Blacklisted! 411

The official hackers magazine

HACK THE SYSTEM...

Cyber Extortion & Blackmail

Organized crime on the net?

Also inside this issue:

Using Limited Resources

DoS Attacks

Securing Grub

VOLUME 7 ISSUE 2 **SPRING 2005**

This publication is dedicated to all of those before us who built the foundation for the hackers of the world to express themselves openly and without prejudice.

While we attempt to continue in our quest to obtain knowledge and understanding, we invite you, the reader, to join in and share any thoughts you may have regarding the magazine, hacking, life, work and anything else that you feel is important enough to be shared.

We're not going to knock anyone down for asking questions or ridicule the steadfast elitist folks who believe that knowledge should not be shared. We believe knowledge should in fact be shared with one another, no matter how trivial the information may appear to be. After all, knowledge is power.

Think back to the way it was, when hackers stuck together and had a good time. An amusing time when hackers shared their stories of exploration and ultimate conquest. A wondrous time when hackers were considered the good guys and looked up to by those not fortunate enough to understand the technology around them. A simple time when a hackers harmless efforts gained a new understanding of technology issues and the praise from their peers and superiors alike.

That time can still be NOW. Hackers of the world unite and exercise your freedom to disseminate information!

Blacklisted! 411 staff & contributors

Editor in Chief
Zachary Blackstone

Assistant Editors
Alexander Tolstoy
Dave S.

Office Help
Pixel Pixie, Jess, Lexus, Dark Paladin, DoctorWHO, MomoPi, Mr. Asshole

Artwork
Derek Chatwood - A.K.A. Searcher
Kate O., Parallax, Mason/Wolf

Distribution
Greg, Boiler, Syntax, David B.

Photography
CHS, Dark Paladin, Daniel Spisak

Forum Admin
*Spratt_*

Writers
ML Shannon, Goldfinger, BarfBag, Kingpin, Double-O-Jake, Grandpa Hackman, Trash-00X, Wild E. Coyote, TechnoHeap, Rogue, The Crypt Phreaker, Erik Giles, Sam Nitzberg, Mother Goose, Cactus Jack, Bob Blick, Ustler, Stank Dawg, MobbyG

ISSN 1082-2216

Blacklisted! 411 Magazine
P.O. Box 2506
Cypress CA, 90630

9035768ABBAJBVJB-0022

DBBL 01,07,32,41,52

PRINTED IN THE UNITED STATES OF AMERICA

Blacklisted! 411 shout outs

Doc Salvage
ECSC
oleBuzzard
Dark Tangent
DEFCON
Freaky
Blackwave
IrvineUnderground
Consumertronics
Wizguru
Greyhawk
*Spratt_*
The Underground Mac
Bobeeve
German
Big Dog
Skippy
Avatar
Neuromancer
Doc Jones
LineTech
Alaric
Short Circuit
Mingle
The Goldfinger
E. Coli
Group 42
SWAT
Trash-OOX
Doule-O-Jake
Ender Wiggin
TechnoHeap
GI Electronics
Lucky225

....and a few ANONYMOUS people

Inside this issue

Additional information

How to Contact us:
Blacklisted! 411 Magazine
P.O. Box 2506
Cypress, CA 90630

Subscriptions:
$20 U.S., $24 Canada, $35 Foreign
Check or Money Order (U.S. Funds only)

Articles:
Blacklisted! 411 Articles
P.O. Box 2506, Cypress, CA 90630
(Include name & address—we PAY for articles)

Letters:
Blacklisted! 411 Letters
P.O. Box 2506, Cypress, CA 90630

Distribution and Sales:
Blacklisted! 411 Distribution
P.O. Box 2506, Cypress, CA 90630
Email: sales@blacklisted411.net

Advertising:
Blacklisted! 411 Advertising
P.O. Box 2506, Cypress, CA 90630
Email: advertising@blacklisted411.net

World Wide Web:

Website: **http://www.blacklisted411.net**
Store: **http://store.blacklisted411.net**
Forums: **http://www.bl411forums.com**

Blacklisted! 411 introduction for those of you who are new…..

