2600 Magazine − Volume 20, Number 3

Payphones From Egypt

Completely different from the four we printed two issues ago. This one is a Menatel, probably the most popular and widespread payphone in Egypt. It uses prepaid chipcards.

What the connection is to the former Beatle we don't know but these phones use prepaid cards and are only found in Cairo and Alexandria.

This phone was found in the middle of the desert. Not much is known about it other than the fact that it only takes coins.

This is actually the exact same kind of Telecom Egypt phone we printed in the Spring issue but this one is a completely different color! And that makes all the difference. And no, she isn't giving us the finger.

Photos by Encrypted_Error

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

Volume Twenty, Number Three
Fall 2003, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly

> "I do know I'm ready for the job. And, if not, that's just the way it goes."
>
> - George W. Bush, August 21, 2000

Staff

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Photo
Bob Hardy

Cover Design
Mike Essl

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dalai, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, David Ruderman, Screamer Chaotix, Seraf, Silent Switchman, Mr. Upsetter

Webmasters: Juintz, Kerry

Network Operations: css, mlc

Broadcast Coordinators: Juintz, Pete, daRonin, Digital Mercenary, Kobold, w3rd, Gehenna, Brilldon, Chibi-Kim, lee, Nico, Logix, Boink, John

IRC Admins: Antipent, daRonin, Digital Mercenary, Redhackt, Roadie, Shardy, The Electronic Delinquent

Inspirational Music: Deep Purple, Desmond Dekker, Kraftwerk, Mary McGoon, Gene Kelly, Steve Reich, Wendy James

Shout Outs: Mescalito, Melborp, Duat, Aurelijus, Ilya, Balthazar, Johny, Pajkus, Tomasz, Al Lewis, and the CCC crew

RIP: Wesley Willis, Johnny Cash

Welcome: Zoë Olivia

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

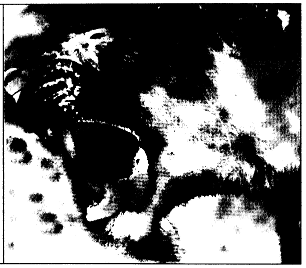
POSTMASTER:
Send address changes to
2600, P.O. Box 752, Middle Island,
NY 11953-0752.
Copyright (c) 2003
2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada -
$20 individual,
$50 corporate (U.S. funds).
Overseas - $30 individual,
$65 corporate.
Back issues available for 1984-2002 at
$20 per year,
$26 per year overseas.
Individual issues available from 1988 on
at $5.00 each, $6.50 each overseas.

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

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

Trouble

Feeding the Frenzy



Lately our society has become completely obsessed with the concept of threats. We live in a dangerous world. There are all kinds of people out to get us and destroy the American way of life. Strangers are a menace to our children. The streets aren't safe. By default, we're encouraged to look at anything unusual as if it were a predator waiting to strike. Everything, after all, is a potential threat. And, just so we don't let our guard down, we have the federal "threat level" reminding us just exactly how dangerous the world really is.

And then, of course, there's the Internet, where we can panic freely without ever having to leave our homes. Everything from chat rooms to websites to hackers has become something to fear, reinforced by media stereotypes. The real threats, such as the failure of companies to protect customer databases and the private information contained within, are usually glossed right over in favor of an easier, more sensationalist target. For instance, when the Bank of Montreal recently sold computers containing sensitive bank account information for thousands of their customers to a private citizen, most media reports focused on what hackers could have done with this information rather than the notoriously bad security practices that allowed this to happen in the first place.

This summer has seen a virtual plethora of nonsensical threats on the net. It's easy from our perspective to laugh at the utter stupidity of so much of it. But oftentimes in our holier than thou smugness, we fail to realize that the absurdity has become the reality.

Such change always occurs gradually. Were it to happen all at once, it would be a lot easier to see the faults. When people have a chance to get used to changes and, more importantly, when people begin to forget what it was like before the changes, the reality landscape change is complete. It's essential to recognize this, even if it seems to be impossible to change it.

What happens online frequently mirrors events in "real life." And on the Internet, we're being encouraged to become paranoid about our safety, hostile to outsiders, and dependent on things we really don't need to survive. And if we're not careful, we'll soon forget just how ridiculous this is.

The Summer of 2003 will be remembered as the summer of worms and viruses, where names like "LoveSan" and "Blaster" became synonymous with online terrorism. The net became clogged, commerce was affected (the claims of billions of lost dollars quickly became accepted as undisputed fact), and our very way of life was once again being threatened.

Yes, it's easy to see how absurd this situation is. But very little is being done to address that point. Instead, the discussion focuses on increasing prison time for people who write these programs (possibly charging them as terrorists), putting the Department of Homeland Security in charge of Internet security, and continuing to connect critical and non-critical systems together so that any threat can easily become a catastrophe.

It's almost as if we need the excitement of utter chaos. Systems are designed poorly and then tied together so that the cascading effect is realized when there's a malfunction or security breach. People capable of causing more mayhem by writing some simple code are more than happy to oblige, ostensibly because they want to enjoy the chaos as well. Of course they fail to realize that the final act of this little drama invariably needs a villain to blame and punish in order to reestablish some semblance of normalcy.

So instead of dealing with the fact that we've become hooked on operating systems with large security holes that any idiot with a basic knowledge of programming can exploit, we handle it as if it were some sort of "cyberwar" complete with enemy combatants, spies, and a terrified populace. It's a not-so-distant cousin of the Y2K hysteria when many became convinced that the world would be plunged into anarchy when the calendar changed. In such cases we need to remember some rational thoughts: Don't become entirely dependent on *any* single system because failures and flaws are inevitable; Keep regular backups; Put the whole picture into perspective and realize that an occasional glitch in your e-mail or a temporary outage for amazon.com is simply one of the growing pains of the net, *not* the end of the world; *Always* have a different way of achieving the same ends so that if a piece of software or hardware becomes unreliable, you won't be completely stuck. This latter point can apply to individual applications or entire networks - even the concept of bypassing computers and networks altogether should that become necessary.

When a massive power outage hit some major cities in the United States in August, speculation quickly pointed to hackers possibly being somehow responsible. Although this was mostly dispelled by the same media reporting it, a profound level of ignorance was revealed by these ponderings. The ignorance that we're all used to is that of blaming a hacker whenever something goes wrong with a computer or network simply because nobody has any idea what's really going on. But the newer and more disturbing addition to the existing ignorance is that the concept of tying together critical and non-critical systems is becoming acceptable to many. The mere suggestion that computers involved in keeping the nation's electrical grid online could be affected by an errant piece of e-mail on the public Internet seems, once again, absurd. Yet it seems to be growing ever closer to reality. This gap in logic is possibly the easiest way to achieve this world of eternal crisis that so many in the media, government, and populace seem to crave.

But before we get to the stage where a denial of service attack by some idiot somewhere causes the lights to go out in a major city or a surge of pornographic spam clogs the life support systems in hospitals, we ought to change our way of dealing with these issues. If a critical system is vulnerable, covering up that fact is every bit as bad as attacking it. We don't advocate the crippling of any system or network, critical or non. We're certainly not in favor of imprisoning people who do something stupid and simple without thinking - as if they did something requiring detailed planning with a clear intent of malice. What we do support is the full disclosure of any wide open security holes that could result in either a royal pain in the ass for people trying to surf the web or something a bit more life threatening. Such disclosure needs to be encouraged and even rewarded. It's clear there's a lot we're not being told - and that there are many in power who would like to keep it that way.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for September 29, 2003. Annual subscription price $20.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, ST. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, ST. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, ST. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6 Extent and nature of circulation

	Average No. Copies each issue during preceding 12 months	Single Issue nearest to filing date
ATotal Number of Copies	81,000	83,000
BPaid and/or Requested Circulation		
1Paid/Requested Outside-County Mail Subscriptions	4653	4346
2Paid In-County Subscriptions	65	68
3Sales Through Dealers and carries, street vendors, and counter sales	71,268	74,860
4Other Classes Mailed Through the USPS	0	0
CTotal Paid and/or Requested Circulation	75,986	79,274
DFree Distribution by Mail (samples, complimentary, and other free)		
1Outside-County	447	447
2In-County	3	3
3Other Classes Mailed Through the USPS	0	0
E. Free Distribution outside the mail. (Carriers of other means)	4564	3276
F. Total free distribution	5014	3726
G. Total distribution	81,000	83,000
HCopies not distributed	0	0
I. Total	81,000	83,000
J Percent paid and/or requested circulation	94	96

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

Getting to Know Your Neighbors

by Shiv Polarity
(shivPolarity@myrealbox.com)

Note: In most places, connecting to your neighbor's network without their permission is illegal. Additionally, you can be prosecuted by your neighbor's Internet provider for theft of services if you access the Internet through their network. These instructions are purely for informational purposes and are intended to help you learn how to secure your own wireless network by learning the tactics of potential attackers. Do not invade the privacy of your neighbors - it is rude. Do not steal Internet access - it is wrong.

The use of devices such as 802.11b network cards in schools, coffee shops, and the workplace is becoming more and more common every day. In a setting such as an apartment complex, it is common to have one or more neighbors who have laptops or computers equipped with such a device. If you have a wireless network in your home, you should know how a motivated WiFi user might try to gain access to your network. In order to adequately protect your network from invaders, you should understand what tools and tactics could be used against you.

The first thing you would need to explore a neighbor's network is a computer with a correctly configured 802.11 network card. I use a laptop with a Compaq WL100 PCMCIA card. The drivers I have found most useful are the linux-wlan-ng drivers from http://www.linux-wlan.com/linux-wlan. For the purposes of this article, the use of these drivers will be assumed. Other cards may require other drivers, though almost any Prism2-based card should be fine with linux-wlan-ng. Download the source and follow the instructions to compile for your specific configuration.

Phase 1: Discovery

The first step toward exploration is discovery. By default, your network card will try to connect to the strongest available signal it finds. This is good for accessing the Internet from coffee shops or school, but for our purposes we need a little bit more information. This is where a little app named Kismet comes into play.

Kismet is an "802.11 wireless network sniffer," available from http://www.kismetwireless.net. Once it has been downloaded and configured you can use it to scan the surrounding airwaves for wireless networks.

To start Kismet you must first use the root account to start the Kismet server by running "kismet_monitor." This will put your card into scan mode, which will disconnect you from any previous networks you may have been connected to. The kismet_monitor command starts up the Kismet server application. Once that has been started, open a different console and run the command "kismet." In your kimset.conf file, you should have configured Kismet for a default user. This is the only user that can start the application, so be sure you run the kismet command as that user.

The graphical interface presented by Kismet can be confusing at first. I suggest you read the documentation at the Kismet website and get to know what all the symbols and sounds mean. Personally, I find the sounds irritating and usually turn them off by pressing the "m" key. Kismet offers a great deal of information, providing statistics and details for all detected wireless signals. For our purposes, all we are interested in is the list of available access points.

The perfect access point will be unencrypted (access points named "default" are particularly delicious). Kismet will tell you whether or not a given access point is using WEP (Wireless Encryption Protocol). If all of the listed access points for your location are encrypted, you will not be able to proceed. WEP can be broken, but it is a time consuming process and is beyond the scope of this article (a little too invasive for my taste). Though I will suggest you visit http://airsnort.shmoo.com if it is not beyond the scope of your personal ethics.

Once you have identified an unencrypted access point, write down its SSID (name) as well as the channel the signal is using and quit Kismet. Once you have closed the Kismet application, run the kismet_unmonitor command as root. This stops the Kismet server and puts your Wifi card back into its normal mode of operation, though it doesn't hurt to also run "/etc/init.d/pcmcia restart" just for good measure, assuming you are using a laptop.

Phase 2: Connectivity

The next step is actually connecting to the access point you have identified. The steps involved in connecting to an access point will differ from one 802.11 driver to the next. These instructions apply to linux-wlan-ng drivers only. If you use different drivers, consult the instructions for those drivers.

Edit /etc/wlan/wlan.conf and look for the line beginning with "SSID_wlan0". The value for that key should be the SSID of the access point you wish to connect with.

Next, look in /etc/wlan for a file named wlancfg-DEFAULT. That file is your template config file. Do not edit it or overwrite it. Instead, use the cp command to create a copy of it. The name of the copy is important and is determined by the SSID of the access point you are trying to connect with. For example, if your target access point is named "myAccessPoint" you would use the following command.

```
cp wlancfg-DEFAULT wlancfg-MyAccessPoint
```

This will create a new file named /etc/wlan/wlancfg-MyAccessPoint. For access points named "default" create the file /etc/wlan/wlancfg-default. Remember, this is Linux so wlancfg-DEFAULT and wlancfg-default are totally different files. The linux-wlan-ng drivers will use this new file the next time your wireless connection is initialized.

After you have the new config file, edit it. The contents of the file should be pretty easy to understand. Enter the channel in the appropriate place, as well as the WEP key if needed (if you used Airsnort to acquire one). Most of this file can probably be left as-is.

Once all of your values are entered correctly into the new config file, restart your wireless connection. Personally, I use "/etc/init.d/pcmcia restart" to do this, though you may have a different means. If everything is correct, you will connect to your target access point. My card gives me two high-pitched beeps to indicate a good connection. One high-pitched beep followed by a low-pitch beep indicates failure.

There are several reasons your connection attempt might fail. If the access point uses MAC address filtering, you will probably not be able to connect to the access point. In this case you are probably up against a fairly savvy access point and you're better off seeking lower-hanging fruit. You may also have made a mistake in your wlancfg file. Double check it. Restart Kismet if you need to make sure you got everything right to begin with. Also double check to make sure the access point isn't using encryption. Another reason for connection failure could be poor signal strength. Again, check Kismet to make sure there is a reliable signal getting to you. If not, try walking around (assuming you have a mobile computer) and see if you can get a better signal somewhere else. Sometimes just a few feet in the right direction can make a huge difference. If all else fails, check /var/log/syslog or one of your other error logs.

Phase 3: Exploration

Now you're connected to your neighbor's access point. Congratulations, you outlaw. Before proceeding, be aware that your connection has been logged on your neighbor's access point or wireless router. Of course, if your neighbor has left his access point wide open, they probably don't even know what the log means and probably never check it. But you should be aware. They have a log of your MAC address, what time you connected, what IP you were assigned, and, depending on the access point, they may be logging everything you do on their network.

So what now?

Well, my first thing would probably be to see what IP I have been assigned. It is usually 192.168.0.x where x is some number greater then 1. Also, pinging 192.168.0.1 usually works because that is probably the IP to the access point or wireless router. Try opening a web browser and entering in http://192.168.0.1. If prompted for a username/password, try typing in "admin" as the username and leave the password blank. If they are truly using the out-of-the-box configuration, this will usually let you into the configuration page. If you can get into the configuration page, you now have full control of the access point and/or router. One good idea might be to clear the activity log. But hey, this is your gig. Do what you like.

Another interesting venture could be to look at any port-forwarding rules. Finding out which ports are forwarded is a good way to determine what sorts of things go on over this network. Is there a web server somewhere? An SSH server? Does anyone play video games? If so, what IP do these services run on? This is all very interesting stuff.

If you can't find the access point right away, try using a tool known as nmap (http://www.insecure.org/nmap/). As root, run the command "xnmap" to get a nice graphical interface for this incredible tool. You have several options you can perform with nmap. One of my favorites is an IP scan using operating system detection. If you tell it to scan 192.168.0.*, it will scan every possible IP on that segment and return to you a list of all active IP addresses, along with which operating systems they are using. The IP for the access point will have an operating system such as "D-Link DWL 900AP+" or something along those lines. It should be obvious.

So now you know where the access point is. You also know what model the access point is. Try a Google search for that model number. You can sometimes find interesting bugs or vulnerabilities on web forums for specific models. At the absolute least you should be able to download the PDF manual for the access point to learn how it works along with a confirmation of the default username and password.

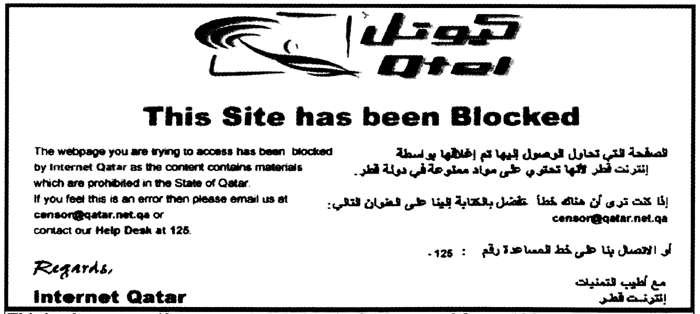
You also know how many clients are using the access point, and you know their IP addresses. So now it's time to be neighborly. Go grab an application called LinNeighborhood (http://www.bnro.de/~schmidjo/). This program gives you a graphical interface to your local network, much like Microsoft's famous "Network Neighborhood".

Once you've started LinNeighborhood you probably will only see your computer listed in the main window. Since it is highly unlikely that you're on the same workgroup as your neighbor's computers are, you will have to do a little work to find them. Click the button at the top labeled "add". This will bring up a dialog asking for a name, group, IP, etc. Enter an IP from the list given to you by nmap, then click "query". LinNeighborhood will fill in the rest of the values for the "add" dialog. Once the rest of the values have been filled in, click OK. The new computer should now show up in LinNeighborhood. Do this for each of the computers found by nmap.

Clicking on the computers listed in LinNeighborhood will show you any shared folders they have. You will need to know the usernames and passwords to access them, unless they have been shared publicly. But at this point, why would you suspect your neighbor of not sharing his files publicly? LinNeighborhood will mount the shares to your local file system, and you can look around and see what is there. My personal suggestion would be to not look at the files, and (assuming you can get write access) politely leave a conspicuous text file explaining how to properly secure a wireless network, suggesting WEP encryption, MAC filtering, and setting new passwords and IP addresses for everything. If you do this, most definitely be sure to clear the activity logs in the access point or router.

At the absolute least you should be able to learn the names, groups, and IP addresses of your neighbor's computers. You can use the port forwarding rules from the router to determine what roles the network clients perform and you'll be able to access the Internet, albeit illegally.

Of course, the smartest thing to do would be to not try any of this stuff yourself and instead double check your own access point or wireless router configuration to be sure they are secure. Also, be sure to change your WEP keys from time to time and keep an eye on your logs. You never know who lives nearby. It could be another *2600* reader.



This Site has been Blocked

The webpage you are trying to access has been blocked by Internet Qatar as the content contains materials which are prohibited in the State of Qatar.
If you feel this is an error then please email us at censor@qatar.net.qa or contact our Help Desk at 125.

Regards,
Internet Qatar

الصفحة التي تحاول الوصول إليها تم إغلاقها بواسطة
إنترنت قطر لأنها تحتوي على مواد ممنوعة في دولة قطر.

إذا كنت ترى أن هناك خطأ تفضل بالكتابة إلينا على العنوان التالي:
censor@qatar.net.qa

أو الاتصال بنا على خط المساعدة رقم : 125.

مع أطيب التمنيات
إنترنت قطر

This is what you get if you try to access our site from parts of Qatar. Although it still pisses us off, at least they refer to themselves as censors rather than netnannies or the cyber patrol.

Image by lazypoltergeist

Servers on a Ghetto ISP

by Lirakis

Many ISP's today restrict their customers from providing services by blocking ports. It is unfair that ISP's do not give their customers what they pay for and instead opt to make more money by charging a lot for business service on which you can run servers, all while saying it is in their customers' best interest. This article is meant to be an in depth follow up to "Fun With Hosting On Your Cable/DSL" by Toby in 20:1 and also includes how to set up a POP3/SMTP email server with a port blocking ISP. This article specifically addresses restrictions as well as statements made by Cox communications. Depriving customers of abilities, in my opinion, is not protecting them. It is cheating them. Perhaps if Cox did not use up so much of its bandwidth tracking customers ("Cox or someone acting on its behalf may engage in the anonymous monitoring of Internet activity. This means that a customer's session may be tracked" - Cox T.O.S. at www.cox-internet .com/terms.html), they would be more willing to provide the full service that their customers have paid for.

Below I have listed the ports that Cox blocks and the reason why they say they block them.

Port	Transport	Protocol	Direction	Reason for Filtering
25	TCP	SMTP	Both*	SMTP Relays
80	TCP	HTTP	Inbound	Web servers, worms
111	TCP	Portmap	Inbound	RPC services, worms
119	TCP	NNTP	Inbound	NNTP servers
135	UDP	NetBios	Both	Spam/Pop-ups, Worms
136-139	UDP/TCP	NetBios	Both	Worms, Network Neighborhood
1900	UDP	MS-DS/NetBios	Both	Worms, Network Neighborhood
27374	TCP	Subseven	Both	SubSeven Trojan

As you can see two of the three ports we need to set up web and email servers are blocked, port 25 and port 80.

Setting Up a Web Server
(The Easy Part)

Register your domain name with a DNS that provides URL redirection (I used www.123cheapdomains.com) and get a router that supports port forwarding or port mapping (portmap (a *nix utility) can also be used but it is notoriously insecure so I will not cover it). I use a D-link 614+ router which works great. Set up your web server (I used Apache) behind the router and give it a static IP on your internal network. Let's give it 192.168.0.150 for use in this article. Now open up your router's admin menu and somewhere in advanced settings you will find port forwarding. Here you need to set your router to listen to an external port and forward any request to an internal IP on the same or different port which you specify. So let's set the public port to listen to public port 2600 and forward it to private port 80 on 192.168.0.150. Now go to your DNS and create a record for your public IP. Now you also need to create a record for URL redirection (DNS does not allow port specification, so this is why we use URL redirection). Create a URL redirect record containing http://xxx.xxx.xxx.xxx:2600 substituting your IP in for the x's. The :2600 is the port specification, just as if you were typing in an ftp site into a web browser's address bar. Now your web server will work just fine.

There is one more issue that comes up that is not a big deal. When someone goes to your website http://your-ip + :2600 will show in the address bar, not your domain name. To make it show your domain name you must specify URL forwarding with address masking on your DNS and give it the domain name that you want to show. That wasn't so bad now was it?

Setting up a POP3/SMTP
Email Server (The Hard Part)

Well, if you want to set up an email server it is not so easy, but it is still doable. I am using sendmail in this article but I will not cover basic setup of it; they have whole books devoted to that. Install and configure sendmail according to your needs. Install and configure a POP3 daemon of your choice (I used popa3d). Now you need to set up port forwarding for the SMTP portion of the mail system. You should not have to do any port forwarding for the POP3 daemon because, oddly enough, Cox does not filter port 110. Open your router's admin page and go to the port forwarding section and let's specify public port 2700 and forward it to private port 25 on 192.168.0.150.

The next part is more difficult. Because there is no way to specify a port for MX records (mail server records), you can't just use URL redirection like you did with the web server. What you need to do is set up a mail redirection host. This means you need a remote machine somewhere that you can set up a mail server on that can receive on port 25. You're on your own as far as getting a remote machine. (Maybe someone could write a follow up article to this one about social engineering heh heh.)

When you have a remote machine, you need to install sendmail on it. After you have done this, you need to make sendmail listen to port 25 and redirect it to your port blocked computer on port 2700. To do this you must modify a few lines in the sendmail.cf file.

From this:

```
Mesmtp, P=[IPC], F=mDFMuXa,
S=EnvFromSMTP/HdrFromSMTP,
R=EnvToSMTP, E=\r\n, L=990,
T=DNS/RFC822/SMTP,
A=TCP $h
```

To this:

```
Mesmtp2700, P=[IPC], F=mDFMuXa,
S=EnvFromSMTP/HdrFromSMTP,
R=EnvToSMTP, E=\r\n, L=990,
T=DNS/RFC822/SMTP,
A=TCP $h 2700
```

Now you need to add your entry to your mailer table and indicate that you want to use esmtp2700:

```
example-domain.com esmtp2700:[mx-blocked.
    example-domain.com
```

You're almost done! Now all you need to do is to go to your DNS and create an MX record pointing to the relay mail host. Now you can send and receive email @yourdomain.com, POP3 on port 110, and SMTP on port 25.

We see that although many of today's ISP's are stripping their customers' rights to share information that, with a little creative administration and some time, we can keep the spice flowing.

I would like to thank Graymalkin for helping me to test the mail server. Also Solthae, DZNTZ, and all of the members of 2600tucson for helping with testing the web server, http://freebsd.peon.net for info on sendmail relay configuring, and of course Cox Cable. Without their unfair restrictions and blatant breach of privacy I would have had nothing to write about.

