://black-of-hat.blogspot.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 Spring issue: 2/25/11.**

*"Security is mostly a superstition. It does not exist in nature, nor do the children of men as a whole experience it. Avoiding danger is no safer in the long run than outright exposure. Life is either a daring adventure, or nothing."- Helen Keller*

## staff

Editor-In-Chief

Associate Editor

Layout and Design

Cover

Office Manager

Writers:

Infrastructure:

Webmaster:

Network Operations:

Broadcast Coordinators:

IRC Admins:

Forum Admins:

Inspirational Music:

Shout Outs:

*2600 (ISSN 0749-3851, USPS # 003-176); Winter 2010-2011, Volume 27 Issue 4, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

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

# 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:** At Student St in Old Main in front of Tim Horton's, 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 Plaza) near Doutor Coffee.

**Tokyo:** Moving 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:** Lola Coffee House, 4700 North Central 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

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

Connecticut

**Waterbury:** Brass Mills Mall second floor food court. 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.

**Sebring:** Lakeshore Mall food court, next to payphones.

**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.

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.

**Davenport:** Co-Lab, 1033 E 53rd St.

Kansas

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

**Wichita:** Riverside Perk, 1144 Bitting Ave.

Louisiana

**New Orleans:** Z'otz Coffee House uptown 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:** Arch Reactor 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

**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, 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. 7 pm

**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

**San Juan:** Plaza Las Americas by Borders on first floor.

**Trujillo Alto:** The Office Irish Pub. 7:30 pm

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. 7 pm

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

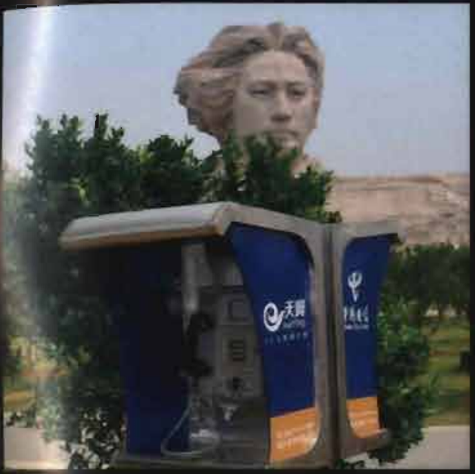
**Spokane:** The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

**Madison:** Fair Trade Coffee House, 418 State St.

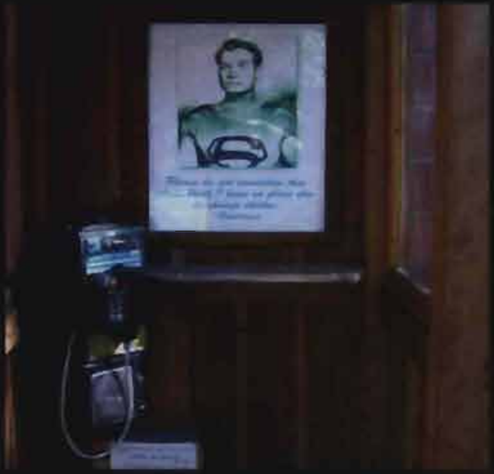
**All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.**

# Payphones with Distractions



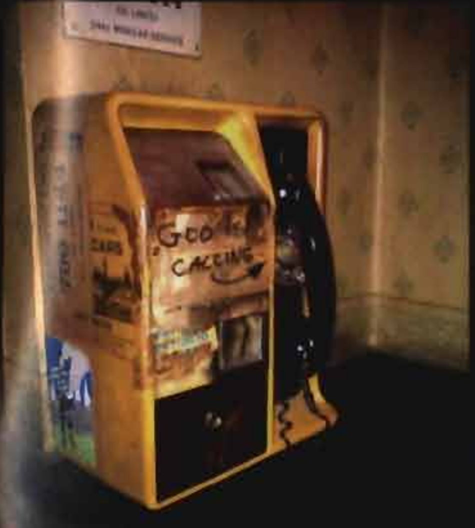
**China.** Seen in Changsha, the capital of Hunan province. This is where Mao Zedong was supposedly converted to communism. If you look carefully, you should be able to see his statue in the distance.

*Photo by Tony Anastasio*



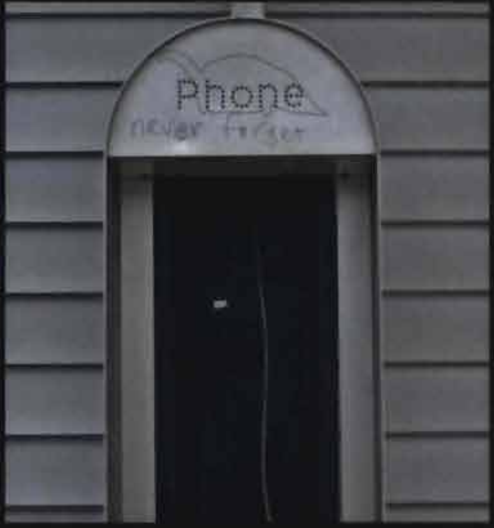
**United States.** Found in a place called Volcano, California, this phone, like the previous one, also lies in the shadow of a national hero. Superman's plea reads: "Please do not vandalize this phone booth. I have no place else to change clothes."

*Photo by Scott Webb*



**England.** This phone is said to still exist in the George Tavern in East London. The fact that God himself may be trying to get through is overshadowed by the fact that this is actually a true rotary-dial phone.

*Photo by Sam*



**United States.** Seen in New Paltz, New York, it's not really fair to call the message here a distraction to a payphone, since in fact there is no payphone. But the message is one that we must always heed, even if the phone companies won't.

*Photo by Rocco Rizzo*

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.