Who we are… and were…

The question often arises on the subject of, "How did it all start?" in reference to our magazine and it's history. In response to this popular question, here is a quick history lesson of *Blacklisted! 411* magazine, including names, dates and little known facts which have, thus far, been hidden away for years…

Blacklisted 411 magazine dates back to October 1983 with a group of friends from a Southern California high school that shared a common interest. We were all into our Atari computers, Commodore computers, electronics, sciences, arcade games, etc. We built projects, hacked into this n' that, came up with grand ideas and tried to make them into some sort of reality. The group started a monthly hackers "disk magazine" (an early form of what is now known as an e-zine) called "*Blacklisted 411, the hackers monthly*". This may sound strange today but circulating information on disk was the best way to get it out without all the cool toys of today. We didn't have the internet to send it out, and no one had printers that could print anything other than plain text (and didn't even do that well). With a disk based system we could send text files, primitive graphics/pictures, and utilities more easily and it could be copied by anyone who had a compatible computer. At our peak we distributed 150 disk copies <per month> of the disk magazine, though there is no way to know how many were copied by others.

Eventually modems caught on and we began to distribute the monthly via crude BBS systems. Using the power of a Commodore 64, we put up a *Blacklisted! 411* info site, which anyone could log into without handle or password. It was a completely open message center. Using X-modem or Punter file transfer protocols, you could download the latest *Blacklisted! 411* files or read/leave "messages" which later became known as a "message base" and has evolved into what are now commonly known as "newsgroup postings" or "forum postings". We had only one message center, no email capability & only 1 phone line. Primitive, indeed. Effective, however.

Around 1984 we purchased a 9 pin dot matrix printer that could <gasp> print basic graphics. We experimented with printing out copies of the *Blacklisted 411 monthly* and copying them at the media center at the high school. The media center staff graciously allowed us to make these copies free of charge which was very cool at the time. We'd pass these out at the local "copy meets" (an interesting phenomenon of past times - hordes of computer users would meet at a predetermined location and setup their computers with the sole purpose of copying software and exchanging this software with each other). We'd leave a pile of our magazine copies anywhere we were allowed to do so. One popular location was next to the Atari Gauntlet and Gauntlet II arcade games strategically located at 7-11's all over the place. We're only guessing here, but we think people photocopied our copies and then those were photocopied, etc. There's no telling just how many generations of early printouts of *Blacklisted! 411 monthly* made it out there.

Years went by and *Blacklisted! 411* evolved. The short life-span of the printouts was both a great success and a miserable failure. No matter where we left them, they were taken - and taken quickly! The feedback was awesome in that people wanted more. The interest was very high, but our inability to meet this growing demand was completely overlooked. We had to officially pull the plug on the printout experiment and we stuck with electronic files. It was really the easiest way to go. The *Blacklisted! 411* info site grew into a 2-line system. This was a big deal in 1985. By that time, information was almost exclusively passed around by modem (unofficially on paper) and we were still releasing disks at this time.

June of 1987 marked the end of *Blacklisted! 411, the hackers monthly*. Our last disk based magazine was distributed that month. Now that all of us were out of high school and onto college, work and the bigger/better things in life, nobody had the time or inclination to put any effort into the disk based magazine anymore. The once thriving *Blacklisted! 411* group broke up and people went their separate ways. Naturally, we all assumed this was the end and *Blacklisted! 411* would never come back in any form.

In the summer of 1993, one member (and the original editor-in-chief), Zack Blackstone, felt it was time to revive the *Blacklisted! 411* concept, but this time do it as a print magazine. It was extremely difficult to get started because the group was no more. He was the only one of the original group members remaining that had an interest in bringing the hacker group and magazine alive again. With some money, will to make it happen, and with the help of some top of the line (at the time) computer gear and page layout software *Blacklisted! 411* was reborn. *Blacklisted! 411* Volume 1, Issue 1 was released in January 1994. *Blacklisted! 411* was finally BACK. The issues were released monthly and distribution was small. After a year passed, it was decided to try a quarterly format in an effort to increase distribution. During that year Zack managed to get in contact with many of the old group members and they are now active staff members once again.