More Methods For Hosting FTP on Broadband

by Apratt

After reading about how to set up a web server behind a broadband router in 20:1, I was inspired to offer some ideas about setting up an FTP server behind such a router (or other device doing NAT or IP masquerading, such as a *nix box or Windows box with Internet Connection Sharing; for convenience, I'll refer to all of these as "routers").

FTP's M.O.

Unfortunately, FTP doesn't play well with routers. Since no routers existed when FTP was invented in the early-to-mid-1970's, it didn't need to. Your FTP login and commands travel over a typical TCP connection (the "command connection" aka "control connection"), usually to port 21 of the FTP server. The actual files and file listings to be received, however, all require a separate TCP connection (called the "data connection"), usually to an unpredictable port greater than 1023. In active mode (the old style), the server will initiate these secondary connections to the client, to a port of the client's choosing. In passive mode (the new style), the client will initiate these secondary connections to the server, to a port of the server's choosing. The direction the file is being sent has no affect on who initiates the data connection. If the client is behind a router, active mode won't work. If the server is behind a router, passive mode won't work. If both are behind a router, no files or file listings can be transferred.

Light at the End of the Tunnel

Fortunately, there are several solutions to the problems caused by routers. You can forward some ports in the server's router, forward some ports in the client's router, use a proxy, or just ditch FTP altogether.

Empowering the Server

Using passive FTP and forwarding some ports on the server's router is probably the best overall solution. You'll need to use an FTP daemon (server program) that can be told to restrict itself to using only the forwarded ports and to have the client connect to the *router's* IP address. If your FTP server is behind a router, it would advertise its address as being 10.x.x.x or 192.168.x.x, which will confuse the client. It's more practical to just download PureFTPd, ProFTPD, or GuildFTPd instead of forcing your preexisting FTP daemon to play nicely with your router. According to PureFTPd's documentation, you need to forward two ports per simultaneous connection you wish to support. It doesn't matter which ports you forward as long as they're all in one contiguous block, they don't conflict with anything, and they're all greater than 1023. If you have your router configured to silently ignore uninvited connection attempts, you also might want to avoid using any ports that are famous for being sought by port scanners, such as the ports commonly used by Back Orifice, WinGate, etc. just so you don't attract any unwanted attention.

Empowering the Client

Another remedy is to use active FTP and forward some ports on the client's router. The bad news is that most FTP client programs will report their internal IP address, such as 192.168.x.x or 10.x.x.x, instead of the router's IP address. This will confuse the FTP daemon. SmartFTP is one client that can report your router's IP address as well as restricting itself to using only the handful of ports that you've forwarded from your router to your FTP client computer. Your FTP client program needs to have *both* of these abilities for this method to work. As for which ports to forward, the guidelines are the same as for an FTP server.

Other Options

Proxies: I don't like proxies in general, and their configuration is beyond the scope of this article. Thankfully, there are better ways of transferring files across the Internet, and none of them use the strange multi-connection scheme that FTP does.

SFTP: On the surface, sftp is very similar to FTP. The actual protocol, however, consists of a single SSH connection, so you have encryption and optional compression. Sftp gives you directory listings and all the commands you're used to (chmod, rm, rename, delete, etc.). Since sftp programs are less common than FTP programs, you can't expect sftp programs to be as luxurious as their FTP counterparts. This is especially true for sftp daemons. I hope to see more variety soon. Sftp is not suitable if you need the fancier features found in some FTP daemons.

SCP: Scp is basically the SSH-enabled version of cp, Unix's copy command. Since it uses SSH, it is also secure and compressable. Unfortunately, you need to know the exact pathname and filename to download anything, as scp is incapable of listing what files are available. There are programs like NiftyTelnet 1.1 SSH for Macintosh that include an scp client, but scp programs are also disappointingly uncommon. Did I mention how irritating it is that you have to know the exact path and filename of everything you want to download? It may be an option for uploading to a drop box, however.

HTTP: You shouldn't *totally* discount web servers. If all you need are insecure one-way file transfers, a small web server is all you need to set up. Besides, you could always configure it to support passwords, SSL, and the HTTP "PUT" method. You *do* have a bottle of Advil, right? WebDAV should be an excellent file transfer protocol in the future, but it's only in its infancy right now.

Upgrading to an FTP daemon that is router-aware is the smoothest solution, requiring only that the clients support passive transfers. Security enthusiasts will have to settle for a less convenient method.

Greetz to Selene135, Slan, Smasher, Satan's Intern, and Kurakkuboi.

Hacking *The Look*: Revisited

by mojomonkee

After reading ZenLogic's "Hacking The Look" in 20:2, I decided to author a follow up article that might shed a bit more light on the world of desktop customization in Windows. Now I know this isn't a customization magazine, so I'll keep it short and sweet. Maybe your interest will be piqued and you'll want to dive into this kind of thing by article's end.

While ZenLogic's article touched on some integral customization techniques (res-hacking, registry editing, etc.), there is still much more that can be done to make your desktop *truly* your own. One big thing that you can do to completely change your desktop look and have people say "Is that *nix?" (or even "Is that OSX?") is to change your default Windows shell.

Windows Shells

In Windows, the desktop environment is known as a "shell." The default shell is explorer.exe and is merely a suggestion by Microsoft on how you should run your desktop. It's not set in stone. There is a myriad of alternative shells you can use to completely change this look, and here are just a few that are in active development.

BlackBox4Windows. Known as bb4win to its users, this linux clone runs exactly like its *nix counterpart. With the ability for expansion with user-made "plugins" and support for native linux themes (no porting necessary), this shell is ready to go right out of the box. Just extract the latest nightly build to C:\Blackbox and you're all set to go. For more information on bb4win, go to http://www.bb4win.org.

GeoShell. Geoshell is a newcomer to the shell scene (about a year old) and uses "geobars" to load such items as Winamp controls, command line, clock, system stats, tasks, systray, etc. Much like bb4win, these are achieved through using user-created plugins. Load what plugins you want and others that you don't to achieve what you feel is *your* desktop. For more information, go to http://www.geoshell.com.

Litestep. Litestep started as a Windows clone of Afterstep but has evolved significantly from that. Today it bears more resemblance to Enlightenment due to its extensive customizability. You can make your desktop look, run, and feel *however* you want in just a short amount of time. Litestep is the most complicated of all the shells I've used, but it really gives you complete control over your desktop. With hundreds (yes hundreds) of "modules" (DLL's) that you can apply, there is no end to the functionality of your desktop. Animated auto-hide bars, draggable boxes, 32-bit alpha-blended png support, and ability for highly advanced scripting make the sky the limit for Litestep. For information concerning Litestep, go to http://www.litestep.net and http://lsdocs.shellfront.org.

Shell Installation

Sometimes a shell comes with an installer that can set the shell as the default for you by automatically editing the registry. While this may be a good idea since it allows you to keep your hands out of regedit.exe, I recommend opting out of this option and setting the shell yourself. This allows you to learn how Windows handles shell settings for individual accounts and also lets you have control over which accounts have which shell.

Windows 2K/XP: I recommend having a main administrator-level account that uses explorer.exe as the shell for system critical driver installations and Windows updates. This insures that nothing goes funky because the default shell isn't loaded (MS isn't fond of third party software running at the core of the system and certain Windows updates might get b0rked if explorer.exe isn't loaded as the shell).

Once you have your explorer account all ready to go, create a new account for your alternative shell (I have one called brian_litestep and one called brian_bb4win). Log into the shell and then run regedit. In regedit, follow these steps (Thanks to Omar Hussein!):

```
HKLM\Software\Microsoft\Windows NT\
   CurrentVersion\IniFileMapping\system.ini\boot
set the 'shell' String to:
USR:Software\Microsoft\Windows NT\
   CurrentVersion\Winlogon

HKCU\Software\Microsoft\Windows NT\
   CurrentVersion\WinLogon
set the 'shell' String to:
x:\path_to_shell\your_shell.exe

HKCU\Software\Microsoft\Windows\
   CurrentVersion\Explorer
set the 'DesktopProcess' DWORD to:
```

Note: If you don't have a "shell" string, then just create it.

If this is too difficult (or you can be bothered to mess with the registry), then make a registry file (*.reg) that will do it for you. Open up a text editor and paste in the following information (Thanks to Paradox!):