In 1999, we published what was to be our last issue of *Blacklisted! 411* (Volume 5, Issue 4) for many years to come. We didn't know it at the time, but many pitfalls would ultimately cause the demise of the magazine. After 4 years of regrouping and planning, *Blacklisted! 411* magazine is back in print form again. We are one of the oldest group of hackers still remaining and releasing gathered and compiled information within the hacker community and the mainstream community as well. We still have the same hacker mentality and code of ethics from the 80's. Hackers are not thieves - they're curious people. We are not elitist hackers by no means and no question is a stupid question. We're not going to knock you down, call you a "lamer" "lamah" or give you crap for being a newbie! Every hacker started somewhere. We remember this most fundamental fact and we will never forget it.

What's Next…

Community
Over the next few months a lot will be happening. We are becoming more active in the Hacker Community. As we are based in the Los Angeles area, we are building relationships with the local Hacker groups such as LA2600, SD2600, twentythreedotorg, Irvine Underground and more. We will be attending and sponsoring Hacker Conventions and Conferences. The first being the Layer One Convention, June 12-13, at the LA Airport Westin. We will have a booth at this event where we will be selling subscriptions, current and back issues of the magazine, and other swag. We will also be having several "convention only" promotions so look for us there.

Magazine Development
A major effort is being made to increase our exposure to the Hacking and Information Security Community. Our distribution goals are for the magazine to break 100K copies distributed each quarter sometime next year. Based on the demand, and orders from distributors we are on the right path. We are seeking and hiring freelance writers, photographers, and editors to increase the quality and scope of the magazine. Additionally, we have people who are actively trying to promote the magazine both inside and outside of our close community.

Merchandising / SWAG
We wish to have a whole series of *Blacklisted! 411* themed swag and merchandise. This includes stickers, apparel, posters, and whatever else our creative minds can come up with. Input, help, and direct submissions for this will be accepted and appreciated.

Charities
Blacklisted! 411 is run by real people who care about other things aside from hacking. No, really. In the spirit of helping people and organizations outside of our community, *Blacklisted! 411* Magazine has officially donated to the local chapter of the Ronald McDonald House charity. After all, children are our future. *Blacklisted! 411* Magazine wholeheartedly supports the Ronald McDonald House mission and their programs. Additionally, we've donated heavily to the Westminster Parish Festival, specifically with the intent to help support their youth programs and special classes for the mentally and physically handicapped.

If you have questions, comments, articles, ideas, flames, general "screw you guyz" messages or wish to offer support in some way, please contact us immediately and let's see what we can do. Thanks for your support, hackers! ***BL411***

Letter from Zachary Blackstone, editor-in-chief…..

Welcome to another issue of Blacklisted! 411 Magazine. Yep, it's that time again. Welcome to the latest edition of Blacklisted! 411 magazine. Due to some issues with the way we were running things (ie: no real backup plan in place), we missed distribution of the Winter 2004 issue and this issue (Spring 2005) was severely delayed. I'm happy to report that we're back on track, have disaster plans in place and have both the Winter 2004 and Spring 2005 in print. The Winter 2004 issue will be sentout to all subscribers as a "freebie" which will not count towards their subscription.

Our forums (www.blackklisted411forums.com) are doing well despite our lack of presence for the last two seasons. Though, come on people, it could do a lot better. Get on there and post post post like it's going out of style. We know you're out there, so take a few minutes from your hacking and make a few posts. And to those of you that somehow failed to notice we had a forum, go check out the forums and voice your opinion right now. Pretty much anything goes…..as long as it's legal.

We've hired several new people to help with day to day operations which will help keep myself and the editorial staff free to be creative rather than deal with the boring stuff all businesses have to put up with. Because of this, we've been able to look into other areas of the magazine, trying to expand the scope of what we have to offer.

In fact, we've been tossing around the idea of a DVD documentary for Blacklisted! 411 magazine which would take the viewer on a tour of our day to day operations and bring into perspective the lives of hackers, how what they do affects the world on a local scale as well as a global scale. We've already got a lot of footage ready to go, but we're still arranging interviews with many people, so there's no timeframe on when the DVD will be done. Though, it's a priority, so we'll be putting a lot of effort into making this happen ASAP. When we're done with the DVD, all current subscribers will get the DVD free of charge. Everyone else will be directed where to purchase. Keep your eyes open for this one.

We're also thinking about opening up a "lab" which would be accessible to anyone who is interested in getting hands on experience with new technology and old technology, located in one convenient place with an easygoing, laidback atmosphere. In other words, a place where we can get together, have a good time and dig into the guts of technology. Our intent is to make it open to the public M-F 9-5 with the idea that real hackers would be working hand in hand with manufacturers and suppliers to pull apart, test, modify and review technology.

This idea has been going around and around for some time now and we haven't been able to get a grip on the specifics, but I just wanted to let all of you know that this is a serious possibility. I would really like to hear from the readers in case they have any ideas on this subject or possibly anything tangible to offer in an effort to bring this idea to a reality.

Additionally, we've made contact with several graphic artists and manufacturers which has provided us with some solid leads on having SWAG available by Defcon 2005. We'll probably go with shirts, hats and stickers...you know, the usual crap. Although, I would really like to offer something unusual and exciting. What? I have no idea…..yet. If you have any cool or unusual ideas for branded merchandise, send me a note and let me know what's on your mind.

Calling all writers. We're looking for talented writers who have a technical background and who would like to write for us. Blacklisted! 411 has always been known for the type of material it's provided our readers with, however, lately it has gained a reputation for more technical articles than that of our counterparts. In the spirit of trying to maintain that level of recognition, we're inviting all writers with a solid technical background to submit their sample articles and/or to submit their exclusive material for us to review and possibly include in an upcoming issue. We are the only widely distributed "underground" hacking magazine on the planet which actually pays it's writers. Why go elsewhere when we can show you the money?

So, get around to it and inquire ASAP. Make contact through our contact form available at www.blacklisted411.com or snail mail a letter to the editor.

Are you an artist? Same as above - we're looking for graphic artists who can supply us with material for use inside (and outside) of the magazine as well as on our website, merchandise and the upcoming DVD project. Yes, it's a paying gig, too.

In fact, if you have anything at all to offer us; swag ideas, merchandising, promotional, meetings, layout of the magazine, distribution, value added ideas ….even things we haven't even considered yet, why don't you give us a buzz. We want to keep this magazine fresh and interesting. We've done a great job so far, according to most people who bother to offer an opinion. If we can continue to kick ass, that would be great. So, if you have anything to offer us, speak up now! We'd really like to hear from you.

Send your stuff to:

Blacklisted! 411 Magazine
P.O. Box 2506
Cypress, CA 90630

Or you can contact us here:

http://www.blacklisted411.net (go to the contact form)

Many people have noted the changes we've made across the board with the magazine since our comeback with the Winter 2003/2004 issue. We'll keep reading those comments and apply them where needed. It's good to know that the hard work has not gone unnoticed. Thanks everyone!

Ok, so we have a great issue with some excellent articles which should keep you glued to your seat....for a little while anyway.

The Goldfinger has supplied us with some really interesting topics, including interviews with various folks and the fringe side of the hacking community. This issue, there's a Q&A interview with Lucky225. He's fairly well known to the community, so no introduction should be necessary.

There's an article on electronic surveillance by M.L. Shannon on page 19. It's part three of an ongoing series he's written exclusively for Blacklisted! 411. It's a good read.