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\
   Microsoft\Windows NT\CurrentVersion\
      IniFileMapping\system.ini\boot]
"shell"="USR:Software\Microsoft\
   WindowsNT\CurrentVersion\Winlogon"
[HKEY_CURRENT_USER\SOFTWARE\
   Microsoft\Windows NT\CurrentVersion\Winlogon]
"shell"="C:\path_to_shell\your_shell.exe"
[HKEY_CURRENT_USER\SOFTWARE\
   Microsoft\Windows\CurrentVersion\Explorer]
"DesktopProcess"=dword:00000001
[HKEY_CURRENT_USER\SOFTWARE\
   Microsoft\Windows\CurrentVersion\
      Explorer\Advanced]
"DesktopProcess"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\
   Microsoft\Windows NT\CurrentVersion\Winlogon]
"shell"=
```

Save the file as a *.reg extension and don't forget to edit the "shell" line to your specific settings! Double-click the *.reg file to add it to your registry and you're all set to go.

You can do this for as many accounts as you want (try out all the shells!). This way, if you get sick of the shell and want to return to the safe haven of explorer.exe, you can just delete the account and go back to the administrator account.

Windows 95/98/ME: Since 95/98/ME isn't a true multi-user OS, there can only be one shell set a time for all users. This has both positive and negative sides to it. The positive is that there is only one file that you need to edit in order to set the alternative shell as the default. The negative is that you will want to have explorer.exe loaded when installing Windows updates and other critical system upgrades since some software/driver installations rely on explorer's services for proper installation.

Never fear! This is an easy problem to get around. How do we fix it? We get a "shell manager!" A shell manager... manages your various shells so that you can choose which one you want to use on startup. Think of it as the stepchild of Lilo. I recommend "shellON" which is available at http://www.dx13.co.uk/sov3/. To set the shell in 95/98/ME, follow these steps:

Make sure system files and hidden files are shown (so you can see the file you need to edit).

Navigate to C:\Windows\ and find the file "system.ini".

Open system.ini in notepad (or your favorite text editor) and set the shell of your choice in the "shell=" line. If you wish to use just the alternative shell (e.g. bb4win) then just set it to "shell=C:\Blackbox\blackbox.exe" but if you want to use a shell manager, set "shell=" to the proper executable.

Note: If you ever are left with a blank screen and no way of fixing it, reboot your machine into DOS mode and edit the system.ini file to point back to explorer.exe as your shell. Since there is no task manager, it is one of the only ways to get back to your desktop to fix things you may have messed up.

End Notes

Desktop shells are just one part of desktop customization, but they can do a lot for the way you run your desktop and up your production level by reducing the amount of clicks to get to simple tasks. You can't really muck up your system too much, but always make sure you know what registry or system file you're editing before you reboot your system... you might lock yourself out of your OS. If you want more information on running an alternative shell on Windows, visit the following sites:

http://www.shellfront.org
http://www.shellscape.org
http://shells.loose-screws.com
http://shell-shocked.org

Shouts to #litestep, #fpn, customize, and deskmod.

case mods Made Easy

by X3N0X

With the advent of flashy new Main boards and fancy looking heat-sinks, modded cases have become a new trend in the computer world. Fancy, expensive cases can be bought at retail outlets such as CompUSA and many other stores, complete with fluorescent lights and other frills. The only problem is the exorbitant cost of these pre-modded cases, not to mention the lack of personal expression caused by the limited number of choices available.

Taking this into consideration, and also the hacker community's general propensity for modifying things, there may be those of you out there who would enjoy doing such things to your own computers and not spending large sums of money on a fancy case. This article addresses some of the methods and tools that can be used for modding cases and sources for things such as lights.

First, I would like to remind you that I am not responsible for damage or injury to your computer or person resulting from following the procedures mentioned herein. Also, those of you who worry at the thought of soldering some wires or other similar activities should stop reading this article now.

The tools required to mod cases are very simple and easy to find. I would imagine that if you live at home your father probably has all of them handy and would let you use them if you asked. For those of you without tools, well, you get the idea.

You will need a good electric jigsaw and some fine tooth metal blades. The finer the teeth, the easier it will be to cut the metal. Also, you will need a good electric drill with an assortment of sharp drill bits. A couple of coarse files, one round and one flat, will be of use as well. All of these tools are available at your local home improvement store.

Lights can be found at your local Super Target, Auto Zone, and virtually any other store that sells things for "customizing" your car. The type of stores to look for typically cater to the Honda-driving rice-boy types and sell anything from EL-Strips to sound activated fluorescent lights of all colors and sizes. The reason you want the kind for cars is because they typically run on 12 volts which makes them easy to power from your computer's power supply.

After you have decided what you want your finished case to look like, it's time for the fun to begin.

First, figure out how you want the "window" to be cut. I have seen anything from windows in the top to windows on all sides. I will use a side window as an example in this case.

The first task is to remove the side so that it can be laid flat to allow cutting. I recommend buying a cheap case with sides that are separate, as this makes it easy. After the sides have been removed, you need to draw a sketch of your desired window shape. Use a pencil as it can easily be erased if you goof up.

Next, drill a hole at least an inch away from the outside edge of your window sketch. It should be large enough to allow the saw blade to pass easily through the metal. Aim the saw towards the outer edge of your window and start cutting. As you approach the edge of your shape, gradually turn the saw to align the blade with the line you drew. Take your time and make your curves gradual. This will prevent broken saw blades and injury. If you want, some wide masking tape can be applied to the outer surface of the case to prevent nicks in the finish while you are cutting.

Now that you have a gaping hole in the side of your case, remember those files I told you about? Now clean up the edges of the hole you made. Use the round one for curves and the flat one for flat areas. (Duh.) It is also a good idea to take the sharp edges off of the metal. Do this by filing the edges of the hole at an angle to create a very slight bevel. This will prevent snags and also make it look more professional. It is even more of a plus if you are going to repaint the case, but this is the subject of another article so I will not cover details here. If you were careful when you cut the hole, a couple of passes with a damp rag should take care of any scuffs made on the finish by the saw.

Installing the window is the tricky part. The plastic you need is available at your local home improvement store, or quite possibly at a craft store or a place that frames pictures. Don't buy anything thinner than 3/32" as it will crack very easily even at that thickness. Don't buy anything much thicker than about 1/8" either, as it will be difficult to mount. The plastic comes with a protective coating on it, usually some kind of plastic film or in some cases paper. The plastic film is easier to remove but does not provide as much protection as the paper. Leave this film on the plastic until it is ready to mount.

If you want to use a window rubber type mounting, the plastic should be slightly smaller than the window and needs to be the exact same shape. This approach is very difficult and should only be attempted by those with the proper expertise. It looks very neat, but very satisfactory results can be obtained using the screw mounting method described below if it is done carefully.

The plastic should obviously be slightly larger than the window you plan to use it for and does not need to be the same shape. Try to stick with more rectangular or square shapes for the plastic, as this will make it easier to cut. The curves on your window will hide the square edges of the plastic. The plastic can be cut using the same saw and blade you used for cutting your case up. Just be sure to support the plastic so it will not crack while you are cutting it.

The holes for mounting the plastic should ideally be drilled at the same time in both the plastic and the metal. This will help to ensure that the holes line up properly. Many different types of screws and fasteners are available at your local home improvement store for a minimal cost. All the fasteners I used cost less than $1 total. Do not use self-tapping screws or the like, as they will make the plastic crack. It is best to use some sort of screw-washer-washer-nut combination.

Pick some locations for mounting holes. These should be about half an inch from the edges of your window and should leave enough plastic to prevent breakage. Use some double stick tape and mount the plastic to the back of your window hole, aligning it so that it fills the window nicely. This is a good time to make sure that your screws will not interfere with assembly of the case. Relocate any if necessary and very carefully drill through the metal and plastic together. Drill at the lowest RPM possible and take your time to avoid cracking the plastic. After you have drilled your holes, remove the plastic from the metal and remove the protective film from the plastic. If you cleaned the rough, sharp edges off of your metal you should have no problem mounting the plastic without scratches.

And finally, the lights can be mounted using a good double stick tape and powered from an unused power connector inside the computer. Just remember that red is 5v, yellow is 12v, and black is ground.

If you want to make "round" IDE or floppy cables, Radio Shack sells some cable ties and cable wrapping supplies. Take your normal flat cables and a nice sharp razor blade and separate the flat cable into small strips of about five wires each. These can be easily bundled in electrical tape, cable wrap, or even nylon cable ties. Just be careful not to cut the wires. It works best to make a small start cut with the razor and separate the small strips by hand the rest of the length of the cable.

Enjoy modding! If you have any questions or want some ideas, there are numerous sources online. A google search for "Case Mods" will bring up countless links that may be of use.

DVDs to PocketPC

by Shawn F.

In this article you will learn how to put a DVD movie on a Pocket PC. The basis for the ratios and settings in this article were formed by using the Pocket PC 2002 O.S on an Ipaq 1910. The numbers should work for all systems that run Pocket PC 2002.

As of now the largest SD flash card is 256mb. Usually I get my movies down to 233 or 234mb, from a little over a gig. I encoded all of my movies and keep them on my computer, switching movies as I see fit. The theory is my computer is like the mother ship, and my Pocket PC is a smaller ship that needs to dock. In doing so it erases old movies off its SD memory card, which makes room for different movies of my choice. This is great to have for a plane trip or a day at the beach.

In the Spring 2003 issue of *2600*, there was an article on how to burn DVDs to CDR. One could use two of the three programs from that article. We're only going to use one - I'll explain why later. The programs you will need are all free. First you will need a media player for your Pocket PC. I use DIVX (www.projectmayo.com), SmartRipper (use google to find), DVD2AVI (www.divx-digest.com), and TMPGEnc (www.tmpgenc.net).

Insert the chosen DVD into your DVD drive. Play the DVD with any type of media player (Power DVD, etc.). Click on Smart Ripper while the movie is playing and watch the magic happen. Smart Ripper will copy the DVD onto your computer as "VOB" files. This will take a little bit of time depending on your computer.

After the VOB files are on your computer you will need to use DVD2AVI. There are many other programs you could use such as DVDX, but I like DVD2AVI because I'm a little anal-retentive. Little things bother me and with DVD2AVI I can choose the setting for a really good movie quality, have that particular movie encoded in a folder on the desktop into an AVI and a WAV file giving me the "recipe" to make and tweak that movie as I see fit as many times as I like. I can keep the WAV and AVI files and get rid of those VOB files.

You now should have VOB files in the particular place you chose to save them. Open DVD2AVI >

FILE: > Open > Navigate to the folder that contains the VOB files > Open VOB1 with version 1.76 of DVD2AVI. Once you choose VOB1 it knows to add the rest of them. If you do not use this version you may need to add them manually by simply clicking the add button.

VIDEO:
iDCT Algorithm > 32-bit SSE MMX
Field Operation > none
Color Space > YUV 4:2:2
YUV RGB > PC scale

AUDIO:
Track Number > track 1 (because it's usually English)
Channel Format > Dolby Digital
Dolby Digital > Decode
Dynamic Range > Control > Normal
Dolby Surround Downmix > MPEGaudio > Demux
48->44.1KHz > high

OPTIONS:
Process Priority > Normal

FILE:
Save as > choose a name and place to save your movie. A video compressor window will appear. Select the type of movie compression you want. Personally I choose MS MPEG-4 3688 VI. Choosing any other type may require a codec, but that's a different article. Click the OK button and wait. This will take a few hours depending on your computer. When the encoding process is done you will have two types, an AVI and a WAV.

Now that you have your WAV and AVI files you need the program called TMPGEnc. (VirtualDub (www.virtualdub.org) is also a good program, but this article is oriented towards TMPGEnc.)

Open TMPGEnc > Video Source > Browse > open up your wave file > Audio Source > Browse > Open WAV File. Select the Settings buttons and see the below chart for the Video, Advanced, and Audio tabs. The select the Start button and sit back and relax. If you used my settings (in bold) on the chart, you will have an mpg in a couple of hours that can fit on a 256mb SD memory card. Good Luck.

Settings for TMPGenc

Video

	Really high quality, could use with the 512mb or 1GB SD cards (not yet available) >256mb	Still good quality, could use with the 512mb or 1GB SD cards (not yet available) >256mb	Lower quality <256mb	**My Settings** <256mb
Size and pixel rate	320x192	320x144	240x160	**208x128**
Aspect ratio	1:1(vga)	1:1(vga)	1:1(vga)	**1:1(vga)**
Frame rate	>25 fts	>25 fts	>25 fts	**>25 fts**
Bit rate	400	350	300	**225**
Motion search precision	Highest quality [very slow]	Highest quality [very slow]	Highest quality [very slow]	**Highest quality [very slow]**

Depending on your Pocket PC you may have to change the bit rate, size x pixel rate, or frame rate. The lower you go with these values the lower the quality. But the file size will also lower.

Advanced

	Standard	**What I Use**
Video Source type	Interlace	**Interlace**
Source Aspect Ratio	16:9 525 line (NTSC)	**16:9 525 line (NTSC)**

Audio

	Standard	**What I Use**
Channel mode	Stereo	**Mono**
Bit rate	96	**64**

It's only a Pocket PC. Use mono - it will save some space. If anyone has questions, corrections to my article, or a different way that he or she prefers to encode video to their handheld, e-mail me at Waxycast@hotmail.com

One last tip: don't use a USB card reader/writer when putting movies on your SD memory card. It does not work. You must use active sync with your Pocket PC.

More Xbox Fun and Mischief

by spite
spite_fowl@yahoo.com

Disclaimer: I take no responsibility for what you do to or with your Xbox. This is a purely educational read. I do not claim to know anything in depth about the Xbox. This is merely a primer to get you interested in the Xbox and explain a little of what you can do with it. If you don't understand something or feel I left something important out, check out the sites at the bottom and I'm sure you can find what you need.

Microsoft's first console outing has been received with varied success. You could label it the second most successful console in the States, seconded only to the PS2. In Japan it hasn't garnered nearly as big of a reaction. Of course, not only games or licenses are the sole reason for its success in America. The potential of this system goes far beyond what you see straight out of the box. Many things I mention in this article have been discovered due to the great many intelligent and creative hackers in the Xbox scene.

Xbox Hardware

The Xbox is made up of basically an Intel 733mhz Celeron notebook processor, an integrated nVidia video processor, EIDE DVD drive (mentioned later), and either an 8 or 10gb EIDE hard drive.

Before doing any modification on the XboX hardware or software, you *must* modify your Xbox BIOS. The safest way by far to do this is with a modchip. Modchips for the Xbox come in a variety of options. You can get no solder "pogo-pin" chips like the Matrix. You can get solder/pogo pin/clip modchips like the Xcuter2. You can also get cheaply manufactured and flashed mods from a variety of people and places. The only thing you need to remember when buying a modchip is that you need *one* feature above all: To circumvent the Xbox reading the Microsoft BIOS, but for it to read whatever other BIOS you'd like to use. I will not go further into installing a modchip as you can find instructions anywhere you buy one, though I will recommend a Matrix chip. It is by far the easiest to install in my opinion, especially if you have no soldering skills. If you can solder, the Xcuter2 comes highly recommended. Read more about this at the sites I list below.

Before we talk about the drives inside the Xbox, let me notify you that you cannot just open up an Xbox with your standard Philips or flathead screwdriver. That's all you have/need? Well, expect to encounter Torx10 and Torx20 screws. Torx20 on the case of the box and smaller Torx10 inside.

The DVD drive is using special firmware for an Xbox. There are three manufacturers known for these drives: Thomson, Samsung, and Philips. There is a very important difference in these drives in the amount of media they may or may not read. At the bottom level is Thomson, which can of course read pressed CDs and DVDs, including the Xbox pressed DVDs. They can also read CD-RWs with a varied amount of success depending on brand. They cannot read 99 percent of CD-Rs you may find. The Philips is akin to the Samsung except it has a more successful rate with CD-RWs and especially CD-Rs, yet it's still not entirely compatible. The Samsung is the holy grail of Xbox DVD drives. It can read a staggering amount of CD-Rs and CD-RWs. DVD-R and DVD-RW have varied success on all brands, but as far as I can tell up to this point, only Thomson can read DVD+.

The DVD drive connects with a standard EIDE cable connecting back to the Xbox mainboard. The power cable is a proprietary cable used specifically for the Xbox DVD drive. This means no way to easily swap out a new DVD drive unless you want to attempt to open, solder, and connect a new DVD drive to this cable. There is a PC Samsung DVD drive that *can* be modified - both hardware and software (firmware) - to be compatible with the Xbox providing the ability to play Xbox pressed DVDs as well as every other media you can throw at it. You can find more information about this at some of the sites I list below.

Thankfully the hard drive is a bit easier to swap. The hard drive is using a flat EIDE cable with only two connections (one for the HD and one for DVD), leaving nothing open for future hard drive expansion (of course!). Your hard drive comes locked to your specific Xbox using a code that is hard coded into your Xbox. It is formatted with a file system called XFAT. If you're not happy with that 8 or 10 GB hard drive, don't fret. You can easily replace this with up to 120 GB! First let's talk about the connections. The hard drive also runs off the EIDE cable coming from the DVD drive. The hard drive *does not* use proprietary power connectors like the DVD drive. It uses a standard cable like you'd find in your PC to connect any other IDE drive. The only difference is that it only has *one* connector available! That of course is being used by your hard drive. Again, don't fret; you can easily plug in a splitter for this power cable to give you another connector. This means you *may* be able to connect a PC DVD drive using this extra power connection and removing the EIDE cable from the stock drive to your PC drive. This opens many possibilities but also many problems, such as having to open the Xbox DVD drive to open the PC drive, having to mount the drive on top of the stock DVD drive, etc.

As I said earlier, the Xbox hard drive is locked, meaning it will not function outside of your Xbox because of the key hard coded into your hardware that it needs to read. Don't worry, you can easily replace the drive and the new drive will operate with or without this code. This hard drive is said to be "unlocked." The disadvantage to this is that you cannot run this hard drive like an unmodded Xbox would. Don't expect to use the MS Dash (explained later) and play on Xbox live with that hard drive. It is possible to lock a new hard drive (depending on brand and type) but I will not be going that in depth in this article. Again, look at the sites at the bottom for more reference to this.

You know about the hardware, replacing drives, etc. but you still only have your MS installed software, so it does you no good. Now I will talk a little bit about the software modifying.

When you first get your modchip, it will most likely be unflashed for legal purposes. This means that if you do install it, your Xbox will either see no BIOS, or boot up its own MS installed BIOS, which is no good to us. Depending on the chip you get, you may have different options for flashing it. I will talk about the Matrix chip which is what I use, but mostly anything you get will be flashed in a similar fashion. When you purchase a Matrix modchip you will receive a flasher with it. This flasher has a standard 9 volt battery connection, a small naked 8 pin male connection, and a standard PC parallel port connection. First, find whatever hacked BIOS you want to use. I will not tell you where to get this, but with a little bit of exploration I'm sure you can find it. You need a program to flash this BIOS to your modchip. Again, I will not tell you where to get it, but hey, you should be able to find this stuff on your own. Remember these next steps, because you *can* screw something up if you do it wrong.

Connect the 9 volt battery to your flasher.

Connect the modchip to the 8 pin male connection on your flasher.

Connect the flasher to the parallel port of your computer.

Open your flasher program, select the BIOS you wish to flash, and *flash it!* Once you verify the BIOS is flashed onto your modchip, it's time to install it into your XBOX.

Depending on the BIOS you use, it may modify the Xbox booting sequence to let you know that the install has been successful. See documentation for your modchip and BIOS for any information on installing and verifying your install.

Now that you have an Xbox running off this new BIOS, the possibilities of what you can do are *endless.* I'll briefly go into a few things that you can now do.

Install a New Dashboard

Boot up your Xbox without a game and you'll see a nice green animated menu that lets you explore your memory space, songs ripped from a CD, Xbox preferences, etc. This is your Xbox dashboard, from now on referenced as your MS Dash. There are a few different dashboards you can pick to install to replace this pretty but restrictive software. Most widely known and used is the Evolution X, or Evox Dash.

Find the Evox Dash software, preferably in ISO form, and burn it to whatever media your drive can read. Boot up your Xbox with this CD and *voila,* you're running the Evox Dash. From here you can discover something new your Xbox can do. Notice that little port in the back of your Xbox that looks suspiciously like an ethernet port? Gasp - it *is* an ethernet port! Find a crossover cable and connect this to the NIC in your PC and that simply you are connected. Fire up your favorite FTP client, find the Xbox IP settings in Evox, and connect to your Xbox. Here you see your Xbox hard drive's directory structure: C,D,E,X,Y,Z.

The C drive stores your dashboard software. In there you can replace your MS Dash board with Evox so that you won't have to boot up with a CD-RW or whatnot every time. Remember to *back up your Xbox hard drive before editing, changing, or deleting anything.* It's not that big *so just do it.* You'll thank me later if you make a mistake. Sending files to and from your Xbox is just like FTPing to any site and transferring files, so just replace it outright, rename it, whatever, and you'll have Evox boot up as your default dashboard.

XBE, what the heck is that? You most likely have seen it by now. XBE is the Xbox's version of the windows .EXE, aka an executable file. Your dashboard will have an executable file, most likely called evoxdash.xbe or default.xbe, etc. Some BIOS' are made to look for specific XBEs on boot up, so again read your documentation.

Now that you have a modded Xbox, a new dash, and a network connection to your PC, what else can you do? Well, just about anything. There are *many* pieces of software made by Xbox hackers to do just about anything you want. Want to watch a movie file, listen to an mp3, and browse jpegs? Check out Xbox Media Player. It has the built in ability to play tons of formats in a very nice GUI system. If you want to play these files straight off your PC through the network, check out ReLaX. You can set up network drives just for your Xbox and stream these files right through media player. Want to play your Xbox games but are sick of swapping DVDs? There are many apps that let you install the game files onto the hard drive itself and you *never* need the disc again. Want to play all those consoles of the golden years? There are emulators for damn near everything. PSX, SNES, Genesis, Mame, just look and you can find it all.

Of course we've not discussed nearly everything you can possibly do with this system. Let's talk a little bit about the operating system that runs default in the Xbox. It's basically a watered down, non-desktop version of Windows 2000. Can't tell, can you? How about running Linux on the box? Not possible? Well, it is. Run a standard Windows OS? Also possible. Just look and you may find!

Just a quick closing remark. What would a system admin think if he traced you back and discovered you were port scanning him *on an Xbox?* You know what I'm saying *(wink)*.

Here are a few sites to quench your thirst:

www.xbox-scene.com. Highly recommended. Tons of articles, faqs, links, everything. Go here first and read.

www.gamebuy.com. I've bought from them in the past. If you need a modchip, go here. Great service, quick shipping.

www.xemulation.com. Good info on the emulation on the Xbox.

Shopping For a Security Flaw? Try Retail.

by dead_pilgrim

Author's Note: System vulnerabilities described in this article should be used for the sole purpose of improving and fortifying weak systems, and not to inflict harm, steal, or act in any other malicious fashion.

Within the past few months I have discovered that there are serious security holes within retail store systems and networks. The flaws range from open modem ports to computer ignorant employees. All of which could give you the keys to the kingdom.

Let's take a look at open modems, or modems that are set up for service by vendors or the tech support staff of the company. These modems are installed with most systems. They are often set up when the store first opens, or when the network is first built. After that, the modems are lucky to ever receive use. You can use a war dial program like PhoneSweep to harvest modem numbers. Then you can determine whether you can connect to a retail store's system. Within a three hour sweep, I found eight modems connected to various retail systems, all of which accepted incoming transmissions!

What can you do with these modems? Well, one could download a program called ZOC (this program, as well as PhoneSweep are available from download.com, Kazaa, or Emule). This program is very useful in this situation. It allows you to connect to the modem by dialup and emulate a number of different systems. Many retail systems use telnet or TTY. Again, you can fumble around with the program to see what works the best.

Many major retailers use HP9000 or IBM servers powered by UNIX or NT. They usually use Cisco routers (models 2600 or 2500 are usually standard issue). You would think that a smart business would use a firewall, right? Not usually. Seven out of the eight systems that I found during the war dial session were not protected by a firewall. The most common method of protection was a username and password.

Passwords on these systems usually require a username or password. One could use a brute force attack, dictionary attack, or just try to guess the default password. That's right! Many systems still have the default usernames and passwords set. If you search within Google Groups you can more than likely find a list of the default passwords. If these do not work one could always use social engineering to obtain a username and password. Some companies have in store employees that perform updates on these systems, and they are familiar with the passwords. Or you might try to get a system password from a regular sales associate. A majority of these employees are computer illiterate. You could easily call the store stating that you were with the company's IT department, ask to speak with someone that might handle the store's computer system, and engineer a password from them. Retail stores usually do not hire in house techs.

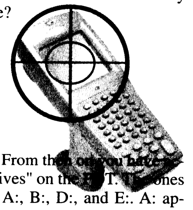
Retail store networks and servers contain a literal cornucopia of information ranging from sales information to server access. I'm sure that the competition would be very interested in sales figures, movement of product, or some new marketing idea that the company is about to deploy. This is where it hurts the most. Most companies work hard to keep sales figures under lock and key, and it's sadly ironic that someone could possibly access this sensitive information from the comfort of their own home.

Sometimes you can also gain access to the store's PBX system. The most common PBX system used in retailers is the Lucent Definity Series. The operation manuals for the Lucent PBX systems are available from Lucent's website in PDF format. If you read these manuals, you will find that there are all kinds of awesome things that you can do with these systems. I'm going to save this subject for a later article.

Granted that not every hacker is interested in the sales figures or marketing information of the local Shoe Emporium, but someone could make a cool amount of cash selling this information. As long as there is competition there will always be a market for this kind of industrial espionage. If they were not interested in selling this information, they could always create some serious havoc, such as removing network devices or changing store system passwords. I wonder if I put on a Verizon, SBC, or AT&T shirt and hat (which you could probably find at your local Salvation Army), walked in to the local super shopping center, and asked to see the store's network or telephone system, how far I would actually get. Since most of these people are improperly trained, I'm sure I could infiltrate the system very easily.

Most of these store systems are designed and set up by very inexperienced system architects, which makes the perfect environment for security holes. Perhaps they should start thinking on the defensive. What self respecting corporation would allow themselves to be brought to their knees by some hacker that found an extremely obvious security hole?

Troubling ⊙Target



by redxlegion
redxlegion@yahoo.com

The inspiration for this article came from an earlier article regarding Target's computer systems, but not so much the PDT/LRT. This article should hopefully fill some gaps. (That is, if I can tame the A.D.D. long enough to form complete and orderly sentences.)

[First of all, for reference, you can make colons on the Symbol 6800 48 key keyboard with Func, Ctrl, O]

To begin with, the Symbol 6800 series PDT/LRT is basically a microcomputer with an annoyingly sized screen, gun-like shape, and barcode scanner at the "barrel" end. They communicate with wireless access points throughout Target buildings over an RF network similar to the type you buy for your home. It's simply ordinary 802.11b. The WEP key might not be easy to extrapolate from network communication, especially not from outside the building where signal strength is pathetic, but should be easily gained from the PDT/LRT (which is from now on known as the PDT in this article, for sanity's sake). Simply reboot the PDT (by turning it off, holding 4 and 5, and then turning it on again) and Ctrl+C during any point in the bootup process. It'll break right out of those annoying batch scripts. From then on you have access to numerous "drives" on the PDT. The ones I've documented are A:, B:, D:, and E:. A: appears to be where the DR DOS OS itself resides. B: Doesn't appear to be more than a mirror of A:, but I could easily be mistaken. E:, however, is very interesting. It contains all the software for operation of the PDT. The software involved is really just a terminal program and some configuration programs. All those files should be contained in the directory ATV3000. Within the root directory of E: there should be a file called net.cfg. Can you guess what's in there? The WEP key mentioned earlier. The good news is you can also get the login information such as user ID, password, and terminal init string, which are vital to accessing the terminal server's applications. Even beyond that you require an employee ID to log onto the network. Those aren't even close to difficult to obtain. You can generate them yourself, in your mind. I've done so on several occasions, being very successful. One such number I came up with was 2922854. It functions as an employee ID and is accepted, but I can't verify if it's actually an employee's ID. Anyways... back onto the point.

You'll want to copy the file roiconf.fil from D: onto E:. The storage on the PDT is a type of flash memory, so you'll have to type in "flashctl /w" to enable flash writing ability in order to copy the file. After you enable it, just type "copy E:roiconf.fil" while you're sitting on the E: drive. You can close the flash control program with "Flashctl /ro" which may later on be a good idea because it eats all available memory on the PDT. Not right yet though. It has to be enabled for options to be saved. Now you can run tncfg3.exe. That's the terminal config program. Of all the configuration programs on the PDT, this is the one you'll have the most fun with. You can make the beeping noises go away completely, if they so annoy you that you consider strangling your nearest Executive Convoluted Team Disseminated Department Leader. Not only that, but you can enable your PDT to scan any type of barcode, even ASCII and control characters. I'm not sure what option those are in directly, but you'll know when you find them. When you reach that menu, you can use the up and down keys to flip through the various barcodes you can enable. Press enter to enable disabled barcodes. You can use the left and right keys to move the arrow up and down to select various aspects of the barcodes. When you find a barcode that asks for "Enable ASCII No," change that to yes by pressing Space (Func+Backspace). Don't worry about the min or max. Leaving them at zero will do no harm or good. Now exit tncfg3. Reboot the PDT. It'll cycle through all its annoying nastiness as per usual. It'll eventually reach the login prompt where you put in your employee ID. Put in whatever you want. But before you do that, follow the next step....

You should've done this the night before. Sorry I didn't mention this earlier, but perhaps now you'll know for later, and can perhaps just entertain yourself with the configuration options. This is for those who really want to trouble Target. Just note, this hasn't yet been tried. Now fire up Mozilla, Opera, whatever, and visit http://www.telepen-barcode.co.uk/barcode-generator.asp. *[Gaping evil grin.* If you're familiar with "A Nasty NT Bug," you may know where I'm going with this. I may be completely off my rocker, but having the server output a tab followed by backspace characters should crash the system, correct? Well, that handy dandy website will output for you a jpeg to print if you enter in [9][8][8][8][8][8][8][8][8][8]. Keep that barcode handy for what happens next.

All right, you've logged onto your Symbol 6800 PDT. You're at the foolish menu of the damned, and instead of inputting a number, type in "Loop" and hit enter. It's a program that's not explicitly mentioned anywhere in any documentation on any of Avalanche Wavelink's (the client/server package Target uses for PDTs) website or any such thing, at least not that I know of. It's just a simple program where the PDT scans something, sends it to the server, and the server spits back what it scanned. Get out your handy dandy barcode you printed the night before. Scan it.

You just scanned a barcode with a tab and nine backspace characters, which should bring the server to a screeching halt. That is, if I didn't interpret "A Nasty NT Bug" correctly somehow, which I'm sometimes guilty of. If my logic is right, though, you've just troubled Target enough that they'll have to suffer through an NT 4 reboot. Another detail I'm not privy to is if each store has its own server, or if the servers are regional.

I'd just like to say that I don't condone the existence of middlemen or retail in general, and I believe that people should experiment without boundaries. So learn all you can despite the ignorant masses, even if you belong to them!

BLOCKBUSTER Tricks

by C.B. Cates

Continuing on a popular topic, here are more ways that you can squeeze some of the most enjoyment out of the Blockbuster Video (BBV henceforth) in your town. The article in 19:3 was insightful on getting rid of pre-existing late fees (called EVF in BBV's industry), but there is an easy way where you don't even have to return a rental at all.

The shortcoming in the method described in 19:3 is that some stores won't even transfer balances, thus rendering the entire method useless. (To transfer balances, one must use credits, and since credits are counted as negative revenue, Blockbuster highly discourages them. Employees have actually been demoted and in some cases terminated for giving out excessive credits.)

There is a better way. First, find the barcode on the item that you don't want to return. For example, let's use the new XBOX game, *Shemnue 2.* The barcode is located on the spine and top right of the case and has 16 (in some cases 14) numbers above it. Example: 3320313843457001. The 33 is a designation number, letting the BBV point-of-sale system know that the item is a rental. 20313 is the store code (in this case bogus). 843457 is the part number and 001 is the copy number. In the top left of the front of the case, you will find the store's telephone number. You will also need to find a dummy store number that you will be calling from. The best way to do this is to just call them up or ask, or just look at any of their rental items.

Call up the Blockbuster which you rented your item from. When someone answers, say something along the lines of "Hi, I'm calling from Blockbuster in [town name here] and I have a wrong store tape(s) for you." The person you called will first ask you for your name and the store number you are calling from. He will then ask you for the item you are checking in. Tell them the barcode number(s) *without* the designator or store number (843457001), as these numbers are redundant in this situation and will raise suspicions. Thank the person and hang up. The item is now yours. Just make sure you call before the item is due or Blockbuster will still stick an EVF (Extended Viewing Fee - BBV store talk for a late fee) on your account.

How this works: Rentals from one BBV must be returned to the same store but many people don't do this. Thus, every time a tape from a wrong store is returned, BBV still needs to track your item. The person you called inputs the item into the wrong store account, thereby checking it in on your account. Because there are so many wrong store tapes when they finally get sent back to their home store (usually once during the second or third week of the month), some fall through the cracks, and this is to be expected due to all-common rampant employee pilferage and general carelessness.

Try dumpster diving at BBV as well. If BBV can't sell a used tape/DVD/game due to a licensing agreement, they are sent to field destroy. This means that the item is thrown away after being destroyed. Often, however, the field destroy list is so large that it becomes an immense time-sink to ruin each individual item, and they are simply thrown away.

Webhacking With CVS

by methodic
methodic@libpcap.net

When a project is checked out of the CVS (Concurrent Versions System; www.cvshome.org) repository, CVS creates files to keep track of the checked out project (i.e., version numbers). Normally this isn't much of an issue, until using CVS to manage web content comes into play.

The severity of this issue is pretty big. Let's take imaginary Company XYZ for example. Doing a quick search on Google you are able to find their homepage, say http://xyzinnovations.com. To check to see if they use CVS to manage their website, you simply have to point your browser to http://xyzinnovations.com/CVS/. If they're using CVS, one of two things should happen. You will either get a message saying directory listings disabled, or you should see a list of files. Either one isn't important. What's important is that you now know they use CVS to manage their website content.

Now on to the fun stuff. There are three common files found in CVS directories. They are Entries, Repository, and Root. The Root file will tell you where the CVS repository is located. The Repository file will tell you the name of the project (the website content) in the CVS repository. The Entries file is the one we're interested in. The Entries file is a list of all files and directories within the project repository. Here's a snippet from the Entries file for libpcap.net:

/patches.phtml/1.1.1.1/Sun Mar 30 15:27:37 2003//

```
D/gfx////
D/orbs////
/code.phtml/1.4/Sun Mar 30 15:48:00 2003//
/exploits.phtml/1.1.1.1/Sun Mar 30 15:48:04
  2003//
/index.phtml/1.2/Sun Mar 30 19:24:37 2003//
D/aimcrack////
```

As you can see this file discloses some very valuable information. Let's go back to our example of Company XYZ. With this information, we point our browser to http://xyzinnovations.com/CVS/Entries. Bingo. Check out what we found:

```
D/includes////
D/docs////
/robots.txt/1.1/Fri Jun 15 11:52:37 2001//
/docs.php/1.4/Thu Dec 13 10:06:26 2001//
/index.php/1.15/Tue Aug 20 17:51:54 2002//
```

Pretty interesting stuff. Company XYZ appears to be using PHP (a powerful scripting language suited for website development). Also notice the includes directory. Since we know they're using PHP, we can assume that the includes directory contains PHP scripts that the website includes when parsing output. If you haven't used PHP at all, one of the most widely used functions in web development is include(). This function allows you to include files in your PHP script. This way, web developers only have to write something once, and they can use it over and over again by just calling an include("/path/to/file"). Common examples of this include site layout (it makes more sense to edit one include file than 15 different static HTML pages), connecting to a database (if each page needs to connect to a database, why write the code 15 different times?), and so on. So let's check out the includes directory, shall we? Be sure to use the same method; don't just go to http://xyzinnovations.com/includes/ because we already figured out XYZ's website doesn't allow directory listings. Instead go to this URL: http://xyzinnovations.com/includes/CVS/Entries. You should see something like this:

```
/connect_db.inc/1.1.1.1/Sun Mar 30
  19:21:20 2003//
/header.inc/1.1.1.1/Sun Mar 30 19:21:20
  2003//
/footer.inc/1.2/Sun Mar 30 19:56:43 2003//
/close_db.inc/1.3/Mon Mar 31 16:56:22
  2003//
```

Notice the connect_db.inc file. Logic would tell you that this include file handles opening a connection to a database. Let's check it out. Since this is a file, not a directory, you can just go to http://xyzinnovations.com/includes/connect_db.inc. If this file is what we think it is, you should see something similar to this line in the file:

```
$link = mysql_connect("xyzinnovations.com",
"xyz", "xyzzyx");
```

Congratulations h4x0r.. you now know the username and password they use to connect to the company database (xyz and xyzzyx respectively). From this knowledge the possibilities are endless. How many times have you seen the same login/password used for different services? I've also seen a database server use the same login credentials for the database as it had on the server itself (same username/password).

Just to recap, to find out if a website is using CVS to manage their content, simply go to http://site.com/CVS/. In fact, since we're only really interested in the Entries file (for now), you can go directly to http://site.com/CVS/Entries. By the output, you should be able to see which lines are files and which ones are directories (the directory entries begin with a D). Using the Entries file, you should also be able to see the files under each directory by going to a similar URL: http://site.com/some_dir/CVS/Entries. Last but not least, know what to look for. I've seen it all. Include files, shell scripts, zip files of the site itself, PHP and CGI scripts with a -sav or -orig extension (the webserver won't parse those!). Another thing you can try is to see if their CVS server is available to the world (usually runs on port 2401). If you find one open to you, grab the Repository file and try to run a "cvs checkout" with the project name. Yes, I've been able to CVS over an entire website, .htpasswd and all. If you're a newbie to CVS, I highly suggest installing CVS and checking out this URL: http://cvsbook.red-bean.com/cvsbook.html.

Webhacking with CVS files isn't a well-known technique, but it certainly is one of the most effective. Not only can you retrieve files off a server that might try to obscure their existence with directory listings turned off or by dropping an index.html file in the directory, but there are multiple ways to hide your true identity. Grab an open wingate proxy, put the IP address in Mozilla, and go to town. Or just r00t your friend's Red Hat 7.3 box and use lynx --source.

I hope both sides of the fence learned a thing or two about the dangers of using CVS to manage websites. CVS is a very powerful tool to manage projects, no doubt about it; just be aware of what it leaves behind and more importantly, who's there to take it.

ShoutOuts: dmuz and the rest of the ap crew. congrats to victim1 on getting the 31336++ jobby, good luck in md. http://libpcap.net like woah.

Basics of Cellular Number Portability

by C3llph

With the possibility of number portability on the horizon yet again, I thought I'd start with explaining some of the basics and then move onto some of the more technical issues.

What number portability will allow the public to do with their preexisting cell phone numbers is similar to what you can already do, and probably get charged for on a monthly basis, with your home phone. On your land-line bill you should see a number portability surcharge. Cellular number portability will allow you to take your existing cell phone number with you to whichever cell phone provider you choose. Your land-line provider, as do cable and power companies, use public utility lines to provide you with service. This just means that no single company "owns" the actual cable or other devices that are used to provide you with their service. In some small and large towns there are some privately owned telephone companies but this still applies to them. Nothing is stopping you from either changing your service to another provider, unless no other exists, because other companies have the right to use the same cables to provide you with service.

So with cell phone number portability if you get fed up with say provider A, you can now change your service to provider B and not have to give all your friends, family, or business contacts a new phone number to try and reach you at. This was suggested to the government by businesses based upon how it costs them money to have new business cards reprinted, etc. in the event that they change service providers.

Currently in cell phones old and new your MDN (mobile directory number) is programmed into the phone or sim chip (GAIT or GSM) to match the other equipment so your provider can identify your phone on their network for placing or receiving calls. I'll use TDMA as an example. When a handset is activated either OAP (over the air programming) or manual programming is used to put the correct information into the handset. This includes the following codes: SOC (start of cell), SID (system identification), and MDN. The MDN is your dialable 10-digit mobile number, also known as your wireless number, reach number, or CTN (customer telephone number).

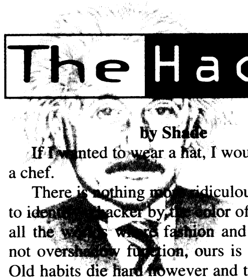
Currently on the newer TDMA handsets there is also a programmable MIN/MSID, for example on the Ericsson T61d, Motorola v120t, C331T, V60T/Ti, Nokia 8265i, 1261, 3360, and probably 3560, I can't remember offhand. The MIN/MSID (mobile identification number or mobile subscriber identification) is a non-dialable 10-digit number that the customer will not know about. If you have an older handset or a new handset that doesn't support the programming of the MIN it will be done in the provider's network anyway. This MIN is what will allow a specific provider to identify your phone to their network. They will use the MIN to keep their side of billing and provisioning of service unique to your phone. Before number portability goes into effect, if you phone has the capability for both MIN and MDN they will be programmed to the same number. After number portability begins later this year if you do decide to change providers the new provider will keep your MDN the same and issue a new MIN for their network from their specific number pools. Again, you will not know what this new MIN is and it is non-dialable anyway.

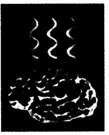
For internal billing identification and identification on their systems the provider will use the MIN to keep track of your account while your bill will show your MDN. The process for a call being routed to you is what will change.

When someone dials you number, it will get routed to the exchange and will first be tagged to your MDN. Then when the call reaches your provider's network it will be call forwarded to your phone using the MIN. This should be an insignificant delay. Dialing out from your phone will be basically the reverse. You place a call from your phone, the MIN will be used to identify you on your provider's network. Your provider will then in turn route your call to the destination, but will substitute your MDN for the MIN so the receiver's system would show your MDN as the number of the incoming call, hopefully.

So, number portability is a good thing if you need to keep your existing number and change to a different provider. To think that cell phone companies will not have any issues while getting their network to implement this without any flaws would be very presumptuous on a consumer's part. Specifically, problems will arise if someone were to try and activate an existing number with a new provider before canceling the service with their existing provider. Hopefully this has shed some light on what will be happening behind the scenes of number portability.

The Hacker Diet





by Shade

If I wanted to wear a hat, I would have been a chef.

There is nothing more ridiculous than trying to identify a hacker by the color of their hat. Of all the worlds where fashion and style should not overshadow function, ours is one of them. Old habits die hard however and today we will attempt to show you more of the well kept secrets every successful hacker holds. Today we discuss diet. In hacker terms.

Appendix C of the mythical and seldom seen *Hackers Handbook for the Initiate,* states "Garbage in, garbage out. A good hacker will know; a healthy diet high in protein is power." We spend countless hours optimizing code, file systems, networks, procedures, and other assorted black boxes, yet rarely consider the real-world impact of all that pizza, soda, caffeine and chips.

The following diet hints and tips scarcely scratch the surface of information available out there. These things may be obvious to the successful hacker, but remember what it is like to know nothing. If "Will Code for Food" is a slogan in Silicon Valley, just think of how many hackers out there who are not successful - yet.

Power Pasta

Prep time: 1 minute
Cook time: 8 - 12 minutes
Cost: $1.00

Ingredients:
1 bunch pasta
1 tablespoon butter
salt & pepper
(optional) Parmesan Cheese

Boil some water in a pot. Don't follow the instructions on that pasta wrapper, you don't need that much water - just enough to cover the pasta and allow for it to expand. Easy. Throw the pasta in, about 8 minutes later fish a piece out with a fork, let it cool so it won't burn you and try it. If it seems right, it probably is. Timing is everything with pasta, so fire up that accurate-to-the-nanosecond timer util you've been dying to have a use for. Drain the water, turn off the flame, throw the butter in, stir it a bit, season, and you're done. Parmesan cheese is optional and is only recommended if you are tired of eating the same old thing.

Pasta is complex carbohydrates. Multiple sugars chained together and difficult for your body to break down. This is good. Simple sugars are known to assimilate rapidly, give you quick energy, and attribute to weight gain if there is more than you need. Complex sugars make your body work harder before they are available, giving you sustained energy throughout the night, but not so much that you start packing on the pounds. And when your hobby does not require you to leave your seat for 14 hours a go, we need all the help we can get. Right porky?

Hackers Stew

Same as above. When pasta is done throw in a can of Campbell's Vegetable soup. Better yet next time you go out to dinner get a cup of the best house soup to go and keep it in the fridge. If it is cold, time it right and throw it in the pot after you drain your pasta, and throw your pasta on top. Heat it up fast, you don't want your pasta to turn into mush.

Almost anything goes good with pasta, and it takes a hacker to discover what all those things are. Variety in diet is extremely healthy.

Relativity Multitask Delight

Boil water, put in an egg or two. Wait ten minutes. Now comes the multitasking and relativity. Put your pasta in. Yes, the same water. Wait ten more minutes. Drain. You're done. Treat as Power Pasta, with the exception of the eggs. Turn on the cold water in your sink. Rinse your fingers in cold water, quickly grab one egg, quickly rinse it, knock the egg against the counter to crack the shell. Remove the shell. If you're slow or your fingers are starting to burn quickly rinse them again.

The goal is to remove the shell in as much of one piece as possible so it is easy to throw away and your food is not crunchy because you smashed the egg too hard. The other goal is to get all this done without your hard-boiled eggs getting cold, then at least you have a warm meal, and the dignity of preparing it. Rinsing your fingers in cold water before exposing them to heat gives you a few more milliseconds of protection against high temperatures. Hackers appreciate milliseconds.

The white part of eggs is very close to the pasta. We've already covered that. The yoke of eggs is extremely high in protein, good brain stuff. It does not taste as good as pizza, but it *is* good for your brain. So wolf down as much as you can. We're going for the end result here.

Einstein was known to cook chicken soup and use the broth to boil eggs at the same time. He was big on protein because this has been a long known aid to intellectual pursuits. We're not making chicken soup here, but we are saving time in the same way, and work our minds as much if not more than any other scientific segment of society.

Michael Crichton has simple meals prepared in the same way day after day when working on a big project, just so that he will not lose focus on the project at hand. Einstein's approach to simple cooking was the same: minimal impact on your mental pursuits, while still providing healthy food to eat. Pre-prepared meals that are healthy may not be a luxury we can all afford, but healthy fast cooking here today is the goal, and each and every time I can get my audience to avoid grabbing one of those microwave grease-boxes, we are all the better for it.

In closing I would like to say if some weekend yokel would like to base another book on an article I've written, more power to him. Just remember your roots my friend, and give credit where credit is due.

Feather.c

```
/*
 * feather.c - preserve a program's atime and mtime after executing
 * Written by Kairi Nakatsuki <kairi@phreaker.net>
 *
 * usage: feather command [args ...]
 *
 * I wrote this little ditty after a session of pondering--Do people think
 * about the fact that the access times of commands they execute are modified
 * on a read(), mknod(), chmod(), or utimes(), when trying to cover one's
 * tracks?  Some breakin attempts I've seen suggest otherwise, which prompted
 * me to write this program to sate my curiousity.  This utility is mainly
 * useful when one wants to cover their tracks further after gaining a root
 * shell.  Note that if you really wanted to be thorough about being covert,
 * make sure you use this utility in conjunction with touch(1) to set the
 * atime and mtime of the shell and compiler to pre-intrusion values.
 * Sure, one could do the very same with touch(1) after each execution, but
 * that would be tedious, no?
 *
 * On most UNIX workalikes, all that is needed to compile this program is:
```

```
 *
 * $ cc feather.c -o feather
 *
 * The functionality of most of the code is explained thoroughly for those new
 * to the scene.  You may notice that I "over-code" things by rewriting the
 * functionality of functions that may already exist; note that this is for
 * portability reasons, as I tested this bit of code on my NEXTSTEP 3.3
 * machine.  Also tested under GNU/Linux (glibc 2.2), NetBSD 1.6.1, and QNX.
 *
 * If you find a legitimate use for this snippet of code, e-mail me, as I would
 * be very impressed to know.  Don't let this program be an open invitation to
 * "own" somebody's machine simply to test it out.  This is intended for
 * educational purposes only.  Allow me to remind you to be responsible.
 *
 */
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <sys/wait.h>
#include <unistd.h>

char *appname;
extern int errno;

static void usage() {
  fprintf(stderr, "usage: %s command [args ...]\n", appname);
  exit(1);
}

/* Get the full pathname of a command. */
char *which(const char *command) {
  char *path = NULL, *tmp = NULL, *buf = NULL;
  int len, cmdlen = strlen(command);

  /* Test to see if we need to find the absolute path name of the command by
   * seeing if the string passed to which() is the filename of an executable.
   * If so, duplicate the contents of command, so the pointer returned by
   * which() can be handled consistiently. */
  if (access(command, X_OK) == 0) {
    if ((buf = (char *)malloc(cmdlen + 1)) == NULL) {
      fprintf(stderr, "%s: %s: %s\n", appname, "malloc()", strerror(errno));
      exit(errno);
    }

    strcpy(buf, command);
    return(buf); /* free() me */
  }

  /* If getenv() doesn't work, there's obviously a serious memory issue going
   * on.  (If someone doesn't code responsibly, who will? */
  if ((path = getenv("PATH")) == NULL) {
    fprintf(stderr, "%s: %s: %s\n", appname, "getenv()", strerror(errno));
    exit(errno);
  }

  /* For each element of the PATH environment variable, test to see if the
   * element, with a slash (/) and contents of command appended, is a valid
   * path to an executable.  If this is the case, return the contents of
   * buf.  buf needs to be free()d, or else we'll have memory leaking all over
   * the place.  I am a neat freak. */
  for (tmp = strtok(path, ":"); tmp; tmp = strtok(NULL, ":")) {
    len = strlen(tmp) + cmdlen + 2;

    if ((buf = (char *)malloc(len)) == NULL) {
      fprintf(stderr, "%s: %s: %s\n", appname, "malloc()", strerror(errno));
      exit(errno);
    }

    strcpy(buf, tmp);
    strcat(buf, "/");
    strcat(buf, command);

    if (access(buf, X_OK) == 0) {
      return(buf); /* free() me */
    }
```

```
    /* Get rid of buf if we didn't find our executable yet. */
    free(buf);
  }

  /* Obviously, we haven't found the full pathname of our command, so let's
   * return NULL. */
  return(NULL);
}

int main(int argc, char **argv) {
  char *filename = NULL, **args = argv+1; /* self-explanatory. */
  struct stat sb;
  pid_t pid; /* used when fork()ing.  Technically not necessary, but here for
              * correctness. */

  /* Used in error and usage messages. */
  appname = argv[0];

  if (argc == 1) {
    /* Print usage and die. */
    usage();
  }

  if ((filename = which(args[0])) == NULL) {
    /* Since which() returned NULL, assume that the command name given is not
     * that of a valid, existing executable.  Complain and die. */
    fprintf(stderr, "%s: %s: %s\n", appname, args[0], strerror(errno));
    exit(1);
  }

  if (stat(filename, &sb) < 0) {
    /* If something happened to make stat() unhappy, complain and die. */
    fprintf(stderr, "%s: %s: %s\n", appname, filename, strerror(errno));
    free(filename);
    exit(errno);
  }

  /* fork() time */
  pid = fork(); /* UNIX mitosis */
  if (pid == 0) {
    /* executed by the new child process */
    if (execv(filename, args) < 0) {
      fprintf(stderr, "%s: %s: %s\n", appname, filename, strerror(errno));
      exit(errno);
    }
  } else if (pid > 0) {
    /* executed by the original parent process */
    struct timeval times[2];

    /* wait for execution of the child process to end before setting the atime
     * and mtime back to their original values. */
    wait(0);

    /* The first element of the struct timeval array declared above always
     * corresponds to the access time of an inode.  The second one is always
     * the modification time. */
    times[0].tv_sec = sb.st_atime;
    times[0].tv_usec = 0;
    times[1].tv_sec = sb.st_mtime;
    times[1].tv_usec = 0;

    if (utimes(filename, times) < 0) {
      /* This happens because the program did not have the permissions to
       * modify the inode's time stamps.  Pity. */
      fprintf(stderr, "%s: utimes(): %s: %s\n", appname, filename,
        strerror(errno));
    }
  } else if (pid < 0) {
    /* We were unable to fork() altogether. */
    fprintf(stderr, "%s: %s: %s\n", appname, "fork()", strerror(errno));
    exit(errno);
  }

  /* Save the environment! */
  free(filename);