There's info on social engineering, hacking XMDirect cables and even a bunch of reviews from yours truly. All in all, this is a good issue and I hope all of you enjoy it as much as we do here at the Blacklisted! 411 HQ.

- Editor

Notes of interest:

- We're accepting design ideas for SWAG - t-shirts, baseball caps, bumper stickers, etc.
- Deadline on all articles, letters, artwork and ads for Volume 7, Issue 3 is July 14th, 2005.
- ALL classified ads are now FREE and are limited to space constraints per issue. First come, first served.
- We're a PAYING MARKET for articles we use! We pay $25-$600 depending on size, quality & use of photos.

Blacklisted! 411,

In a previous incarnation in the 20th century, I wrote an article for Blacklisted411 titled, "The Secret Macintosh"; as I recall, all copies I saw printed my article upside-down (true!).

I teach in Thailand all year and summer in Canada; in both places Blacklisted411 is simply not available so I was delighted to discovered your resurrection during a recent trip to NYC. And I was doubly delighted that you are including so many articles for Mac users. I think we were considered elitest lamers for far too long! (Dontcha just WANT one?)

The police-state is effectively in place everywhere. The goal is to fly under the radar. (I learned this the hard way--cost me two years & I was LUCKY!) If you've been lazy, NOW is the time to teach yourself PGP and how to use anonymous remailers. Don't wait until they're at YOUR door! (Believe me, I'm not at all paranoid but that doesn't mean they're not after me!)

A good example is <www.cryptophone.de>, mentioned in 6:4. Excellent security, except for the fact that you can be listened to by anyone with access to your cell provider, certainly all police and government!

Hushmail, endorsed by Phil Zimmerman, is still tried and true--worth a look. For lighter security, check out the steganography application for Mac OS X called pictEncrypt, sweet.

Personally, I'm still looking for some salvaged TEMPEST shielding. Any of you divers have any for me?

Spike
Routed: Internet

Hi Spike. It's good to hear back from you after all these years. We try to cater to every aspect of the hacking community which is why we've included several MAC related articles over the last few issues. Unfortunately, no MAC articles made it into this issue. It's a shame, but there aren't too many writers who specialize in this area of interest.

Thank you for your comments and suggestions for our readers. If you'd like to send over something for print, go for it. We'll hook you up with a comp sub.

Thanks again for writing.

Blacklisted! 411,

Hey guys...I ran across Volume 6 Issue 4 at Borders and nearly pissed. Great to see there's still rugged individuals who refuse to go corp…

Sorry for the handwritten letter, but...well, you can probably guess (no, I'm not in the pen!), I wanted to throw you some resources that you might want to pass on to your readers if you haven't already…

1. Not all Feds are your enemies. In fact, the absolutely BEST on-line resource for infrastructure, security, signals, and etc.. Is none other than the U.S. Governments OWN auditors! Swing over to the "General Accounting Office" (Now: "Government Unaccountability Office") at GAO.GOV, and browse through the archives. You won't be sorry.

2. For your readers that are hard core coders, fuck Berkley and fuck MIT. If anyone can find a more comprehensive library of algorithms than at the NIST site, have them send me proof and I'll give 'em $5.00 cash. The NIST (national Institution for Standards and Technology) library is priceless (probably only IEEE is remotely close, and that's because both in-breed with each other).

3. Ever wonder where cops and federal agents (and corp. security) shop for non-standard badges and such? (Crdit this one to the GAO)…

   NICE-LAW ENFORCEMENT SUPPLY
   (www.nic-inc.com)

State trooper should patches? UN Letterhead? They sell it all. Although, they stopped selling foreign passports (stamped, no less!) after 9/11.

4. For your readers interested in experimenting with "x-" boxtype, as well as other fun home electronics...they'll need these catalogues:

   a. Contact East (especially the "proto-boards") www.contacteast.com
   b. Jensen Tools (www.jensentools.com)

Jensen sells telecomm linemans hand-sets, ISDN test sets, inductive tone traces, and etc. Why hotwire a network interfect box when for a mere $450.00 you can use what the tech use?

   c. Tech America (www.techam.com) (800-442-7221)

   d. Allied Electronics (www.allied.avnet.com)

If you can't find an IC or component one of the above suppliers, usually they'll tell you where to go for the surplus or discontinued elements.