  return(0);
}
```

Articulated GIBBERISH

Article Feedback

Dear *2600*:

In 20:1 Acidus asks how XM expects to get CD quality sound over 125 kHz per channel of bandwidth while FM broadcasting uses 200 kHz. The answer's simple. While it is true FM has 200 kHz allocated, it uses only 30 kHz to broadcast the right and left channel of a stereo signal. What about the remaining 170 kHz? It's a combination of SCA, RDS, and fluff to cut down on adjacent channel interference.

rFmAn

Dear *2600*:

I am writing in regard to your article about XM Radio. I work for another satellite manufacturer (not Boeing). I found the article interesting, however, I can tell you that the statement that the two Boeing manufactured XM Radio satellites put out 70 megawatts of RF power was outrageously wrong. Satellites in that class typically generate 10 to 15 kilowatts of power from their solar arrays and broadcast maybe one third of that as RF power.

Matt M.

Dear *2600*:

I just wanted to comment on the article about the coupon trick. Seems the person that did this went through an awful lot of trouble when they could have simply found another product in the store, copied the UPC code, taken it home, generated the barcode, printed it out on some sticker labels, and then gone back to the store, stuck the new UPC code on the container, and off you go. Of course in order for this to work you would have to be thinking about the product you are picking up.

Australian Knight

Dear *2600*:

It is a wonder in the day of computers when we can use our "hacking" ways to go to a web site, cut and paste the coupon, and now with the help of this article we can get things free or dirt cheap. Thank you Charles for writing the article and thank you *2600* for printing the article in the last issue.

shaggyeightball

Let's not fool ourselves into thinking that actually doing what the article suggests is hacking in any sense. But it's intriguing to many in the hacker world to see just what it is that holds such systems together and how easily they can be thwarted.

Dear *2600*:

I can't help but comment on "A Hacker Goes to Iraq" in 20:1. Like Chris, my interest in computers began in the early 70's. (My first hack, in '72, was performed with an ASR 33 Teletype and a 300 baud modem.) I applaud Chris' dedication to teaching the children of Iraq, but I strongly disagree with his unsupported accusation that the U.S. was responsible for their pre-war plight. Under U.N. sanctions, Iraq always had the funds necessary to purchase food, medicines, and other humanitarian goods - without limit. It was the regime's manipulation, diversion of funds, corruption, and contempt for the welfare of the Iraqi people that prevented goods from reaching the Iraqi people (http://usinfo.state.gov/regional/nea/iraq/focus/).

My main reason for writing though, is to provide some additional material I feel was missing from Acidus' "The Flawed Future of Radio." Although Acidus provides an excellent technical description of satellite digital audio radio (SDAR), there was no mention at all of terrestrial digital radio. iBiquity Digital Corporation's "HD Radio" was approved for immediate use by the FCC on October 10th, 2002 (http://www.granitevc.com/html/news/2002Q4/10100 2.html). HD Radio is an In Band, On Channel (IBOC) technology, which means it can and will ride piggyback on existing analog FM and AM signals. Unlike SDAR, HD radio is free to the listener. That alone is enough to make it a major force in the market. According to research conducted by the Consumer Electronics Association, 48 percent of consumers are unwilling to pay anything at all for SDAR (http://www.ce.org/publications/books_references/digital_america/mobile/digital_radio.asp).

I'm sure my fellow readers will be interested to know that iBiquity has built a datacasting capability into the format, and is heavily promoting it. I won't attempt a detailed technical description of HD Radio in a letter (it's all on the net anyway), but I do want to express my surprise and concern that in all of my research so far, I have found no mention of data encryption within the standard. If encryption was in fact left out, pirate broadcasters will eventually be able to hijack the datacasting portion and send out everything from incorrect sports scores to fake pages, with the listener being none the wiser. If the broadcasters tie the datacasting sources into the Internet, well, one can barely begin to imagine all the potential consequences.

Tonio K.

Dear *2600*:

When I checked the *2600* website for the topics covered in the Summer issue, I was very excited to see an article entitled "Optimum Online and You" (because I am an Optimum Online subscriber in New Jersey). I hurried out extra fast to pick up a copy and turned right to the article. To my dismay though, I found it to be a rant about Optimum Online. Screamer speaks of "these injustices" brought down on us by Optimum Online. First, he complains about the ISA network card included in his bundle. This is not Optimum Online's fault; it is the fault of the misinformed sales person at the Wiz. Other than that, as long as you have a NIC compatible with Linux, you can use Optimum Online. Next he goes on to point out how he got an e-mail about the use of peer to peer file sharing services. Every user got one of these in December, whether they used services like Kazaa or not. In the TOS, it states that running any type of server is a prohibited use of their service. It doesn't say they can declare anything as a server. It just says it is "not limited to FTP, IRC, SMTP, POP, HTTP, SOCKS, SQUID, DNS or any multi-user forums." It is vague because they are not aware of *every* single type of server, and it is like any other contract you will sign from any other service provider that doesn't allow servers to be run. After receiving that letter I still run Kazaa and I haven't had any troubles from Optimum Online. I'd also suggest you check your Apache server because I have been running a web page off my computer for a while now with no problems. Maybe test it out with a different web server before you start pointing fingers.

Scott

Dear *2600*:

A minor point, but I feel it should be clarified that XM uses terrestrial repeaters to fill areas that the satellite signal can't reach such as in between large buildings. These are located usually on two-way radio sites near or in major cities. It is a repeater. It receives the same signal from the satellite as you do via a dish and retransmits it on a different frequency at transmitter power levels of 1,000 or 10,000 watts. The XM repeater I saw looked like a generator housing with air intake and exhaust vents on the ends. It was a cute little white box with a large XM logo on the side. It has since been removed as they found coverage from the satellites was much better than predicted.

The subscriber XM radio has a diversity receiver that looks at the data stream from both sources and chooses the less corrupted one to give the best reception. The only control XM has on the repeaters is diagnostic. When your activation or deactivation signal is sent, it is sent via satellite and repeated by *all* repeaters. XM doesn't know or care where you are in their footprint, except for billing purposes.

As for bandwidth, they don't need 125 kHz to send a high quality stereo music signal. A regular FM station using a digital studio to transmitter link needs to have as close to zero latency in the signal to keep from driving the DJ nuts with processing delays so they use a very wide band low compression signal. XM doesn't need that. They can compress the crap out of the signal getting it down to around 56K. 56K ISDN lines were/are used heavily by radio stations for remote broadcasts. Voice can be compressed even further. Even with all the overhead for program ID's and command signals, I suspect you will find that XM can squeeze quite a few more channels.

They, like Sirius, the other satellite radio company, are very close mouthed about encoding algorithms. The articles I have seen indicate they are continuing to work on them in order to improve error correction and depth of compression.

Analog666

This would be a great technology were it not in the hands of corporations who have no interest or obligation in providing access to anything outside of the mainstream. The agreement they made not to ever use their terrestrial repeaters to broadcast locally (which could be done fairly easily) is equally pathetic.

Dear *2600*:

When I got to the last article in this quarter's issue, I found something quite interesting to me: how to make XP non-activating and able to be installed on multiple systems with just one purchase. Reading further into the article, I found that this solution was no better to me than downloading the DevilsOwn corporate edition of XP and slipstreaming the cracked service pack into the iso myself. The entire process relies on P2P warez solutions in order for the "cracking" to work. The only difference between this solution and downloading a full iso yourself is the bandwidth you save by buying the disc instead of downloading it.

mojomonkee

Dear *2600*:

The "Peeling Grapes" by Bryan Elliott referred to using a programming technique for archiving a website. Fortunately, clever people have already done the coding for this. Try the "HTTrack website copier" (http://www.httrack.com) - a free utility. It has numerous filtering options.

Al

Dear *2600*:

In addition to the article written in 20:2 regarding the Nokia 3360 and 3361 I would just like to add that the hack works on more then just those two wireless handsets listed in the article. I have used the hack on my Qwest registered wireless handset - a Nokia 3285 - for a year now. While the standard *3001#12345# code dropped me into the service menu, I ran into a problem trying to access any important menu options such as changing the NAM and Alpha Tag. Instead of all the options for NAM1 all I got was a prompt asking for a "Srvc. Prg. Code." At the time I already had a newer handset and the 3285 was just a backup phone. I searched high and low looking for that damn code to no avail. I got lucky when I decided to practice my social engineering skills. I reported to Qwest that my current handset had been stolen and I needed to transfer the service to my backup phone, the Nokia 3285. The operator was happy to walk me through setting up my old handset including the locked NAM and Alpha Tag section!

In some of the older Nokia phones the emergency number section can store up to a 10-digit phone number and when any number from that menu is dialed, it drops the handset into Emergency Call Mode. While in Emergency Call Mode E911 is activated (if equipped) and no incoming calls can be received by the handset until the user ends the call and then exits the emergency call menu. This also makes any calls in emergency mode free of charge.

In most of the phones where I've used the hidden menu hack I have seen a menu item named Field Test. When you drop into that menu you have two options: Disable and Enable. (Disable is checked by default.) Choose Enable, restart the phone, and use your scroll keys on the phone. You should see field testing information. While I have no idea what the hell those mean, I'm sure some if not all of that information could be of use to somebody. Now if you press the menu button once and scroll through the menu, at the bottom of the menu you should see another menu item named Field Test. Dropping into that menu item will give you a couple of different options depending on the phone and SW ver. you have.

JL

Dear *2600*:

FragSpaz ("Fun with the Nokia 3360/3361") in 20:2 is correct in his guess that the *3001#12345# field test mode applies to other Nokia models. On mine (a 5160 TDMA phone), when you enable Field Test you get an extra menu item (perhaps only after you power-cycle the phone). From that menu screen you can choose a variety of field test modes with a two digit number. Your normal idle screen then provides additional information, such as whether the mobile is on the digital control channel (DCCH, as opposed to analog), what the SID (System IDentification number) is, RSSI (signal strength), and so forth. If you get tired of this, you can select field test mode 00 and your idle screen returns to normal, but you still have the extra menu item available for when you want to explore some more.

D1vr0c

Dear *2600*:

In 20:2 in the article by Lucky225, he had some scenarios that wouldn't pan out too well if he called the telco where I work. If you need information on an account you need to verify the last four digits of the SSN. Now this usually isn't too hard to get, but if you start a call like some of the ones he mentioned you would need to be prepared I would think. Many places require some sort of verification now today. I can see some of these scams working about 20 or 30 years ago but not in too many places today. I can agree that occasionally a customer service rep may forget to ask for this bit of information but it is pushed pretty hard where I work because of regulations.

mAineAc

If your telco is a local provider, then you probably already know that customers aren't required to give out their social security numbers. Wireless companies are allowed to ask for this information since they generally run a credit check on potential customers. But in any scenario where humans are involved, mistakes are possible and a good social engineer can figure out how to exploit them.

Dear *2600*:

In response to the article "Fun with the Nokia 3360/3361," you mentioned not being able to do anything with field test mode and I have some information about that. After entering the code and setting field test to enabled, turn off your phone then turn it back on again. If you go into your menus you should see a new option called Field Test. Press Select and you should see Group/Display and the ability to enter four numbers. Enter 21XX where XX is 01 through 09. At that point you should be brought to some screens with a bunch of data on them. You can press the up and down arrows to scroll through the nine pages. The only part I was able to figure out was around 07 through 09 which seem to be the various towers you are connected to and their signal strength. If you or anyone else finds out what the rest of the numbers are let me know. To get back to the normal screen go to the Field Test menu again and enter 0000. Hope this was helpful.

Jim

Dear *2600*:

I just got 20:2 and it's a good one! ddShelby's article on 802.11 reception tricks is very interesting and sure to get lots of people out there experimenting. I'd like to add a few comments on it though. The "N" connector, the big one in the photo, is an old design dating back to the 40's at least, and was designed by Paul Neill, who went on to co-design the BNC connector with another engineer named Concelman. The name BNC stands for Bayonet-Neill-Concelman. The TNC is a Threaded Neill-Concelman, and a connector that I think does not get the respect it deserves. BNC's are good for quickly connecting and disconnecting, TNC's like N's are threaded and better for somewhat more permanent connections, and less noisy especially where there's vibration. I have found some very... interesting ideas of what BNC stands for out there, but trust me the B is not for British! And reverse polarity connectors are pretty rare, although keep in mind all these connectors have male and female. You can find a good rundown on connectors at http://rf.rfglobalnet.com/library/ApplicationNotes/files/2/johnson1.app.txt.htm where you'll also hear about the SMA, SMB, SMC.... SMA and SMC connectors are really good for 802.11 operations since we're not talking about watts here. Transmitters are low power and cables are that thin bitty coax. The reason N connectors work well for making your antenna is that there's that nice center solder pin to make your "probe" in your can or waveguide antenna. I have heard all kinds of reviews of these Pringles can etc. antennas, including that it's the worst antenna one reputable lab ever tested! I hope to be living in the Bay Area ("802.11'ville" to its friends) within a month and hope to do some experimenting myself.

My second comment is about the dBm measurements being thrown around. A decibel is a logarithmic measurement that's just in relation to a signal. You can increase two different signals by 3dB, but one might be a microwatt and one a kilowatt. Yet it's still a 3dB increase. This is confusing and kind of a floating, vaporous idea even to some engineers so they invented the dBm, which is dB's in relation to one milliwatt. RF engineers talk in dBms a lot. A good article on dBm's is at http://www.privateline.com/decibel/decibel.html and in fact I recommend that whole site - it's pure mind candy. If you have a good RF power meter (no, not a Bird, I mean a good one with a very sensitive probe, think Agilent) you *can* measure the gain in your can'tennas in dBm, but for most of us what you're going to have is the little signal strength bar graph thingie on your puter, or in slight differences you'll get "threshold" effects like less dropouts with Antenna X than Antenna Y. And there's nothing wrong with that! If you can get three more signals with this antenna than that one, then "this" antenna is a better one. Also keep in mind that can and waveguide antennas are directional. The RF wave has to go into the opening, so the opening has to be pointed at the signal source, or in some cases a reflection. A Pringles antenna might be, say, better than the antenna built into your lappy, but it might not be as good as the 10-element Yagi you sit down and build if you're ambitious.

By the way, I'm going to anger some people, but those "wifi log periodic" antennas you see advertised look cool, and may be an improvement over your built in antenna, but LP's are made to cover a wide range of freqs fairly well, not one freq really well. You see the log-periodic principle in TV antennas on rooftops because broadcast TV actually covers a *wide* range of freqs. If you're just interested in one freq, it's really easy to just build something better for mucho cheaper. For a single-freq antenna for what we're interested in, 2.4 gHz satellite dishes built for 2.4 gHZ are probably top of the heap. Many bucks and RF-wizard manhours went into those. They're made to withstand weather, don't have elements to get bent, etc. They're not stealthy but if you can get away with a windowsill mount, chances are no one will notice it's pointed in a funny direction. If someone does notice, tell them it's sick. Now, think about the delicate aiming process involved in setting up a satellite dish - those are directional too. I personally feel some people should turn their robotics skills towards making a motorized X-Y mount for windowsill/rooftop 802.11 antennas, since that would be ever so much more fun than going back and forth from the computer to fiddling with the antenna. For wardriving I'd look at a can or waveguide design.

And while you're having all this fun with RF, consider getting your ham radio license. The info about that (and a lot of stuff about antenna design and building stuff) is at http://www.arrl.org.

Eeviac

Confusion

Dear *2600*:

I've noticed that this site meetup.com is getting a lot of press lately. It is a site that is organizing individuals who wish to meet in the flesh-world to discuss their common interests. There is, of course, a section for *2600* meetings; I suppose that was inevitable. I would suggest that people simply use meetup.com as a way to meet other hackers and then devise their own sites/methods for discussing the meetings and their interests. Meetup.com is fairly limited in its abilities but they have a *pay* service that allows members to perform many more functions. I personally don't like the idea of meetup.com make a profit off of the nonprofit interests of any group, much less *2600* meetings. Perhaps you could suggest that people use their own sites for organizing once they meet each other on meetup.com? Plus, the freedom derived from doing it yourself is a bit more in line with the hacker ethos, wouldn't you agree?

Manga

We agree completely. Read on.

Dear *2600*:

Do you guys know about http://2600.meetup.com/? Firstly, are they lame? Secondly, are they official? Thirdly, why oh why have they got the London meets so blatantly wrong? They have missed out on our meeting point which has been the same for over seven years. I am just wondering whether you are aware of these plonkers.

netj

We've been made aware of them by numerous complaints from readers and meeting attendees. While they could potentially provide a service in helping new meetings start, they're doing nothing but confusing people by showing conflicting listings in existing cities. We've asked them to kindly knock it off.

Dear *2600*:

In your response to Captain B's letter, you refer to articles needing to abide by "guidelines" before they get published, then go on to say they must also follow a "certain level of standards," and then a "stipulation." I'm a little confused, as a guideline consists of a way to help direct someone in the proper bearing for whatever that someone is doing. There are no set rules. A standard is quite different. You must meet certain requirements, follow certain processes, or follow certain rules. A stipulation is a requirement. Which is it, as you then go back to saying that your readers and future writers should "see" the value of these guidelines?

Also, you point out that it's a disservice to reprint information that readers could obtain somewhere else. Strange you would say that, as that was not your mentality nor attitude when trying to help out Kevin Mitnick. I'm sure you would have encouraged distribution of any information pertaining to the case. In fact, you did encourage it. Anything to get the word out, right guys? Well why would you take a different approach for any other hacking related topic? Isn't the point here to free information for everyone, no matter if it's on the Internet or in any other publication?

Sph1nx

We seriously doubt your confusion is being caused by anything we said. We really can't make our article policy any more straightforward than we already have. But to restate it, as a rule we don't want articles that have appeared elsewhere, either in publications or on websites. There are exceptions, especially when it's very unlikely our readers would have discovered these articles on their own because they were in a different language or on a website few people visit.

As for reprinting information, again, your confusion has taken the wheel. Getting the word out on a particular issue or campaign is not the same as reprinting information that's already easily obtainable. You'll find that in the Mitnick case, we didn't reprint material from a website or previously printed article. We published original material and that is what we want to continue to do.

Newbies

Dear *2600*:

I am writing this letter in hopes that something will change. I go by the alias MarBle`. I am an up and coming hacker but I don't even like to call myself that. I am what most people would call lame. But it's not entirely my fault. I have been searching for months to find one person or a group of people willing to help in my search for knowledge. I know it is mostly up to me but when I find something interesting to learn and ask for help, I get laughed at and insulted. According to the documents I have read about hackers we are supposed to be an entire community dedicated to gaining, using, and most of all, sharing our information. How am I supposed to learn anything if I am constantly getting laughed at and insulted because I don't know things that I am trying to learn?

MarBle`

This is one of the questions we're asked all the time. We get letters like yours constantly. What you should try to understand is that hacking isn't something that's taught like a subject in school - except by those people who don't get it and think it can be taught like a subject in school. That's why you'll see conferences and seminars dedicated to teaching you all about hacking and hackers so that you can think and act just like them. But that's just not how it works, as anyone who's a hacker can understand. The knowledge comes from experience, dedication, experimentation, and lots and lots of time spent pursuing things that most people believe are a complete waste of time. And most of this is a solitary endeavor. That's why you meet with resistance and a bit of ridicule if you ask people to help you become a hacker. Nobody can help you with this. You have to put in the time and the effort and once you've figured a few things out and hopefully made some discoveries of your own, you'll have something to share with others who will then reciprocate. Of course, there's always the risk that the people you believe to be hackers are simply going around calling themselves that to impress people and they actually have no interest in opening up their little clique to anyone else. Those people will ridicule you no matter what you do, unless you convince them that you're an asset to them in which case they'll start asking you to help them learn how to become hackers. Does it make sense yet?

Dear *2600*:

I am in Germany working for the Army. What do I need to do?

Henry

Proceed with the original plan. You'll be contacted.

Dear *2600*:

First off, I know lots of kids read this mag who want to learn how to hack so I took my time for all you noobs out there to start learning and telling your friends that you're an evil hacker.

1. Learn programming languages. (I know most of you don't want to waste hours a day doing this, but there are no shortcuts to becoming an elite hacker.)

2. Learn how to operate IRC channels and HTML.

3. *Get a Linux!* (Instead of buying Final Fantasy 136, use those 50 bucks to get a Linux. You *will* need it and must know it to become an elite!

4. Get on the Internet as much as you can, searching for scanner, IP address, etc. tutorials.

And, in case you didn't hear me before, *there are no shortcuts to becoming the hacker you always want to be in your fantasies!*

Drake Smith

The only thing we can agree with here is your last sentence. While nothing you suggest is a bad idea (other than helping to perpetuate the "elite hacker" Hollywood thing, albeit in jest), none of it is an essential ingredient towards being a decent hacker. Hacking encompasses so many different elements in our world that to relegate it to merely programming, operating systems, IRC, or, for that matter, even computers only serves to limit the possibilities. And those possibilities are pretty mind boggling.

Dear *2600*:

I'm curious to know if anyone else has noticed a rather staggering trend of apathy and disregard coming from the IRC technical community? Within the last 13 years, IRC has always warmly been a place to gather and disseminate information; at one point or another, it was even a good place for an interested individual to grow and learn from a wide variety of other individuals who were skilled and versed in practically every trade imaginable - not just computers. Within the last five years, however, I've noticed a common and steady trend of apathy centered around the IRC technical community, specifically in those areas that have the most to do with freedom of information and the hacker community in general: UNIX and Linux.

Join any #linux channel on any major IRC network, attempt to ask any community related question (such as opinions about the latest lawsuit by SCO, which has attempted to claim copyright infringement over its acquired proprietary UNIX source code that it claims has illegally found its way into a number of different UNIX and UNIX-like operating systems, and most significantly the Linux kernel itself), and you are greeted with nothing but apathy, contempt, and utter disregard. This same trend continues on into the UNIX and Linux coding community, and manifests itself prominently in any #perl channel on any major IRC network.

I can only attribute this squarely, from my personal experience and observations, as originating from a badly stirred mixture of old traditional hacker values, which often centered around earlier and harder to obtain, modify, and learn-from UNIX and early Linux operating systems, and newer traditions arising around the latest BSD's and easy to obtain commercially packaged Linux distributions (such as Redhat and SuSE) that seem to be creating more isolated, self-sufficient Linux users and less community involved, curious, exploratory hackers who are more than willing to both learn and share. This feeling of collective apathy that is now surrounding much of the technical community on virtually every major IRC server, but that has remarkably not contaminated the email/usenet/and BB groups is very disconcerting to the average Linux or UNIX newbie, who is either starting out, returning, or simply expanding his or her knowledge.

Without more friendly and avid technical communities such as *2600* I honestly do not understand how the UNIX hacker tradition is going to expand past the elite few and into the majority or even continue on with the same traditions of free information and open knowledge that have been passed down from hacker to hacker over the last 20 years. Perhaps no one wants it to expand into the majority - that would, after all, rob us of the very thing that makes our knowledge valuable: that it is rare.

Perhaps, despite such omens, it can all be chalked up to the reality that many of us just simply do not play well with others, or too many are just simply sick of the waves of questions they receive which can summarily be answered by a simple web search. This is definitely a shame, as there is so much information out there waiting to be shared, and so many people who want to share what they know but can't, as the community in which they live has too many preconceptions about what they might do with their newfound knowledge and the community in which they turn to for that knowledge is afraid that too much of it will be learned too easily, thus lessening the toils of their labor. What a shame indeed. And if this becomes a trend, we will be isolated, not from society but from each other.

Joseph

We've seen such concerns addressed before many times in various communities, both online and off. We think it's less a thought out strategy and more a case of people simply being overwhelmed with the same questions over and over. They come to forget that there's a virtually unending supply of new thinkers out there and at least some of them will play a major role in the future. The new people oftentimes take things way too seriously and give up very easily or, worse, engage in some pointless battle of insults which quickly overshadows whatever it was they were interested in in the first place. It's not unique to your community and it's not at all uncommon in the IRC world. You will always have people who are there just to get attention and cause trouble. You could fill a book with methods of dealing with this. And there will always be people bemoaning the fact that things aren't what they used to be. They're not, nor should they be. Change is good, essential, and should be embraced. On the other hand, the people who have experience and knowledge are a vital part of this community and they should never be dismissed as out of touch or old school. One thing IRC still has is the ability to surprise us with its effective and often unintentional community building.

Dear *2600*:

I am sending this mail from West Africa and I am very interested about the hacking. Maybe you know it but there is no hacker in West Africa and me too I am not one. I would like to learn how to become a hacker but I don't know who I will contact. I would also like to represent your magazine here in West Africa. Please let me know your decision about my case.

Thierry

Read the above responses for our take on learning to be a hacker. We believe there are lots of hackers and potential hackers in any part of the world. The trick is figuring out how to reach them. We agree it's a challenge to do this. If you believe there's a chance that there's an outlet for our magazine in your particular part of the world such as a bookstore that would be agreeable to stocking it, then send us specific information and we'll gladly follow through. We find that when people have a place where they can get ahold of the magazine, it's a lot easier to do things like set up meetings and build a community.

Have You Heard?

Dear *2600*:

Has anyone heard of the Super DMCA? It's ridiculous! Now your provider for cable, Internet, whatever has the right to prosecute you criminally if you have "unauthorized" devices attached to your computer or TV. For example, if you have a VCR, DVD recorder, or even a TiVo hooked to your TV, the cable company can turn you in for "attempting to circumvent copyrights." I'm outraged!

Jesse W.

The so-called "Super DMCA" is another flavor of the federal DMCA but on a state level. At press time, this or similar legislation had become law in Delaware, Illinois, Maryland, Michigan, Pennsylvania, and Virginia. It's very close to becoming law in Arkansas and Florida and it's being considered in a *number of other states. Only in Colorado has it been vetoed by the governor. Unlike the existing DMCA, these bills don't have any exceptions for previously defined legitimate activities and they could also be used to outlaw such things as firewalls and encryption. We suggest checking the status of this legislation in your state and looking for more updated information on the net, such as at http://www.eff.org or http://www.freedom-to-tinker.com.*

Dear *2600*:

I don't know if anyone is aware of this but on Mac OS 10.2.2 (and possibly others), holding down Command-S after the opening chime on booting the machine seems to drop the system into a root access full screen shell.

I stumbled upon this on a message board while searching for something unrelated. I tried this and did a little poking around, running cats of files in other people's personal directories. I couldn't seem to copy files to my own directory, due to some read-only status. Also, lp didn't work.

I have only moderate experience with UNIX systems so maybe someone with more can fiddle with this? Just a thought.

PhrenicGermal

Dear *2600*:

Here is something interesting I stumbled upon today. I'm an avid user of BitTorrent (mainly because of the random stuff one can find, such as the "Satisfaction" Bikini Babes with power tools video) and I troll the many BT sites daily. Today I found *Freedom Downtime* available for download, but noted it was only about 90 megs in size. Checking the IMDB I see that it is 121 minutes and started to wonder about the quality. Well, turns out it was a .ram file. All I want to know is why someone would go through the bother of ripping a movie only to keep it in a Real Player format. Granted, it can compress video to a small file size, but that is just it.

Just thought I'd give you guys a heads up that your video had been ripped and was being shared (which I think is cool and I believe you would agree), but also that it had been saved in one of the worst formats available. I mean, come on, do the film justice and give us an SVCD or 700 meg DivX rip!

MacAllah

This is really the only problem we have with the film being available online - people will think the film looks like shit because of how it looks there. This is something hardly isolated to us though - a majority of films on the net look and sound awful. While we specifically approve of the film being spread around (for free and unaltered), we do ask that if you can afford to buy a copy that you do since it's coming directly from us and not from some Hollywood distributor who will use the money you give them to send out letters threatening their customers with lawsuits. In our case what we sell translates directly into other projects that require huge investments, like the Freedom Downtime DVD and future HOPE conferences.

Taking Action

Dear *2600*:

I was sitting at home the other day, minding my own business, and the phone rang. I went to pick it up and it was the trademark telemarketer nuisance call. As some of you may remember from the past few issues, there have been some articles which describe how telemarketers work. Occasionally telemarketers' computers will call more people than they have available telemarketers. When this happens, they hang up as soon as somebody picks up. That's called a nuisance call. What was interesting this time was that caller ID actually reported a number, rather than "Anonymous" or "Unavailable." When I called it back, it said something like "Code 1563" and promptly hung up. I didn't write down the exact code, but it was something to that effect. I was curious so I called it back again and it just rang. Does anybody know exactly what this may be? I'm assuming it was a telemarketer. However, it was odd that it actually gave me a number on the caller ID. The phone number was 702.889.08XX. It was a harassing phone call, so I have no hesitation about posting the number.

Patrick

This is getting a bit silly. Your phone rings once and you're ready to declare war on whoever dared to dial your number? We agree that telemarketers are a royal pain in the ass and should be dealt with harshly when they annoy people. But this could have been an innocent wrong number, something that used to not be a big deal in the days before caller ID. If you get an actual sales pitch attached to a phone number, let us know and we'll print the entire number. And before anyone starts to scan out all the numbers to fill in the above X's, the number was disconnected when we called it. We can only speculate as to why.

Observations

Dear *2600*:

At school we went on a walking field trip to some play or something, and on the way we saw an ATM. And I told my friends that I had read an article in *2600* that said if you press the right buttons you can get to a hidden menu. So I went over to the "standalone" ATM and pressed all four corner buttons and the menu came up and it started beeping (like a PC does). It beeped eight times. All my friends were laughing and we still make jokes about it to this day. Thanks for the laughs, *2600!*

Satch379

We're always happy to provide amusement. And the fact that you probably have no idea at all what your field trip was supposed to be about is just icing on the cake.

Dear *2600*:

It was kind of an accident finding this. In the cover of your 19:4 issue (what building is that?), if you place the issue on the floor, take a few steps back so you're like three to five feet away from it, and look down at the issue, the sun's reflection on the building looks to me like a person's face. It kind of looks like Hitler's head because towards the bottom it looks like a third of a mustache. I don't know if that was intentional but it's weird looking. Thanks and keep up the good work. I love the little things you hide in the issues.

SeKToR

The building was the library in Paris which had been taken over (with permission) by members of the Chaos Computer Club who outfitted it with lights that could be programmed from around the world to display various images. The one you saw was most definitely a face (not Hitler's). To find out which (and to be scared speechless), watch "1984" (the version made in 1984). We can only hope to be able to do something like this to a building in the States someday.

Dear *2600*:

Recently I sat in on a seminar on network security in Arizona. A Phoenix FBI agent discussed some of his concerns and practices on network security. His first PowerPoint slide was on phreakers and *2600*. He made an explanation of *2600* representing the 2600 hertz that could be used to hack the phone system and a brief history of the man "Captain Crunch" who discovered this vulnerability. This was presented as a security problem that still exists. He held up the latest issue of *2600* and made a point that such "problem" literature could easily be picked up at the local Barnes and Noble. He covered Kevin Mitnick and his book *The Art of Deception* and commented on how he liked to read books written by the "enemy." He even went through a couple of examples in the book. He commented on the agency's lack of knowledge and said that there is at this time only one computer trained agent. He went through a scenario on how long it could take to actually trace back a security breach. His talk was given with a lack of actual real knowledge and seemed to be presented in fear of not having control. It is amazing how afraid and ignorant our nation is.

Spua7

Fear and ignorance has become the driving force behind much of our nation's activities lately. Individuals can learn quite a bit if they recognize this.

Dear *2600*:

Some of you may have heard of Echelon. For those that haven't it is supposed to be a global eavesdropping system that flags communications based on keywords. After placing "Echelon Keyword List" in Google and opening the first URL listed (http://www.angelfire.com/wa/militia/echelon1.html), I saw the words "2600 Magazine" in the list. Just wanted to pass this on. I thought it was funny. Love the magazine. Keep up the good work.

Dave C

We're honored to share the spotlight with other dangerous words like football, rhosts, and Sex. It takes about a millisecond to realize that this entire site is a joke.

Dear *2600*:

I noticed something peculiar when I installed a second phone line in my apartment for business. I use the phone line with a fax switch. Before I installed the fax switch, I had started to get telemarketing calls within one day of the phone line being activated. After installing the fax switch (Comswitch 5500), the telemarketing calls have stopped. This particular switch picks up the call on the first ring and "listens" for a second or so to determine where to route the call. Evidently, this fools the telemarketing equipment into thinking the line is data related. At first, I would get calls but only hear a dial tone when picking up the phone (when the switch directed the incoming call to the telephone). This became less and less frequent and now I seldom get more than one call every two or three weeks. Anyone else had similar experiences?

John Tate

We've heard similar tales. Of course now you have to watch out for junk faxes.

Dear *2600*:

I was reading through 20:2 and remembered a letter in the past about nothing ever being on the bottom of the 33rd page in the magazine. So ever since I read that letter I always would look on page 33 to see what little surprise you guys put there. This time I found something interesting - it looked like Morse code. Sure enough, I translated it using http://www.qsl.net/kb5yae/phonetic.htm and it came up to be "Page Thirty Three." Nice guys, keep the surprises coming!

CPUHaxxer

Dear *2600*:

Is it ironic that the price of a lifetime subscription of *2600* has the number "2600" in it?

aaron t

No flies on our readers, that's for sure.

Dear *2600*:

I just finished reading 20:2. I then sat down to watch a movie with family I was visiting. If anyone wants a State of the Union address, watch *Enemy of the State*. Most of it is easily plausible even for non-conspiracy theorists. A (not perfect) quote from the movie: "When buildings start blowing up, things change." This movie was made before September 11th, 2001 but it deals with the same issues we face now. Laws are being passed stripping us of our rights and privacy.

Another random thing I heard after making connections - the main antagonist, the NSA official played by Jon Voight, is said to be born on September 11th, somewhere around 1940 in the movie.

Eric

Keep The Faith

Dear *2600*:

I know I am addressing an old letter but it really struck me when I reread it today. In 19:3, David wrote about "why even bother" with all the anti-civil liberties going on. *2600* said not to stop. I agree. I just wanted to tell David and everyone else out there that I know of at least three groups of small, like-minded individuals who will not give up. I am a member of one of them and have friends in the others. They are all in different towns, one of them in a different state. They know of others. We may be small in number, but we are fighting for something we feel we are losing: the ability to be who we want to be and to respect others' rights to do so also. That's what it's all about. Good luck, David.

tWiST

Dear *2600*:

Hi, I am currently stationed in Kuwait in support of Operation Iraqi Freedom. I was introduced to your magazine a few months before I left. I love all you have done to keep the world on guard for people trying to take our freedoms. I greatly miss reading your magazine and can't wait to be able to read it once more. Thank you again.

c0l0r3dfr34k

Is it forbidden or risky to receive our magazine while in the military? We honestly don't know so we'd appreciate any insight.

Dear *2600*:

I've been a longtime fan of *2600*. I'm a hacker/network engineer. I started playing with my dad's computer after my parents went to bed, sometime back in the early '80s. I wasn't allowed to use it. Being only age 14, I would probably break it. Well, I secretly maintained it and then discovered how the modem worked. I started calling BBS's all around the country. It wasn't until the first big phone bill came that I was discovered. Ahhhhh... nostalgia!

Anyways, I always look forward to the first article in your magazine. It's such good stuff. Makes me proud to be American. I'm with ya.

I think it's a shame that, for the most part, the only people who read that first article, are... us. I want to reprint it on the forums that I visit. Who do I give credit to? Just plain old *2600?*

Bob

If you could give out the name of our magazine along with our address and/or website that would be great.

The Past

Dear *2600*:

In 20:1 ByteEnable mentioned emoticons in teletypes in the 60's before the Internet (sic). Since the TinyTot machines used CR (carriage return) and LF (line feed) separately, one just said "C.U." then CR LF "OO" CR ".." and that put two eyeballs looking at you. Can a PC do that?

walt

Dear *2600*:

Just a quick letter to compliment you on your magazine. I am embarrassed to say that I know very little about computers. My curiosity level far exceeds my skill level, and almost all my efforts to explore/enhance my machine have turned into horrible disasters requiring emergency help from my brother. But, thanks to my brother and his interest in computing or whatever you want to call it, I have read every issue of *2600* for the past five or so years and they have taught me so much. As a law student, I find many of your articles to be extremely relevant both to my studies and to my interests. You raise issues that I haven't heard anyone else speak of, ever. It's a shame most people in my position will never have the opportunity or desire to read *2600* or similar publications - it's not so easy to find different viewpoints on the news and politics if one does not actively go looking for them. And it has been my experience that most people just don't care enough to seek out and compare different versions of the truth. Thanks for keeping me aware, and keep up the good work! Hopefully someday I'll have something to contribute in return.

kdg

Dear *2600*:

Just to add another note, Screamer Chaotix ("Unlearn") makes the point "why even bother" defining the terms etc. Primarily because it's the ignorance of these terms that promotes wrong usage. I do clearly remember the day where if you didn't answer a list of 25 questions correctly, you were denied access. We should go back to that.

Fruber

The letter you refer to said "why even bother" in relation to the specific term "cracker" which was demonstrated to be meaningless. As for your 25 question thing, that may have been true in one particular clique but it certainly didn't define the entire hacker world. There's a fundamental problem with emphasizing certain specific bits of knowledge as important or vital if one is interested in being a hacker and then having the ability to deny access to those who don't share these specific values. This kind of hierarchy goes against the open structure of the community and only reinforces the mainstream values that embrace memorizing facts as an indication of intelligence.

Destructiveness

Dear *2600*:

I was browsing on kazaa and I found a copy of the latest issue of *2600*. I had bought it but I figured since I don't have a scanner it would be nice to download a copy to have on my computer. Well, a text file included said the following:

"I hope you enjoy it as much as I enjoyed making it. FUCK YOU goes to 2600, for though the reading is quite interesting, I find it ironic you're capitalizing on something which YOU YOURSELF claim wants to be free (Information).

If you charged a max of $2.50 for this magazine then I'd let you live, but you're ripping ME off, hence be prepared to be ripped off from now to eternity by me or my."

I am appalled at this. Doesn't he get the concept of supporting a cause? Yes, you are charging for the information but is $5 unreasonable? You guys don't even object to people giving out the information in the magazine for free. In fact you encourage it. I really don't understand these people who bitch about paying $5 to support a cause that deserves it. When will the insanity end?

Lord Kahless

We've been dealing with idiots like this since Day One. As you seem to realize, we've always supported the free exchange of information. What we charge for is the printed publication which costs us quite a bundle to print, ship, get into stores, plus the many things that go into keeping it all running. We like to think that our existence enables more people to discover and become a part of the real world of hackers. And unlike virtually every other magazine out there, we are entirely reader supported. We can't raise our advertising rates when expenses go up since we don't have any advertising. (If we did it's likely we wouldn't be able to print much of our material in the first place.) Also unlike most other publications, much of our material comes from readers turned writers. And as a completely reader supported venture, we have no middleman collecting cash and making the price unreasonably high to satisfy a profit motive. So the righteous indignation just isn't going to cut it. There are numerous examples of entities profiting off the hacker world by charging outrageous amounts for conferences that supposedly tell our secrets, distributing recycled information to people who don't know any better and charging them premium rates, and a wide assortment of other smoke and mirror ploys designed to get cash from the gullible by capitalizing on the attention given to hackers. We've deliberately chosen over the years not to go down that path, despite the huge amounts of money that could have been made. We've chosen instead to do what we do for as long as we can do it. If our readers were to emulate the activity you found, we certainly wouldn't be able to continue this for very long. But as this person so eloquently stated, he clearly doesn't support us in any way. We can only hope that there are many more out there who do.

The Quest For Knowledge

Dear *2600*:

Locally here in South Bend, Indiana, I've noticed a "flaw" in the payphone system. I'm not sure if this affects other non-payphone lines; I haven't had the balls to test it on my home phone. The problem occurs when you dial what used to be the Proctor Test Set (at least, for this area). I saw a new payphone with an ugly yellow receiver and "SBC" etched in the top. I picked it up and dialed the Proctor Test Set (200-222-2222). But the instant I had finished dialing in the "200," it clicked. I waited to see what would happen, then it clicked again and played a recording: "This number is not allowed to be dialed from this phone!" Then it hung up on me. I tried this on two other payphones in the area. On the first I kept dialing during the clicks. I may have pressed "2" ten times, I lost count. But what happened next weirded me out. The line had ambient mechanical noise (that's the best I can describe it), and it was ringing as though I had called someone, but all sound on the noise was distorted. Almost like it was underwater. Even the DTMF was messed. So I stayed on ten minutes to see who picked up. Nothing happened, it just looped over and over. So I hung up and came back five minutes later to find it still doing that! It's probably still doing it to this day! The second payphone I tried, I let it get the best of me and stopped after the "200." It clicked twice, then the line went silent. The number pad was disabled (or at least not making sounds), no echo from the receiver, nothing at all. It remained like that quite a while later after hanging it up, just like the other phone. If anyone knows what this is, please tell me!

slax0r

Consider the word out. It's amazing what you can still find on the telephone network just by dialing strange numbers. That's one form of hacking that can never die.

Dear *2600*:

How can you find out someone's name and address from their car's license plate number? Are there any sites on the Internet that allow you to do this?

Brainwaste

In many states this information can be obtained directly through the motor vehicle department for a small fee. Some enterprising people have even taken to distributing this information in other ways. In those places where it's not that easy to get (and even in those where it is), there is no shortage of sites offering to obtain it for a not-so-small fee. And, of course, cops can pull this information any time they want.

Dear *2600*:

At my age, 56, this magazine is *Mad* magnified, sort of. Cool kids, go for irritating authority. As a discouraged optimist, it is nice to see that hope for a better world lives on.

Thanks for the uplift. I look for your little mag every time I go to B&N since I discovered it six months ago. No, I'm never going to be even a script kiddy but my kitties and I read your little bit of chaos/anarchy knowing that we can cross the bar when the time comes and the world is in good hands.

Helen

Piracy Prevention

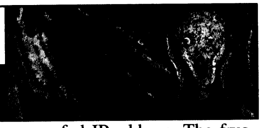
Dear *2600*:

Recently, I bought the Sony MZ-N505 Minidisc recorder. I wanted to use it to make high quality recordings of my band and my friends' bands in live situations. I had no intention of clandestinely "bootlegging" the copyrighted material of paranoid mega-acts like Metallica or Linkin Park, due to my lack of interest in their lousy, overproduced, overprotected, irrelevant garbage.

A few weeks ago, I decided to try to get a good live recording of a friend's band at a club. The result

continued on page 48

Denial of Service Attacks, Tools of the Tools



by bland_inquisitor
Bland_inquisitor@hotmail.com

Disclaimer: All of the information contained in this article is for *informational purposes only!* I do not approve of DoS attacks used for the sake of mindless violence; I think that in this form they are the direct opposite of hacking. If you manage to use this information illegally, it's your problem not mine.

We've all heard their names: Teardrop, Fraggle, Smurf, Bonk, and many more. DoS attacks are small, nasty, readily available, and take zero technical proficiency to use. This is a bad combination for everyone. EBay, ZDNet, CNN, and countless other systems have fallen victim to this type of criminal activity. DoS attacks cost corporations millions of dollars every year in lost productivity. In this article I hope to show the basic theories behind how DoS attacks are possible, explain some of the generic DoS scripts out there, and show how DoS attacks have evolved into more precise and lethal tools of destruction.

Types of DoS Attacks

Bandwidth Consumption: The least personal, and most easily detected, type of DoS attack is based on bandwidth consumption. How it happens is that the attacker will eat up all the available bandwidth on the victim's system. There are two possible ways this can take place.

1. If the attacker has more available bandwidth than the target, he can simply flood it by being able to receive more information than he needs to send. (Ever heard the term "ping flood?")

2. Some DoS attacks, as we will see later, can be amplified by using the combined resources of another network. By doing this, an attacker can flood even the largest networks with relative ease.

If a criminal is going to DoS someone, they will most likely execute it from a system they have already "Owned." However, it is not uncommon for an attacker to deny service from their personal Internet connection using a spoofed IP address. The frustrating part of this type of attack is the fact that it is based on a fundamental flaw in TCP/IP architecture: the substandard way in which systems handle SYN requests.

Resource Theft: What if an attacker feels the need to DoS someone but doesn't have either an 0wned system to send from or a network connection capable of overpowering the target? Never fear, someone's already thought of that. A resource theft attack over-utilizes access that the criminal already has. This causes the remote computer to hang or crash by using all the available memory or overtaxing the CPU. For example, an attacker could spawn multiple executions of freecell on a computer, thereby using all of the available system memory. This would result in a computer not allowing any more processes to be run and denying service to legitimate users.

Flawed Programming: There are other types of attacks that make full use of programming oversights. The Pentium f00f attack allows someone to crash any x86 environment by executing the bogus instruction 0xf00fc7c8 because of a flaw in Pentium microprocessor programming. We know that it is possible to execute commands in a buffer-overrun situation, and this type of attack is based on that principle. For those who may not be familiar with the term "buffer overflow," it is a condition that allows for code to be run (usually as root) by putting a greater number of characters than allowed for into a variable. The most common occurrence of this is when a program inserts data into a buffer without checking its size.

DNS Cache Poisoning: It is also possible to alter a router so that it redirects all incoming traffic to an unintended location, either through the attacker's system or into a nonexistent one. DNS attacks or "cache poisoning" occurs when a DNS server is tricked into resolving an unintended location. An example of cache poisoning would be if someone redirected all the traffic intended to go to www.stankdawg.com to www.disney.com therefore denying service to www.stankdawg.com. Also, it is possible to redirect traffic to a nonexistent network or "black hole." An example of this would be sending all incoming traffic meant for www.oldskoolphreak.com to an arbitrary address, essentially erasing www.oldskoolphreak.com from the Internet. This could go undiscovered for days, until the host notices their hits went from 5000 to zero!

A Look At Canned DoS Attacks

Smurf: Smurf is a self-amplifying attack that uses directed broadcasts to crash a network. There are three players in this scenario: the criminal, the amplifying network, and the victim system. What happens is that an ICMP ECHO packet is spoofed to appear as though it were sent from the victim's system to the amplifying system's broadcast address. Here's where the shiznit hits the fan. Every box on the amplifying system that is configured to respond to a broadcast ping request will respond to the victim system, thereby flooding it with responses and shutting it down. To keep your system out of the amplification business, simply disable directed broadcasting at your border router. To keep from getting "Smurfed," limit incoming ICMP and UDP at your router to only those systems that need it. If you find your system on the business end of a DoS attack, get with the amplification system and use a tool like MCI's "dostracker" to trace the attack to its source.

Fraggle: Fraggle, a variant of Smurf, is a DoS mechanism that uses bogus UDP packets to port 7 (the echo port), as opposed to Smurf's ICMP. The advantage over Smurf, if you want to call it that, is that if a box on the amplification system is not configured to respond to UDP, it will send back an error message that will consume bandwidth.

DDoS Attacks

In February of 2000, the long theorized DDoS attacks came. EBay fell, then CNN.com, then five other major systems and a myriad of minor ones came grinding to a halt. DDoS attacks require more forethought than DoS attacks, but that doesn't make them any harder to accomplish, or any less common. The difficulty is in 0wning the systems themselves!

There are two parts to most DDoS scripts, the client (used by the criminal), and the servers (placed on unwitting or already 0wned systems). An attacker will place the server software on as many computers as possible, making them his "zombies." Then when the attacker feels the time is right, the zombies will execute the attack command using their resources and IP addresses to shut the victim system down.

The first DDoS attack mechanism was written for *nix systems by "Mixter." The "Tribe Flood Network" offered all the standard DoS attacks, and sported a TCP-bound root shell.

After TFN was shown to be effective, the look-alikes hit the scene, all attempting to offer better features while simplifying the process even farther. Trinoo and Stacheldraht are two major players in the post-TFN market. Of the two, Stacheldraht is the most stable and lethal of the DDoS programs. Offering ICMP, UDP, SYN, and smurf-style attacks, encrypted telnet sessions between client and server, and the ability to blind network-based intrusion detection software, Stacheldraht is the leanest, meanest way to hose a network almost anonymously.

Local Attacks

There are a number of local attacks, but they are not very popular. Also, they are all but outdated. These examples are more aptly defined as "exploits," but I mention them here because they can lead to a DoS situation, even though they are distant cousins. On NT 4.0, there is a way to fill %systemdrive% by exploiting disk quota functionality. In Linux kernel 2.2.0, a local attacker could use the munmap () function call used by ldd to overwrite key areas of the kernel memory, causing a kernel panic.

In closing, remember that the key word in "denial of service" is *denial!* It's not always a matter of using brute force to shut someone down. Almost always, the most effective attacks are also the stealthiest. If you want to learn more about DoS attacks, try them out on *your own* system. Learn safely, and have phun!

Shouts: StankDawg, who for all the editing is hereby officially promoted to co-author, dual_parallel, and everybody at www.stankdawg.com and www.oldskoolphreak.com.

frequency theory for the phone hacker/musician

by The Piano Guy

Like many computer folks, I'm also a musician. I'm much more competent at that, but I have this habit of liking to pay my bills, which is why I also work in computers. Unlike most people, I happen to have absolute pitch memory (which is more commonly but incorrectly referred to as perfect pitch). As a result, I have a polite correction and amplification to autocode's interesting article in 20:1.

For all intents and purposes, the dial tone frequencies in my neighborhood are a 440 A and the F below it. Autocode makes a big deal that an F is 349.23 Hz and that the actual lower tone is 350 Hz. This doesn't make enough of a difference to matter. The note is an F. Partial tones in musical notes are expressed in cents. There are 100 cents between half tones. The distance between an E and an F at that frequency range is 19.6 Hz. To be off 0.8 Hz at that point (the difference between 350 Hz and 349.2 Hz) is about four cents. This isn't enough to make a difference to anyone whatsoever. The vast majority of people on the planet can't even recognize the difference (including many with absolute pitch memory). Most piano tuners won't even fix that if the strings match each other.

All this is moot when it comes to tuning your guitar to the phone because the top note (which is right on) is exactly one octave above the A string on a guitar, which makes it ideal for tuning (for those that lack absolute pitch memory). For those with relative pitch (much more common ñ being able to hear intervals), the F below the A is a perfect fourth below the note to tune a trumpet.

Of more relevance to the target audience (this is *2600,* after all), is that there is a reason for this very minor frequency shift. Frequencies tend to beat at twice and half their original frequencies. That 440 A tone has harmonic tones at 220 and 880 Hz. Harmonics colliding could confuse phone switch circuitry. The phone company in their wisdom (not sarcastic, for a change) picked frequencies that were not harmonics of each other. This is why hackers have to have precise tone generators. Close isn't usually close enough. The difference between the E-flat and the E (in the neighborhood of 2600 Hz) is enough that someone playing the organ in the background wasn't likely to get anyone a free phone call back when a Captain Crunch whistle did the trick. I'm sure this was a conscious choice too.

I'm not aware of a software frequency counter, but I have to think that one exists. If someone has a good keyboard with tuning capability (to work with detuned instruments), then it is probable that the keyboard can be made to generate whatever single frequency is required for whatever purpose.

A Trip down Memory Lane

by Jimmy Yu

This past April marked the tenth anniversary of the Mosaic web browser. Mosaic was easily the first GUI based, mouse clicking web browser. For an historical timeline check the links listed at the end of this article. The final release of Mosaic 1.0 was November; Netscape was next in 1994 and then Internet Explorer in 1995.

This little celebratory event got me to think of some of the modern Internet conveniences that we have and their ancestors, many of which are still in use today. The first example would be Lynx - a text only browser. You can "navigate" or "surf" the web on Lynx by using enter, backspace, and of course, those arrow keys. There was no flash, shockwave, animated gif, etc.

In the early days of the net there was no instant messenger as we know it now. On the old mainframe computers you had to login and see if the person that you wanted to contact was also logged in. This was done by the "w" or "who" command showing the users on the host. If the person in question was on another system, you would then have to "finger" them (finger username@host-site). You would then have two options. Echo them a message or "talk" (talk username@host-site) to them. Both methods would cause text to be displayed on their monitor console, usually a Wyse. In the case of "talk," the other person would respond back with another "talk" and thereby establish a connection. You would have a split screen and be able to see each other's text messages. When the "talking" was over, one of you would use control-c to end the session. (Usually loud cussing is heard when someone is in vi doing programming homework and foreign text appears on their screen.)

E-mails were just text. After logging in, the system would notify you that new mail had arrived. You would type "mail" and a listing of the mails would come up on your screen. Type in the number and the content of the mail is displayed, "r" replied to the sender, "d" deleted the mail, "q" exited the mail program. To include a file into the e-mail, you had to do "~r filename" or if you wanted to edit the file, "~e filename". You would have a period at the beginning of the line or control-d to end text input of your mail. A Cc: prompt would then come up and ask for carbon copy recipients. A far cry from the drag and drop file include, text formatting, hypertext colored background of today's modern e-mail.

For get-togethers we didn't really have chat rooms, but we had MUD (Multi User Dungeon). Users would telnet in, choose their own name, and be interactive among all people that logged in. One of the earliest ones and probably among the oldest on the web today is End Of The Line. I used to play and interact with players on this site for pretty much all of my college days. People from around the world can access this site and see an early version of computerized Dungeons & Dragons. Players accumulate experience points by slaying monsters and rise in rank, eventually reaching the goal of a wizard. A wizard then has the ability to code more monsters and expand the realm of the MUD by adding their own areas. Another MUD where I used to play and hang around is Acropolis. I do not believe they still exist.