5. For those that absolutely must solder their own kits…

   Electronics Rainbow Inc.
   (www.rainbowkits.com)

6. A subscription to "Amateur Radio: Communications and Technology" (a CQ pub) and the back issues on disk is another MUST for those who can't resist pissing off the FCC and other feds. (cq-amateur-radio.com) The March '05 issue should still be around ("CQ VHF/UHF" is just as good).

7. For great Linux code, "Linux Journal" has it's back issues available to subscribers.

Anyway, I'll leave it to your discretion what's worth including. Keep up the good work and good luck.

P.S. "High Speed Digital Design" A Handbook of Black Magic" by Howard Johnson & Martin Graham ISBN 0-13-395724-1

ACXScott
Routed: Snail mail

Hey ACXScott. Thanks for the tips. We're well aware of many of the tips, but you can bet that most of this is news to many new readers. As for tools, Contact East and Jensen Tools are the best! In addition to the companies you listed in #4, I would like to mention the following places to round off your selection:

Parts Express
(800)338-0531
http://www.parts-express.com

MCM Electronics
(800)543-4330
http://www.mcmelectronics.com

Jameco Electronics
(800)831-4242
http://www.jameco.com

JDR Microdevices
(800)538-5000
http://www.jdr.com

BG Micro
(800)276-2206
http://www.bgmicro.com

Mouser Electronics
(800)346-6873
http://www.mouser.com

JGL Components
(408)980-1100
http://www.jglcomponents.com

We've done business with all of these sources and fully recommend each and every one of them. Of course, we have many more resources on tap, but these few will cover most hackers needs. If you need something specific and you're having a difficult time locating it, contact us. We'll be glad to help.

Blacklisted! 411,

I think you should give free copies of your magazine to libraries. It is a great way to spread your message and information. I would be willing to pan an extra 10-50 cents an issue to see this happen and it would probably boost sales with the new publicity. Great job on 6:4 and kudos to the people who submitted articles.

Ringo K.
Routed: Snail mail

This is something that Blacklisted! 411 Magazine already does. Given, we're not in every single library in existence, but we exhaust an enormous amount of gratis copies of each issue to various institutions, one of which are many libraries both in state and out of state. If you are the point of contact for a library and you wish to get your free copies, please contact us and provide us with your address and identifying information. We'll be happy to hook you up. Additionally, we give out a free care package to all hacker groups as each new issue comes out. If you can send us a verifiable contact for your hacker group, we'll get you setup.

Blacklisted! 411,

In regards to the info Lint requested in Volume 6 Issue 4: I used to work for the company that manufactured the BART cards, along with cards and tickets from transportation systems all over the world. Unless they have changed in the last five years or so the BART cards are Low Coercivity, 300 Oersted. The 0.25 inch magnetic stripe is applied directly to the card extruded from a slurry of magnetic "ink" that we manufactured ourselves. Our job in production was to apply the stripe in the correct position and to the specified electrical properties which we tested by writing a signal to samples and reading back the return on a digital scope. There were many other parameters to deal with making for a hair pulling experience. These contract jobs are offered by a sealed bidding process, so what's made by one company today may be made by another next time around. The manufacturers of the equipment the tickets are used in design and quote the specifications of the product and it is up to the supplier to deliver cards that meet or exceed the specs. Hope this helps.

Dark Purpose
Routed: Internet

Thanks for the information. I'm sure someone will find this of use.

Blacklisted! 411,

I am a new reader of your magazine. Although I have been in the Hacker community since 1998, I found your mag right next to 2600 and I for the first time in a few years decided that I wanted to try something different. Any ways I saw your call for photos and I was what time of photos you were looking for and even more importantly what type of photos you would compensate for. I have some photography skills and a lot of spare time.