This article brings back and possibly shows the younger generation of net users what has happened in the past ten years since the first GUI browser was introduced to the population. And for me, writing this article has also brought back memories of the bygone years.

Credits and References

http://access.ncsa.uiuc.edu/Releases/04.24.03_NCSA_Celeb.html

http://www.blooberry.com/indexdot/history/browsers6.htm

http://www.cc.ukans.edu/~grobe/earlylynx.html

http://www.eotl.org/

Finding Ogg -

Audio Evangelism

by The Dark Shirt

MP3 - everyone worth his or her salt (and those not even worth a pinch) have heard of it. It's caused a storm in the music industry, most notably through the RIAA attacking Napster and other P2P file-sharing operations, making music files small enough to download, even over a 28.8k modem connection. And if that wasn't reason enough for an enthusiastic world of music lovers to embrace it, it's free as well. Isn't it? Well, not exactly....

MP3 development began in 1987 in Germany. Fraunhofer Gesellschaft, a German research organization, led the way. The following year, the Motion Pictures Expert Group began researching and creating standards for audio and video compression, eventually incorporating the Germans' work into the MPEG-1 standard as Audio Layer 3 - hence MP3. Here's the important bit - Fraunhofer Gesellschaft were granted the patent for MP3.

Those of you with quick minds will realize that this means Fraunhofer are therefore able to charge for the use of MP3. And guess what? They do! A company known as Thompson Multimedia are in charge of collecting royalties for Fraunhofer. Thompson Multimedia collect $0.75 for every MP3 player/decoder and $5 for every encoder sold. That's hardware *and* software, folks. If the software is free, then the makers are currently exempt from paying royalties, though this isn't actually stated in the license anymore.

The main reason for the proliferation of free MP3 players available is that until last year, Thompson Multimedia's terms of licensing MP3 technology stated that "no license fee is expected for desktop software MP3 decoders/players that are distributed free of charge via the Internet for personal use of end-users." The ominous removal of this part of the terms has led to some of the more paranoid among us feeling that there may be a possibility of having to pay to listen to MP3s. But surely Thompson and Fraunhofer wouldn't take the opportunity to make a bit of extra cash? I mean, they have the market pretty well cornered, everyone knows and uses MP3s, and... ah... oops.

So far Thompson have denied that the collecting of license fees for free players is being considered. But then, why change the licensing terms?

If this alone is not enough to consider looking for an alternative, consider the following:

MP3 encoding is closed-source. If you want to give it an overhaul, or improve its encoding from Average Bit Rate to Variable Bit Rate, you can't.

MP3 encoding is ten years old. How much software/hardware do you use that's as old as that, that hasn't been changed/upgraded/improved in some way? And leave off with the emacs and all that stuff, you know what I mean....

So what's out there in the way of alternatives? Thompson would probably suggest MP3PRO, which apparently uses advanced compression algorithms and VBR to produce a file with half the file size of a comparative quality MP3. However, MP3PRO is still closed-source and subject to the same patent and licensing issues (Decoder $1.25 per unit, Encoder $5 per unit).

In the licensed/patented corner are also Fraunhofer's AAC (Advanced Audio en-Coding) which has been adopted by Quick-Time, and WMA (Windows Media Audio) which has the backing of You Know Who. Both Microsoft and Fraunhofer seem more than happy to kowtow to the music industry's demands for tighter control of rights management, and are therefore incorporating DRM (Digital Rights Management) into their software. DRM allows the use of license keys to "lock" music and wonderful things that allow the end-user to play the music for a limited number of times, or days. This MP3 will self-destruct in 5... 4... 3... 2... you get the idea. Maybe I'll just read my eBook... oh.

DRM seems to be expected to work along the same lines as the MCPS (Mechanical Copyright Protection Society) in the UK and the RIAA in the US. This is not quite the case, though. DRM actually exists to prevent or restrict the copying or playback of music.

DRM has been known to produce negative effects, from reduced sound quality, to no playback on older computers, and even in some cases, the locking of the CD inside the drive, rendering it useless and requiring a service.

One of the earliest attempts to implement DRM was by the SDMI (Secure Digital Music Initiative), who in September 2000 offered a cash prize to anyone who was able to break one of four SDMI "watermarks." A team from Princeton University and Rice University succeeded in removing watermarks from all four. They declined the prize, which would have meant keeping their techniques secret and instead wrote a paper, which was to be shown at a conference in April 2001. The SDMI tried to prevent the release of this information, and, predictably, the RIAA tried to prosecute under the much-loved DMCA. The paper was eventually produced at a conference in August 2001 and the RIAA gave up in 2002. The paper can be found at: www.usenix.org/events/sec01/craver.pdf. The SDMI's last posting on its site was in May 2001, labelled "Current Status." Don't expect an update too soon.

We're not entirely up the proverbial creek yet, though, thanks to the folks at www.xiph.org, who have created the quite strangely named Ogg Vorbis audio compression format. Ogg has comparatively smaller file sizes than similar MP3s, and a better compression algorithm too. But here's the kick. It's open source. It has no patent or licensing issues. You can help it evolve. Everyone can help it evolve. It won't stagnate. Cool, huh?

There are two problems holding back the rise of Ogg, though. The first is that as a relatively new technology, there isn't a great deal of support for it at the moment. There aren't really any Ogg players in hardware format at the moment, though Xiph say they have plans for some very shortly. There are a number of players/rippers/encoders in software form though; Linux users should know about Audacity, which is also available for Windows machines, and players such as Winamp, Sonique, and Zinf to name but three, all support Ogg. CD rippers with Ogg support include CDex, Easy CD-DA extractor, and CD'n'Go.

The second issue is that Ogg is a bloody silly name. That's been the hardest part in convincing people to try it:

"I've found a free, open-source audio compression format that gives better quality and smaller file sizes than MP3."

"Sounds good. What's it called?"

"Erm...Ogg. Ogg Vorbis, to be exact."

(muffled laughter)

Yikes. But hey, look at it this way. When Thompson finally make the move to charge for all MP3 players, and we're all grooving on our free, better looking, better sounding, and goddamn sexy Ogg players, who'll be sniggering into their sleeves then?

Find out more about Ogg Vorbis at: www.vorbis.com and www.xiph.org

Infidelity in the [redacted]

by atoma

On a recent Chicago evening, while my live-in girlfriend of three and a half years was at work, I performed some routine maintenance on my home/office DSL/LAN computer network (three PC's {2W98SE 1 XP Pro}, one laptop {XP Pro}, one Xbox, one shared printer, and other PC's and Macs as business dictates). I am a computer repair technician and during the previous week I serviced three computers for virus-related troubles. They were each plugged into my home network after I disinfected them. All of them were error-free after I finished working on them, but I am very protective of my network. I spent many hours building it, and many more making sure no one corrupts it.

After completing repairs on the three PC's, I was checking the created and modified dates on files on each of my workstations. I gave my girlfriend an old computer of mine a year and a half ago (a P2 400 W98SE); I set it up for her, kept it running lean and clean, and never once found any anomalies in my routine network maintenance. However, on this night, her computer displayed a modified file date of 2037 on her "sent items.dbx" file. Since emails are a notorious, tried and true path for virus infection, I immediately grew curious. Her email client (Outlook Express 6) was password protected, and I wanted to see if any suspect email attachments existed in that dbx file.

I copied the suspect dbx file:
(\WINDOWS\ApplicationData\Identities\
{AC228580-7D44-11D6-8CF5-D78FC
E200233}\Microsoft\OutlookExpress\
Sent Items.dbx) to my PC.

(For those of you who don't know, this is where OE stores your emails, in files *.dbx, one dbx file for each folder you create in your respective identit(y) or (ies).)

I opened it with a disassembly program (W32Dasm V8.93) and I didn't find any suspect attachments. However, amidst the gibberish of random characters, I saw an email that my girl sent earlier that day to a name I immediately recognized as trouble. It was an ex-boyfriend. The message was very concise, six words to be exact. She asked him, "Are we still on for tomorrow?"

This freaked me out, because the tomorrow she spoke of was just hours away. I was supposed to go out on a service call for the day and she was planning to spend it with an ex-boyfriend. I extracted all of the emails from that file with (DBXtract V 3.50) and was absolutely floored. Before my eyes, in forensic black and white, was the outline of 18 months of betrayal. Times, dates, graphic reflections on the sex acts she committed, outpourings of emotion to men I was assured were "just friends." All of it was in front of me, taunting me, sickening me, destroying me. In the midst of making sure her computer was running at its best, so concerned with the performance of the computer I gave her, working into the wee morning hours so that she can painlessly experience the joys of computing, I got violated to such a degree I still struggle to describe it.

I copied all of the dbx files from her identity folder to my PC (oh yes, that OE password protection was so helpful to her huh?). I set up a new "dummy" identity in OE6 on my PC and imported all of her emails into it. I took all of the emails and put them into one folder. I sorted the whole stinking mess chronologically and gave myself a timeline to look at. I went down the list and read all of the emails (about 400) and took notes on the dates and times that stuck out in my mind, some dates where I was out of town, other dates where she convinced me she was working late or going out with her "girlfriends." Can you say "Deleted Items, wow they're still there! Thank you Microsoft!"

I started searching the cookies on her PC within the parameters of the dates and times I was able to map out from reading the emails, and I found even more evidence of her infidelities. The cookies from Mapquest and Google were especially revealing. By simply opening these cookies in Notepad, I had before me addresses that she got directions to, searches for restaurants and nightclubs, movie showtimes, even lingerie browsing at Fredericks.com! All of it beautifully time-stamped, frozen tracks of her lies and deceit.

I tell you it was enough to make me crazy with rage. But I wasn't through yet. At this point, with everything I was thus far able to uncover, I felt it was all up for grabs. Privacy? Fuck her, she had total freedom and look what she did with it. I found enough in the digital world. Now it was time to go "analog."

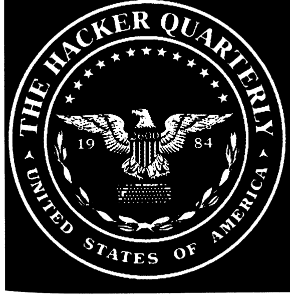
I went into her cell phone records. She meticulously filed each monthly bill away in a folder. I, in a manner quite similar to her precise filing, painstakingly entered all of these phone calls into a spreadsheet in Excel (almost two years' worth). When I finished, I sorted these by phone number. Boom, an easy to read detail of who she called and when. I took these telephone numbers and typed them into Google. Voila! The address of record on these "unknown" phone numbers corresponded to the address searches from the Mapquest cookies.

How about her bank statements? In the same file cabinet, not far from her cell phone folder, was the BankOne file folder. I cross-referenced the suspected rendezvous dates against this folder of info and again, voila! Black and white records of ATM transactions at ATM's very close in proximity to the addresses I found in the cookies from Mapquest and Google. These also fit right into the cell phone records' timeline, some phone calls were made to these other men within minutes of using the ATM! Talk about being busted!

A bomb burst in my chest that night. I medicated myself with 13 beers and a pile of cocaine while I reread the comprehensive, chronological, revolting realities of the double life my woman led. It was sickening, like it was two different people. Confronting her with this evidence has been the most difficult task of my adult life. At times I wish I never knew anything about what she did behind my back.

I've always been an advocate of total privacy for the individual, privacy free from the prying eyes of those with higher powers. Being able to find out so much detail about my girlfriend from her PC gave me a wake-up call. The things she did were indeed terrible; they managed to hurt me immensely. But look at how easily I was able to construct a virtual "play-by-play" of 18 months of her life. This is what shocks me even more than the awful things she did.

As "hackers," we all need to be aware of the digital "footprints" we leave behind while we traverse the world we call "cyberspace." It is a place full of so much information, a world full of the knowledge we love to collect pieces of. It is also a place of danger, for the trails we leave behind us can be collected and analyzed. These trails can be used against us, by powers much larger than any one of us. As the years march forward, we will have to evade, in order to survive.



continued from page 39

sounded excellent and when I got home, of course I wanted to put it on my hard drive to edit, EQ, and burn copies of it (with the full knowledge of the band - they even requested a copy). It was to my surprise when, after installing Sony's bundled Open MG Jukebox and NetMD software, that there was no feature to transfer (or "check-in" as they call it) data from the MD to the computer using the supplied USB/MD cable.

I learned that the USB interface was only to be used to "check-out" purchased music from the hard drive to the MD unit. The only permitted function of "checking-in" is to return previously "checked-out" music from the MD back to the hard drive, a function that I cannot imagine ever having a use for. Apparently, Sony did not include a truly digital USB/MD option in order to discourage piracy (Sony is, after all, a major publisher of music content as well as audio hardware).

So what are underground music enthusiasts and "tapers" like myself supposed to do to transfer uncopyrighted music to their computers? Here's the only answer I have come up with: We must play the MD, in real time, into the analog line-in in the computer's sound card, and then edit it using a sound-editing program (I use ProTools Free).

This outrageous example of prohibitive software is infuriating to people like me, whose main purpose in getting an MD recorder was for the perceived ability to record high-quality music and transfer it digitally to the computer. I've searched the net for shareware or freeware programs that enable high-speed USB/MD interface, but have come up empty. Mostly I just find entries on bulletin-boards full of complaints just like mine. At least one petition has been started, but I doubt Sony will alter or update their software.

If anyone has any alternatives or answers, I would love to hear about them. I just hope I don't hear, "You shouldn't have gotten a Sony." It's a shame that such amazing technology should be so incredibly limited because of baseless corporate fear.

Thank you for your great magazine.

semicerebral

This is a brilliant example of corporate stupidity shooting itself in the foot. Instead of encouraging people to use technology to be innovative, thereby creating all sorts of new markets they could capitalize on, they choose instead to stifle such innovation due to fears of losing money. We wish these dinosaurs would simply go back to the analog world and leave the digital technology for those who truly want to work with it. We're confident more companies will come along who don't cripple the technology, especially when more people like yourself make their presence known.

Dear ***2600:***

As recently as a year ago I had about the same opinion on piracy as revanant in his letter in 20:2; piracy is fine if it is just to "test out" a product. However, I've reached a stage now in my life that I am designing software and I finally understand why that idea is wrong. When you pour your heart and soul into something like a big project the finished product is a part of you. It is something you created and therefore own. If I want my work to be freely available, it is; if I want my product to cost $1,000,000 per license, it will because it is mine and I get to decide if/how anyone else gets to use it. It is wrong for someone to take what is mine under their own terms. I think that our freedom to create and to decide how our ideas are shared are fundamental, and software piracy deprives us of this right.

eigenvalue

Of course it's wrong for someone to take your hard work and leave you with nothing - or at least substantially less than you deserve. But you have to balance this with a dose of reality. If we were to decide that each of our issues should cost $1,000,000, does that mean that anyone who obtains it for less or, heaven forbid, steals it outright, is guilty of stealing a million dollars? Maybe in our opinion but nobody else would go along with it. And by pricing something so high above the reach of individuals, we'd be setting it up so that people would have to find some nefarious way of obtaining it. In other words, we'd be fools to be surprised and we'd have nobody to blame but ourselves when people don't play by these rules. Of course, there's no way we could ever get a magazine into a store with that kind of price. Software companies manage to come up with incredible markups as do record companies and that's a significant reason why so many people are not only reluctant to pay their prices but also completely unable to. It doesn't make it right but nobody should be surprised when it goes this predictable route.

Recently a filmmaker friend of ours wanted to buy the new version of FinalCut Pro to edit his movie. He went to the Apple store prepared to shell out the $1000 it cost. But he wanted a guarantee that it would work on the MacIntosh he owned before he paid for something that couldn't be returned. They told him that if it worked on a Titanium (the most advanced and expensive machine they sold), that they wouldn't be liable for any problems he encountered on a cheaper machine. In their words, it was his decision not to upgrade and buy a new machine. The decision he wound up making instead was to buy the program off the street for $50 and never use Macs again after this project. (And yes, the program wound up working on his machine which meant that Apple would have made the sale if they had shown some support of their customers.) Now there's no question that he ripped them off since he didn't pay them for the program and in fact wound up paying someone else for it. But who set this situation up? Has Apple earned anyone's sympathy with this kind of behavior?

There are ways of keeping customers and ways of losing them. And that, despite everything else that's going on, is the real bottom line.

Insecurity

Dear ***2600:***

A friend of mine found a simple way to get around the $9.99 price of the popular AOL/AIM instant messaging bot SmarterChild (www.smarterchild.com or IM "smarterchild") if you have a PayPal account. Once your trial period runs out, click on the link SmarterChild provides you with, then copy the link on the PayPal button. Merely change the "9.99" to "0.01" within the link and send the one cent payment. You just got SmarterChild's services for virtually free!

tr

There are so many references to stupidity in this letter that it probably sets some kind of record - AOL, instant messaging, PayPal, ripping people off, obvious security holes....

Dear ***2600:***

I recently took a vacation on the Tahitian Princess Cruise. Onboard the ship they have an Internet Room where you can pay $0.50 a minute to use the Internet. Of course there was no way I would pay to use their Internet so I sought out methods of bypassing their Internet program. They made a terrible mistake when designing the Internet Room. The power strips are exposed slightly underneath the desks for each computer, so all you have to do is turn the strip off and on and enter "Safe Mode with Command Prompt." If you type "dir" you will notice a file called "kiosklog.txt" which logs every site a user goes to as well as their account number on Princess and time spent at each site.

Change directory (cd) to "c:\documents and settings\administrator\desktop\" then run "setupkiosk.lng".

You will notice a wonderful GUI menu come up with hundreds of settings to fiddle with. The most important of course, the tab called "Pricing." You can change the cost of Internet and make it free altogether by hitting "Free Internet without timer."

To make sure that this would actually save, I came back to the room at around 1:00 am. At the time I didn't know if any "hidden cameras" watched activity in the room so I didn't create the free Internet. Instead I changed the name of "Internet Cafe" to "Internet Cafe..." (just a test) and it worked.

Later I talked with a Princess employee and she notified me that those "harmless" webcams sitting next to all the computers are actually security cameras that keep video for two weeks, so change their settings at your own risk.

osiris

And keep in mind before you really piss these people off that you are in fact stuck out in the high seas with them for what could be quite a while.

Dear ***2600:***

I from time to time have picked up your magazine from the newsstand here locally. I was stunned and surprised from the very first issue I bought and read. I agree, there needs to be someone in this world with your position on information and knowledge. The next opportunity I have, I plan on subscribing to your magazine and buying *Freedom Downtime.* Please keep up the great work that you guys do at enlightening others. What they choose to do with knowledge is on them.

By the way, I have a cousin who works for Fedex and she recently wanted to buy a nostalgic item that her job carries. It was some sort of model plane. Well, when she was there on eBay's site she noticed some other items from Fedex on sale.

The first thing she noticed was a used uniform. She thought to herself, and then asked me, "Now who in the world would want to buy a used uniform that says Fedex on it?" She told me "the uniforms are free, we wear them until they wear out and the company gives us new ones." My immediate answer was "terrorists, rapist, thieves, conmen, and property masters and costume personnel from the filmmaking industry."

She told me that many stops on her route are places of importance to our government and no one ever thinks to check or question the identity of a delivery person from Fedex. Just out of habit, security and other personnel tend to "let them through."

So after hearing this from her, I went to eBay to take a look for myself, and lo and behold there the items were. I saw them there for sale too, shirts, sweaters, and whole used uniforms.

I was wondering if Fedex knows this? This can't be legal, right? Aren't they concerned about individuals using their name for fraudulent or even worse possible activities?

I thought to myself that *2600* should know about this. My cousin already reported it to Fedex. That situation's progress is pending.

Big B. Statz

As soon as we verify that you can indeed receive in the mail full Fedex uniforms as well as other kinds of corporate and government clothing, we'll let the world know. (But we're keeping what we buy.)

Suggestions

Dear ***2600:***

I wasn't sure where to send suggestions for merchandise but this seems as good a place as any. Have you ever given any thought to selling *2600* stocking caps? I would buy one.

drlecter

Your vote has been logged. We're always open to new ideas. It takes time, money, energy, and that sort *of stuff to put out each item so we want to be sure people want something before we start investing. So please keep sending in suggestions as well as feedback on what we've come up with so far.*

Dear *2600:*

In a letter in 20:2 regarding the past article "Fun with Hosting on Cable/DSL" in 20:1, Toby asked to be informed if anybody knew of good dynamic IP DNS services. I personally use DHS (http://www.dhs.org) which picked up after Monolith went under (.ml.org - ah, the nostalgia). For $5 they'll give you a few subdomains (the limit was four when I signed up but I can't seem to find any reference to exactly how many you're allowed). It used to be free but not enough people were donating. I'm not sure if this is exactly what he had in mind but I figured it was worth sending in.

Ion

Dear *2600:*

I found a very simple way for telemarketers to automatically delete your number from their call list. Just answer as "Customer Service" every time someone calls you. As soon as a telemarketer hears that, by law they have to delete the number because they are not allowed to call businesses.

PCBootleger

There's no law we can find that prohibits telemarketers from calling businesses. Your method will work though if the telemarketers are targeting individuals. However you may very well wind up opening the floodgates for a whole new kind of pitch.

Dear *2600:*

In your latest issue (20:2) there is a letter from Encrypted explaining the difficulty of overcoming bios passwords in order to overcome Deep Freeze. An extremely simple way to remove any bios password is to simply use the reset CMOS jumper on the motherboard, which clears all settings for the bios, including the password. If you aren't familiar with motherboards enough to find a cmos reset jumper, simply unplug the computer and remove the tiny clock/cmos battery on the motherboard (usually the size of a quarter). This should reset the CMOS and solve any bios password difficulties you may have, although your school may find it rather suspicious for you to be popping open computer cases and fiddling with the motherboards.

scissorjammer

Dear *2600:*

In reference to 20:1 letters, may I first suggest to Ray who is having problems with billings from AT&T that he check out bigzoo.com for prepaid long distance service. My daughter told me about it more than two years ago. I checked it out for three months before kissing AT&T goodbye forever. (They're 2.9 cents a minute anytime.)

Second, to DriZakE, same issue, you did not mention returning the check to the "old woman." If you didn't, you have joined probably dozens of other lowlifes who also ripped her off. Since she lives in your area, you and your wife should visit her to see if she is all right. She might be eating only dog food by now.

Concerned Grandma

The Authorities

Dear *2600:*

I just bought my second issue of your magazine. First off, I'd like to say that I think you are doing a great job and I think that the "Future of Computing" article was a very thought provoking scenario. This approach would be brought on by the ignorance and paranoia of people who make the rules. Case in point: My school has announced that at the beginning of the 2003-2004 school year they will punish students for activities on the Internet deemed inappropriate by the school, whether they are conducted in school or not, regardless if they have any relation to school at all. If the school deems it inappropriate, you will be punished. The Supreme Court has already ruled this unconstitutional, but this has no bearing since I go to a private school. I suspect that if I brought your magazine to school, I would have a "talk" with those in charge.

Well, I will be in 8th grade starting August 19th, and that means only nine more months of this crap. I'll probably go to a public magnet school, so I can finally enjoy what's left of my constitutional rights.

Performaman

Just don't be surprised when you don't enjoy them as much as you think you will.

Dear *2600:*

After reading your article "Disrespecting the Law" in 20:2 I felt compelled to write you about this matter. I actually live in The Hague (luckily at quite a distance from the ICC) but as pointed out by you it is not impossible that some day we will see American troops running around this city on a quest to free a fellow soldier. While this may seem perfectly reasonable to the American government (I mean no real American would ever consider committing a war crime (at least if you don't count invading a country without reason and holding prisoners outside of the U.S. effectively removing the possibility of a fair trial))!

What I am more concerned about are the recent developments in America's war on drugs. As in the above case America seems quite happy to strong arm any country by disrespecting the local laws and saying it is in their own interest to comply. How is this done? Well, quite simply by doing it! Recently the Netherlands have deported about six Dutch citizens to stand trial on drug charges. While I am all for stopping the production and distribution of drugs, this must be done while staying within the bounds of the law. Dutch law differs in quite some areas to American law. For one, entrapment is illegal here in Holland and any evidence obtained through this method is inadmissible in (Dutch) courts. The DEA has been sending agents over to the Netherlands who use methods that are illegal here, like entrapment and the use of criminal informants. And on the basis of the American reports these people are sent to America for trial. But in all the cases up until now they have accepted plea bargains. Why? Because they were promised that they could return to the Netherlands for the remainder of their sentence as long as they pled guilty.

I hope you see the pattern here. In a plea bargain the evidence is no longer of any interest and no further inquiry is made to look at how it was obtained. To be honest, the Dutch government is as guilty as the American government as it would appear there are no checks or controlling government bodies in place to regulate America's activities here in Holland (although there are voices growing in the government about this and hopefully soon there will be more clarity about this matter). Also the Dutch justice department should be more concerned with the validity of the evidence and the way it was obtained than they are now. Only yesterday I was watching a documentary about these matters on Dutch public television and in an interview the head of the DEA said that America always works within the bounds of the law of the country they reside in. When confronted with the evidence that this was not the case, the camera crew had to leave the building immediately and the interview was finished. I would like to think that soon America will come to realize that if they keep on acting in this way they will not only alienate themselves further from the rest of the world, but will also create an air of fear throughout the world as it would appear that nobody is safe from the American justice system. I would like to think that the Dutch government will start to stand up against these Wild West policies of America and start protecting its citizens against illegal and unfair methods such as those being used by the American government at this time.

All I need to say now is keep up the great work. And don't let your voice be silenced by those who fear the truth and try to force their way of thinking on you. We all have minds capable of making our own decisions. Let's use them instead of accepting someone's word for it!

Alan
The Hague

It's an amazing parallel to some of the things individuals are going through in the States when you see how governments around the world seem to be giving up their rights in deference to the USA. At least you still have media with the guts to confront this head on. Hopefully the populace will shame the Dutch government into reversing this trend of embracing intimidation.

Concerns

Dear *2600:*

Long time reader, first time writer. I have been purchasing your magazine from the local Barnes and Noble for the past three years and have been considering getting a subscription for quite some time now. The only thing that is stopping me is that all of my current magazines are all nice and pretty, without the subscription label, and I fear that if I subscribe then the magazines will come defiled with my name and address. I was wondering if this was the case, or if it came in a plain brown wrapper. Keep up the good work!

Caps Lock

Fear no more. We haven't put labels on the magazines themselves for a number of years. Subscriptions, as well as back issues and all the other stuff we have, are sent in envelopes and - not only that - they don't reveal that it's actually from 2600 in case you share a house, office, country, etc. with ignoramuses.

Dear *2600:*

Funny how your magazine has a picture of what appears to be a telephone or power line pole cut in half and only a week after getting your magazine, parts of the Northeast lose power. I'm not pointing fingers - I'm just saying that's very peculiar.

Sam

Yes, our timing continues to be an attribute and a curse at the same time.

Dear *2600:*

I was watching the TV today and saw that a large section of the eastern United States was in a blackout. Everyone immediately though it was terrorists, and I guess I can see a reason behind that, but the kicker was when I flipped on CNN and saw the ticker at the bottom of the screen say "FBI: Hackers are confirmed not to be responsible for blackout." How come when a power outage happens (and they do happen quite often), "hackers" are instantly a suspect?

Martin

Whenever something happens that people don't understand, who better to blame than those who are least understood?

Chastising the Ignorant

Dear *2600:*