Fluidicslave
Routed: Internet

Hello and thank you for your interest in supporting Blacklisted! 411 Magazine. We're interested in anything at all that has to do with hacking. Pictures of people using computers, utility poles, phone booths, interesting sights, trade shows, hacker meetings, unusual equipment, etc. This answer goes for anyone interested in helping us out with photographs, artwork, articles, letters, etc. Simply get on over to our website at www.blacklisted411.net and go to the contact form. Send us your information there and someone will contact you right away. If you're afraid of direct contact, send it to us through the snail mail. We'll get it.

DoS Attacks: Instigation and Mitigation

During the release of a new software product specialized to track spam, ACME Software Inc noticed that there was not as much traffic as they hoped to receive. During further investigation, they found that they could not view their own website. At that moment, the VP of sales received a call from the company's broker stating that ACME Software Inc stock fell 4 point due to lack of confidence. Several states away, spammers didn't like the idea of lower profit margins do to an easy to install spam blocking software so they thought they would fight back. Earlier that day, they took control of hundreds of compromised computers and used them as DoS zombies to attack ACME Software Inc's Internet servers in a vicious act of cyber assault. During an emergency press conference the next morning, ACME Software Inc's CIO announced his resignation as a result of a several million dollar corporate loss.

Scenarios like the one above happen a more than people think and are more costly than most will admit. Denial of Service (DoS) attacks are designed to deplete the resources of a target computer system in an attempt to take a node off line by crashing or overloading it. Distributed Denial of Service (DDoS) is a DoS attack that is engaged by many different locations. The most common DDoS attacks are instigated through viruses or zombie machines. There are many reasons that DoS attacks are executed, and most of them are out of malicious intent. DoS attacks are almost impossible to prevent if you are singled out as a target. It's difficult to distinguish the difference between a legitimate packet and one used for a DoS attack.

The purpose of this article is to give the reader with basic network knowledge a better understanding of the challenges presented by *Denial of Service* attacks, how they work, and ways to protect systems and networks from them.

Instigation

Spoofing – Falsifying an Internet address (known as spoofing) is the method an attacker uses to fake an IP address. This is used to reroute traffic to a target network node or used to deceive a server into identifying the attacker as a legitimate node. When most of us think of this approach of hacking, we think of someone in another city essentially becoming you. The way TCP/IP is designed, the only way a criminal hacker or cracker can take over your Internet identity in this fashion is to blind spoof. This means that the impostor knows exactly what responses to send to a port, but will not get the corresponding response since the traffic is routed to the original system. If the spoofing is designed around a DoS attack, the internal address becomes the victim. Spoofing is used in most of the well-known DoS attacks. Many attackers will start a DoS attack to drop a node from the network so they can take over the IP address of that device. IP Hijacking is the main method used when attacking a secured network or attempting other attacks like the *Man in the Middle* attack.

SYN Flood - Attackers send a series of SYN requests to a target (victim). The target sends a SYN ACK in response and waits for an ACK to come back to complete the session set up. Instead of responding with an ACK, the attacker responds with another SYN to open up a new connection. This causes the connection queues and memory buffer to fill up, thereby denying service to legitimate TCP users. At this time, the attacker can hijack the system's IP address if that is the end goal. Spoofing the "source" IP address when sending a SYN flood will not only cover the offender's tracks, but is also a method of attack in itself. SYN Floods are the most commonly used DoS in viruses and are easy to write. See http://www.infosecprofessionals.com/code/synflood.c.txt

Smurf Attack - Smurf and Fraggle attacks are the easiest to prevent. A perpetrator sends a large number of ICMP echo (ping) traffic at IP broadcast addresses, using a fake source address. The "source" or spoofed address will be flooded with simultaneous replies (See CERT Advisory: CA-1998-01). This can be prevented by simply blocking broadcast traffic from remote network sources using access control lists.