This letter is in response to Amanda, Camille, Meriam, and Christina who are eighth graders at a school in Queens, New York. I am a senior that attends high school in New Jersey. Let me start off by saying that a very small number of chatrooms are used to set up meetings that turn into child abductions. Many chatrooms are used solely to talk about music, movies, computers, and things that have nothing to do with sex and "children and honest companies." Chatrooms are not bad. Are *all* websites bad? There's plenty of child porn sites out there. Have you ever actually read *2600?* In *2600,* they print the stuff that our schools would never teach us. In fact, if you read a lot of letters sent to *2600,* when schools find out we are reading this stuff, they freak out. Freedom of information is what *2600* is about. They print articles that teach how to explore, not destroy. I've never seen *2600* "support chatrooms" before. *2600* supports freedom in all aspects, exploration of technology without malicious intent, and justice. I've been a reader since I was in seventh grade and I have never read anything showing the *2600* staff supporting any injustices or wrongdoing (such as child abductions, etc.).

Now that my rant is done, where do you see *2600* supporting exploitation of children and honest companies? You provided absolutely no evidence, and you have obviously given in to the brainwashing that schoolteachers push on kids everyday. Please, if you're going to write a report, don't write it on chatrooms or anything related to technology because you are very ignorant on the subject when it comes down to it.

leetkurp

We don't consider ourselves experts on the subject but it seems that if one were to plan a child abduction, about the last thing they would want to do would be to discuss it in a chatroom. And now we no doubt will be accused of giving free advice to child abductors.

A Sign of Hope

Dear *2600:*

An interesting thing happened to me yesterday. I had gone to Office Depot to try to find an organizer for school and was waiting around while my mother looked throughout the store. I saw the computer section where all the floor models were being shown off and decided to have a little fun. I went up to one of the computers (they were all running Windows XP) and logged in to the guest account to play around a little. After a while I got bored of this and decided to see if the Administrator account was open. (Any Windows OS based on Windows NT has a default Administrator account with no password.) I logged out of the guest account, then tried first to log into the OfficeDepo account (which was a password protected admin account). Since I couldn't get in that way, I decided to try the default Admin account. From the login menu I held down the Ctrl and Alt keys and pushed Del twice, thus bringing up the Windows 2000-style login box. I typed "Administrator" as the username and left the password box empty, then clicked "Log in." Sure enough, the store had not set the password for the Administrator account and had left it completely open. So I decided to play around a little with the user accounts. I opened up the User Accounts control panel and changed the Office Depot's Guest account to Administrator level, then took the password off of the OfficeDepo's admin account. As I was doing this one of the store employees walked by and asked if I was finding everything to be satisfactory. I said "yes" and he went on his way, paying no attention to what I was doing. I was amazed at how blind these people could be at times, but continued my tinkering.

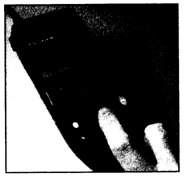
I decided to change the Administrator account password, and as I was changing it, another one of the employees walked up and said "trying to change the password, huh?" Freaked out a bit by his inquiry, I told him that I was "just seeing what the system could do." His next remark surprised me, though. He smiled with a smug expression on his face (like the "I know something you don't know" look) and said "Go ahead, change it. I'll show you a little trick." Well, at this point it was obvious to me that he wasn't going to kick me out of the store or anything. It seemed that he was challenging me to lock him out of his own computer. So I complied with his wishes and put a password on the Administrator account. He then asked me what the password was and I told him, and I then explained to him that I had accessed the hidden Administrator account, which by default has no password. I told him all I knew about it and he was surprised by this information, as he hadn't known of this vulnerability before.

After I told him how it was done, he proceeded to log in to the OfficeDepot account and remove the Administrator account password by changing that account in the Users control panel. I knew of this trick but was surprised that it worked on the default Administrator account. After the little demonstration I chatted for a while about computer security and the failure of the Blaster worm and left the store encouraged and smiling. I figured most people would overreact to what I was doing, but instead the man had actually treated me civilly and kindly and even talked with me about security. I'm glad that not everyone in this world has unjust misconceptions of hackers. I just hope that I'll meet more people like this in the future. The man even waved and said "have a nice day" as I left (though it's possible that's just a part of his job).

theXorcist

This goes well beyond someone just doing their job. That person had a very healthy outlook towards technology, one we would all do well to imitate. He wasn't afraid of what you might do to the system because he understood the basics of how it worked and he was confident in its overall design. He was also willing to listen and learn something new, an attitude which results in people (especially hackers) explaining what they know, as you did. This kind of thing happens all too rarely but it's always good to see it take place.

The Threat of [redacted]



by _cHiCkEn__

My school recently underwent a renovation. Schools in Pennsylvania are spearheading a push for biometrics as identifiers for everything from entry systems to school lunches. Probably has something to do with the fact that our last governor (Tom Ridge) resigned to take the president's position of the head of Homeland Security.

The first - and the biggest - pain to myself and the other students of our hick town is the biometrics for school lunches. It's built using a combination of software made by Food Service Solutions (www.foodserve.com) and a biometrics suite called MorphoTouch made by Sagem Morpho, Inc. (www.morpho.com). To get the system initialized, we were all assembled at lunchtime and scanned in using both forefingers. Along with this, they associated our student ID. Conceivably, the MorphoTouch website says that any data can be stored in these files (obviously this is true, because Sagem Morpho has contracts with several military and governmental organizations).

The MorphoTouch uses a set of 27 non-alterable points on the finger as the basis of its biometrics. These points are calculated and fed into a one-way algorithm. The results of this algorithm are compared to the results stored in each student's file in the Food Service Solutions' database. Supposedly, this number cannot be fed back into the algorithm to get the fingerprint, but one wonders with Sagem's close relationship with law enforcement. Needless to say, the original quality of the fingerprint scanned is said to be non-permissible in a court of law, yet it could still help authorities to some extent.

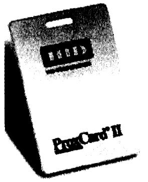
This whole system is said to keep the classic story of the bully stealing someone's lunch money from happening, yet it's a moot point. That hasn't happened in ages at my school and, if they really wanted to, they could just steal the lunch itself. Parents are allowed to deposit money in the student's account and are assured that the money cannot be spent for anything else. They are automatically notified by a printout or even an e-mail when the student runs into the negatives.

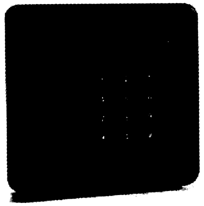
Now, onto the second pain (which has yet to be completed). My school's had a long-running problem of unauthorized access after hours. It is said that back in the day when the school had given keys to the teachers that about 60 percent of the town had a copy. Then they went to a randomly generated keypad system, which, after some time everyone knew the PIN to also. Now they've taken extreme measures on this issue. They've installed a remote smart-card reader manufactured by HID Corporation (www.hidcorp.com). This card can be read up to eight inches from the keycard reader by the doors. The card reader also has a keypad which can use either a PIN number for access or the smart-card. But this reader may also be configured to require *both* the smart-card and the PIN.

I've heard rumors of including the already established MorphoTouch system as a facilities access control as well as the HID system - this stands to reason since all the teachers were required to give up their fingerprints too.

Some students have resisted these advances. Parents have been forced to write notes to the school for their children to be allowed to still eat lunch without giving up their fingerprints. They've been forced to remember their student ID number instead - which is almost as bad since their money is still stored in the same Food Service Solutions' database as everyone else's. The cafeteria manager has been especially hostile to such students, even going so far as to phone students' homes and get into heated conversations with their parents.

Here in South Central Pennsylvania, we're on the bleeding edge of technology, biometrics, civil liberties, and the wish to murder tree huggers.





Gentner GSC3000 for Total Morons

by blakmac
page33@mail.com
http://page33.port5.com

As you know, radio stations use transmitters to relay signal from the towers to receiving antennas, whether they are other towers or the old bent-up clothes hangers that are taped to the back of your radio. One of the more popular transmitter companies is Gentner. Gentner manufactures various equipment, ranging from FM transmitters to hearing assistance equipment. In this article, we will look at some of the features of the Gentner GSC 3000 Remote Facilities Management device as used by one of our local radio stations. Of course, this is for educational purposes only. Besides, if you are stupid enough to tamper with one of these pieces of equipment, you deserve the trouble you will receive.

The Equipment

While I have never seen one of these transmitters in person, I did interact with it on a regular basis while working at a local radio station. At least once per shift, we were required by the FCC to check the transmitter voltage, plate current, and forward power that the transmitter was operating at. We did this by dialing up the Gentner GSC 3000 and feeding it commands via the telephone keypad. We will get to the commands shortly. The location of the transmitter was actually about 15 miles from the station. I'm sure you have seen radio towers; the transmitters for the towers are usually kept in a little hut at the base of the tower. If anyone has been inside one of these and has pictures/information about them, please e-mail me. There are two ways to communicate with one of these devices: via modem dial-in or via telephone with the voice module installed. At the station, we always used the voice module access, probably because the "network admin" was quite incompetent when it came to computers. We will be focusing on this method of communication between the user and the hardware.

Dialing In

Usually the telephone numbers for these machines are not listed anywhere, therefore only a privileged few can access the machine. There are very good reasons for the security of this access. For example, you can change the broadcast voltage of the transmitter, which can cause lots of unmarked vans to appear in your location. You don't want that. In our small town, the transmitter number was at one time published in the local telephone book! However it has since been removed. When you dial the number, if the voice module is installed, you will hear a robotic voice saying something like, "Hello, this is the KXXX transmitter site, please enter access code." It's always a good idea to have difficult passwords, but as we know given that there are only ten numbers on a telephone, they can easily be guessed. The GSC 3000 has two passwords for the system, a five digit general access password and a seven digit system access password (root!). When you enter the general access password, you will hear a message saying that there are either alarms pending or no alarms pending. Basically, these alarms are for signal status. For example, if there is dead air being passed over the transmitter, an alarm would be issued and, in our case, the phone would ring at the station on a special line, as well as at the station owner's house, and a signal would be sent to the program computer at the station to begin playing music. Once you are past the alarm message, you can enter codes to access the various features of the GSC 3000. Here are the available options:

For checking meters:

501# - Sequence One Enabled (runs through the meters and gives you the stats)
601# - Transmitter Voltage
602# - Plate Current
603# - Forward Power
604# - Reflected Power
607# - Microwave (STL) Power
701# - Signal Status
050# - Monitor On
*050** - Monitor Off
000 - Report Alarms
010 - Clear Alarms
030 - Master Alarm Override

Other Commands:

Main Transmitter - *201#* power on, *201** power off
Transmitter Power - *202#* raise, *202** lower
Transmitter Reset - *203#*
Power Adjust - *204#* raise, *204** lower
Power Control - *205#* auto, *205** control adjust
999 - Goodbye

For our local transmitter, there is another telephone number that you dial to get the status on the power going into the transmitter. For example, you dial the number and enter a five digit password, then enter 704* to get the power status report.

Passwords

As with any sensitive equipment, passwords should be chosen carefully and not carelessly. By looking at the commands available for remote use, you can see what kind of power lies in the ability to access one of these machines. At the local station, the password for general access was 11111 and for total system access it was 9999999. It's rather sad to think that these are very easily guessed passwords that can have quite dramatic consequences. Let's imagine that Evil Joe wants to get back at the radio station for something. Joe calls up the GSC 3000, guesses the password, then kicks the power up on the transmitter. The station is then subject to severe fines and penalties if the FCC finds out (and they will). This isn't a pretty picture, especially if and when it can be proven that Joe doesn't work for the station and he's the one that tampered with the equipment. Just imagine the penalties for that. However, I feel that the station is partially to blame in this scenario due to a lack of diligence in setting up their passwords. These machines aren't very secure to begin with, considering the password scheme that they use. If you run a station, be smarter than our local station, please.

Conclusion

The Gentner GSC 3000 is a very useful tool for monitoring radio equipment, however it is insecure. The password schemes should be redesigned, although I realize that it is limited to the ten keys on the telephone keypad. Possibly incorporating a longer password would be a viable solution to this problem. I have listed some resources for more information below, and if anyone has more on these devices, feel free to e-mail me with any information, corrections, etc. that you may have. Please, use this information responsibly.

References

Gentner Technical Support - 800-283-5936
http://www.burk.com/support/manuals/
GSC3000.pdf

Greetings to diversereality, kryptOnOmicOn, Horathgar42, WarHwk1974, the imposter.

Marketplace

Happenings

INTERZONE III. April 2004. Not just another hackers' con! Stay tuned to website for more details. www.interz0ne.com (that's a zero!)

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.

For Sale

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting based on Linux servers. Our hosting plans start from only $4.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. Privacy is guaranteed and you can pay by E-Gold, paypal, or credit card. http://www.kaleton.com

DRIVER'S LICENSE BAR-BOOK and "fake" ID templates. Includes photos, templates, and information on all security features of every single American and Canadian drivers' licenses. Including information on making "fake" ID's on PVC cards, laminating, making holograms, magnetic stripes, software, and more to make your very own license! Send $25 cash in US funds or an international money order in US funds made out to R.J. Orr and mailed to Driver's Bar Book, PO Box 2306, Station Main, Winnipeg, Manitoba, R3C 4A6, Canada. Order now and get FREE laminates with every order! We ship worldwide free!

ONLINE RETAILER OF COMPUTER PRODUCTS is also a *2600* subscriber! 60,000 different computer products from components to complete systems, laptops, PDAs, cables, RAM, and media all available online at http://www.digitaleverything.ca. Worldwide shipping is no problem. Just mention you are a subscriber and I'll give you better prices too. Contact Dave at sales@digitaleverything.ca for more info.

AT LAST AN ACCURATE DESCRIPTION OF THE BELIEFS AND BEHAVIOR OF HACKERS! Social Inquiry offers a research report produced by Bernhardt Lieberman, emeritus professor from the University of Pittsburgh and Director of Social Inquiry, his own social research firm. Professor Lieberman held appointments in the Departments of Sociology and Psychology at the University of Pittsburgh. He conducted a detailed interview of hackers in Pittsburgh and administered five questionnaires to them: a hacker motivation questionnaire, a hacker ethic questionnaire, an attitude toward the law scale, a liberalism-conservatism scale, and a personality questionnaire designed to deal with the myth of the hacker as a social misfit. Professor Lieberman attended H2K2, observed the behavior of hackers in convention, and administered the five questionnaires to hackers attending H2K2. The report also contains a content analysis of *2600*. The report presents a description of the beliefs and behavior of hackers produced by these methods of inquiry. The report is neither a condemnation nor a whitewash of hackers, nor does it justify the actions of criminal justice systems and the disciplinary actions of school administrators. It is designed to offer a more accurate picture of hackers than the pictures presented by the mass media and the criminal justice systems. The report recommends that the desire of hackers to learn about computers and computing should be channeled into constructive ends, as much as that is possible. The report is 140 pages long and contains 55,000 words. Professor Lieberman received no grant or contract money to do this work; he did the work using his own money and was, and is, beholden to no one. To get a copy of the report send a check for $23.50 + $4.50 ($6.00 outside North America) for shipping (in U.S. dollars) payable to Social Inquiry, 627 Beverly Road, Pittsburgh, PA 15243. Those fortunate enough to have institutional funds to pay for the report are invited to send a purchase order. If you want more than one copy, call 412.343.2508 or email blieber@telerama.com.

SIZE *DOES* MATTER! The Twin Towers may be gone forever but a detailed image still exists of the massive 374-foot radio tower that was perched atop One World Trade Center. This high-quality glossy color poster is available in two sizes (16" x 20" and 20" x 30") and makes a spectacular gift for engineers, scientists, radio and television buffs, or anybody who appreciates a unique, rarely seen view of the World Trade Center. Visit www.wtc-poster.us for samples and to order your own poster.

HACKER T-SHIRTS AND STICKERS AT JINXGEAR.COM. Stop running around naked! We've got new swagalicious t-shirts, stickers, and miscellaneous contraband coming out monthly including your classic hacker/geek designs, hot-short panties, dog shirts, and a whole mess of kick-ass stickers. We also have LAN party listings, hacker conference listings, message forums, a photo gallery, and monthly contests. Hell, don't even buy, just sign on the mailing list and have a chance to win free stuff. Or follow the easy instructions to get a free sticker. Get it all at www.JinxGear.com!

WIRELESS SECURITY PERSPECTIVES. Monthly, commercial-grade information on wireless security. Learn how to protect your cellular, PCS, 3G, Bluetooth, or WiFi system from *2600* readers. Subscriptions start at $350 per year. Check us out at http://cnp-wireless.com/wsp.html.

TAP/YIPL The original phreaking and hacking zines! All original back issues on CD-ROM. Only $5 including postage! Write for a free catalog of the best underground CD-ROMS! Whirlwind, Box 8619, Victoria BC, V8W 3S2, Canada.

LEARN LOCK PICKING It's EASY with our book. Our new edition adds lots more interesting material and illustrations. 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 2600 reader price discount.

WEBIEZINE, the first and only monthly compilation CD zine featuring new and popular software, text files, e-books, reviews, tutorials, graphics, videos, music, and more. Please help *Webiezine* to continue and grow by submitting files or links or suggestions to psytekusa@hotmail.com or submit@webiezine.com. Anything is accepted. Order yours online at www.webiezine.com or http://store.yahoo.com/webiezin. Also check out www.webiest.com for the best prices on hosting, co-location, and web design!

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

WORLD'S FIRST "DIGITAL DRUG." Hackers, get ready to experience the next level in wetware technology! VoodooMagickBox is a 100% legal and safe way to enter into a drug-like trip, All you need to do is place the clips on your ears and turn the knob on the VoodooMagickBox. It's like nothing you've ever tried! For details and ordering information, visit www.voodoomagickbox.com (money orders and credit cards accepted).

CABLE TV DESCRAMBLERS. New. (2) Each $115 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132.
Email: cabledescramblerguy@yahoo.com.

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 $3 cash to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

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.

Help Wanted

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

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.

Wanted

BUYING BOOKS AND MORE. Man interested in books related to hacking, security, phreaking, programming, and more. Willing to purchase reasonable books/offers. I do search Google! No rip-offs please. Contact me at lbda@att.net.

FREE SOFTWARE DISTRIBUTION. I have a website (www.eloder.com, come check it out!) that has a fair amount of traffic. Mostly for debian and redhat cds. I am looking for hackers who have made their own interesting programs and wish to share. If you have some really interesting apps, I can give you (for free!) a page or a sub domain. I am looking to assist the open source movement and the hacker community. You can email me at eloder@hotmail.com. Please place "download" in the subject heading. All interesting ideas welcome. Eric Loder.

NEED DIAL UP HACKING INFO (steps involved, current dial ups, etc.) Also looking for places on the Internet where I can get unlisted phone numbers for free. Please contact me at billm2@prodigy.net.

THE NEW YORK CITY INDEPENDENT MEDIA CENTER (NYC-IMC) is looking for donations to help build an IU server to host its open publishing web site. NYC-IMC (http://nyc.indymedia.org) is an all volunteer collective and is part of a worldwide network of over 100 media centers (http://www.indymedia.org) dedicated to maintaining an open publishing web system covering progressive issues and built using open source technologies. NYC-IMC has outgrown its current server and host and would like to create a robust, rack mountable server that can be collocated with a faster provider. If you can donate time or parts to help build our server, please get in touch with the NYC-IMC Tech Team at imc-nyc-tech@indymedia.org.

SEEKING INFORMATION ABOUT TRACFONE. Looking for technical data concerning the Tracfone network and how it operates, especially information about airtime and the manipulation thereof. I have been working for some time to compile an extensive tutorial about Tracfone and how its service works and I am currently working on the fourth revision. The third revision and quite a little bit of information that I have already discovered on my own can be found at www.americasleastwanted.com in the Scams & Fraud section of the site. Send any information via e-mail to tracfone-response@americasleastwanted.com. I will not pay for information and you shouldn't want to charge for it because that would be against your hacker ethics. Or something. I am also looking for people to write tutorials and other content on this site as well. Contact webmaster@americasleastwanted.com if you are interested. These will also be unpaid positions.

IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tactics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

Services

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting based on Linux servers. Our hosting plans start from only $4.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. Privacy is guaranteed and you can pay by E-Gold, Paypal, or credit card. http://www.kaleton.com/

PAY2SEND.COM is an e-mail forwarding service that only forwards messages from whitelisted contacts or people who pay you to receive from them, using a patent-pending identity technique. Sign up via our web page form.

VINTAGE COMPUTER RESOURCES FOR RESEARCH. VintageTech provides a wide variety of computer historical related services for business and academia. We provide: support services for legal firms for computer and software patent litigation and prior art research; props and consulting for movie or film production and photography studios requiring period authentic computers and computer related items; data recovery and conversion from old and obsolete data media to modern media; appraisals of vintage computer items for sale, charitable donation, or insurance valuations; sales brokering of vintage computers and related items; general computer history consulting and research. VintageTech maintains an extensive archive of computers, software, documentation, and an expansive library of computer related books and magazines. Visit us online at http://www.vintagetech.com or call +1 925 294 5900 to learn more about the services we provide.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, without big-brother looking over their shoulder. We provide highly filtered DoS protection. Our main server is a P3 1.2 ghz machine, 1.5 gigs of ram, 512 megs of swap, 40 gig EIDE, with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.

HACKERMIND: Dedicated to bringing you the opinions of those in the hacker world, and home of the ezine *Frequency.* Visit www.hackermind.net for details.

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

VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer viruses. The White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

Personals

RESOURCE MAN is looking for more addresses (snail mail). Please send any addresses of the following: book clubs, subscription services, newspapers, computer/hacking magazines, and any foreign addresses which are a special delight. The further away the better. Also, I am a manga/anime fanatic (dbz, Digimon, Outlaw Star, Chobits, Tenchi Muyo, etc.). Please send any related information to: Daniyel Sigsworth #1062882, PO Box 2000, Colorado City, TX 79512. Will respond if desired.

AN INTERESTED "TO-BE" HACKER IN PRISON: I am a 28 year old in prison who is interested in learning on being a hacker. I'm looking to hear from anyone who can help me get started on being a hacker, for advice, and to correspond with on anything doing with hacking. Please help an up and coming to be hacker out. I will correspond with anyone. Write to me at: Michael Engebretson #245523, Prairie Correctional Facility, PO Box 500, Appleton, MN 56208.

I'VE BEEN BAD! No one thought illegal wire transfers were funny! Can't anyone take a joke? Known as Alphabits for years. I'm bored to death in here and would like to correspond with anyone. Help a hacker out and write to me at: Jeremy Cushing #J51130, Centinela State Prison, P.O. Box 911, Imperial, CA 92251. Will reply to all.

STORMBRINGER'S 411: Am doing a 262 month federal sentence. Would like to hear from those I've lost contact with. Will correspond with others as well. Write to William K. Smith #44684-083, FCI Cumberland, Unit A-1, P.O. Box 1000, Cumberland, MD 21501.

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 Winter issue: 12/1/03.

Meetings

ARGENTINA

Buenos Aires: In the bar at San José 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.
Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.
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").

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.

Manitoba

Winnipeg: Garden City Shopping Center, Center Food Court adjacent to the A & W restaurant.

New Brunswick

Moncton: In the lounge of Ground Zero Networks, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Hamilton: McMaster University Student Center, Room 318, 7:30 pm.
Ottawa: Byward Cafe, 55 Byward Market Square. 6:30 pm.
Toronto: Computer Security Education Facility, 199a College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Terminalbar in Hovedbanegardens Shopping Center.

ENGLAND

Exeter: At the payphones, Bedford Square. 7 pm.
London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.
Manchester: The Green Room on Whitworth Street. 7 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Grenoble: McDonald's south of St. Martin d'Heres.
Paris: Place de la Republique, near the (empty) fountain. 6 pm.
Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

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

IRELAND

Dublin: At the phone booths on Wicklow Street beside Tower Records. 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: Purple Onion. 5:30 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.
Tromsoe: The upper floor at Blaa Rock Cafe. 6 pm.
Trondheim: Rick's Cafe in Nordregate. 6 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.

SLOVAKIA

Bratislava: at Polus City Center in the food court (opposite side of the escalators). 8 pm.

SOUTH AFRICA

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

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.
Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.
Huntsville: Madison Square Mall in the food court near McDonald's. 7 pm.
Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tempe: Telephones outside mall entrance to Game Works in the Arizona Mills Mall.
Tucson: Borders in the Park Mall. 7 pm.

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 (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
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: Wing Zone 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. 6 pm.
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.
Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

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.
South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Santa Fe Espresso, 116 Welch Ave.

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: La Fee Verte, 620 Conti Street. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows.
Marlborough: Solomon Park Mall food court.
Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.
St. Louis: Galleria, 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: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

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 food court.
Greensboro: Four Seasons Mall Food Court (in the back). 6 pm.
Raleigh: Crabtree Valley Mall food court in front of the McDonald's.
Wilmington: Independence Mall food court.

North Dakota

Fargo: Barnes and Noble Cafe on 42nd St.

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): Bedford Arabica, 720 Broadway-On Bedford Square (Commons).
Columbus: Convention Center (downtown), south (hotel) half, carpeted payphone area, near restrooms, north of food court. 7 pm.
Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: The Magic Lamp in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.
Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Heaven Cafe, 421 SW 10th Ave., near 10th and Stark.

Pennsylvania

Allentown: Panera Bread on Route 145 (Whitehall). 6 pm.
Philadelphia: 30th Street Station, under Stairwell 7 sign.
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: The Ugly Mug Coffee Shop, 3445 Poplar Ave Suite 16.
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 Galleria 1.
San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in "The Park Food Court."

Vermont

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

Virginia

Arlington: (see District of Columbia)
Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

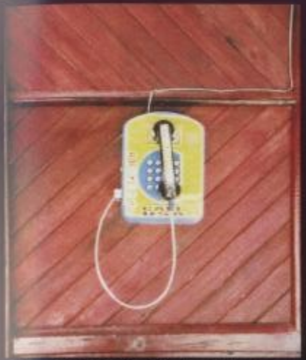
Seattle: Washington State Convention Center. 6 pm.

Wisconsin

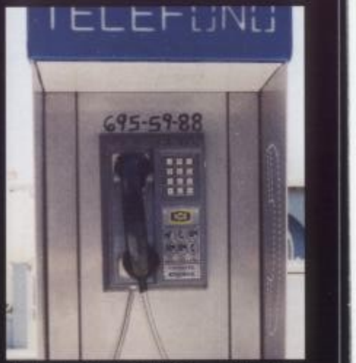
Madison: Union South (227 N. Randall Ave.) on the lower level in the Copper Hearth Lounge.
Milwaukee: The Node, 1504 E. North Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

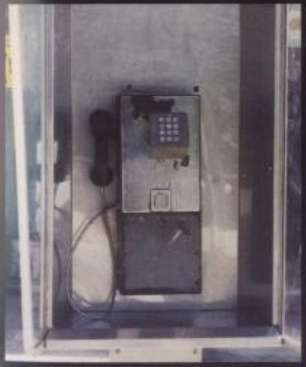
Costa Rican Payphones



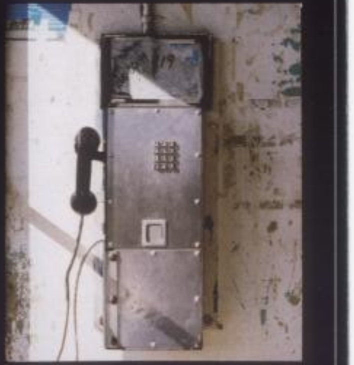
If it wasn't for the "Call USA" on the bottom, we would have had a very hard time telling which end was up on this tiny phone.



Unlike in the United States, many foreign payphones are proud of their phone numbers. We suspect this one may soon be ringing off the hook.



It's kind of hard to believe that this is in the same country, but this old metallic model phone can also be found in Costa Rica.



Our favorite is the even larger metal box with tiny keypad. Think about it - at some board meeting in the past, this design beat out the competition.

Photos by Ricardo Muggli

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