Fraggle Attack - This types of attack is the same as a Smurf attack except using UDP instead if TCP. By sending UDP echo (ping) traffic to IP broadcast addresses, the systems on the network will all respond to the spoofed address and affect the target system. This is a simple rewrite of the Smurf code. This can be prevented by simply blocking broadcast traffic from remote IP address.

Ping of Death - An attacker sends illegitimate ICMP (ping) packets larger than 65,536 bytes to a system with the intention of crashing it. These attacks have been outdated since the days of NT4 and Win95.

Teardrop - Otherwise known as an IP fragmentation attack, this DoS attack targets systems that are running Windows NT 4.0, Win95, Linux up to 2.0.32. Like the Ping of Death, the Teardrop is no longer effective.

Land - This attack alters the TCP SYN traffic with the source address being the same as the target IP address. This causes an "implosion" of sorts and causes the system to lock up. Most new systems are immune to this type of DoS.

Resource starvation - This method is the same as the name suggests. You simply send enough traffic to the target that the server starts to deny resources to legitimate requests. A simple resource starvation attack can be perpetrated by an army of zombies that open a socket connection on the target server and leave it open until the connection times out. The goal is to open more connections in a faster period of time then the server will release them. A crude example of this DoS attack is to open up a telnet connection on port 80 (telnet target.server.com 80) and then start another session as soon as the first is open. If thousands of systems were to do this at the same time, the attack would not only be impossible to stop, but very effective. Unlike a SYN flood, this traffic is seen as valid since the three-way handshake of SYN-SYN/ACK-ACK has been completed.

Ping flooding - Another type of resource starvation attack, a ping flood causes congestion to occur on the target by sending ICMP echo request.

Mail Bombs - These can be done by sending a large amount of emails to an email server, thus backing up the server and creating a situation to deny legitimate email traffic through.

Rumplestiltskin attack - is an email reconnaissance method that creates an involuntary DoS attack while developing a database of valid mail addresses used in spamming attacks. Many of the new Internet worms are using this to collect targets for spam engines.
DNS DoS - This is another attack that is self explanatory. This Denial of Service attack targets a DNS server by altering the DNS redirection scheme. For example, target.server.com would point to 192.168.1.1, but an attacker alters this data to reflect 192.168.2.1. This would prevent regular traffic from reaching the real server at 192.168.1.1.

Application Attack - These are DoS attacks that involve exploiting an application vulnerability causing the target program to crash or restart the system.

Kazaa and Morpheus have a known flaw that will allow an attacker to consume all available bandwidth without being logged. *See http://www.infosecprofessionals.com/code/kazaa.pl.txt*

Microsoft's IIS 5 SSL also has an easy way to exploit vulnerability. Most exploits like these are easy to find on the Internet and can be copied and pasted as working code. There are thousands of exploits that can be used to DoS a target system/application. *See http://www.infosecprofessionals.com/code/IIS5SSL.c.txt*

Black Angel's Cisco global exploiter has several Cisco router attacks including several Denial of Service attacks that can help you test vulnerabilities in your Cisco IOS.

Viruses, Worms, and Antivirus – Yes, Antivirus. Too many cases where the antivirus configuration is wrong or the wrong edition is installed. This lack of foresight causes an unintentional DDoS attack on the network by taking up valuable CPU resources and bandwidth. Viruses and worms also cause DDoS attacks by the nature of how they spread. Some purposefully attack an individual target after a system has been infected. The Blaster worm that exploits the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135 is a great example of this. The Blaster targeted Microsoft's windows update site by initiating a SYN FLOOD. Because of this, Microsoft decided to no longer resolve the DNS for 'windowsupdate.com'.

DoS attacks are impossible to stop. However, there are things you can do to mitigate potential damages they may cause to your environment. The main thing to remember is that you always need to keep up-to-date on the newest threats.

Mitigation

Antivirus software – Installing antivirus software with the latest virus definitions can help prevent a system from becoming a DoS zombie. Now, more then ever, this is an important feature that you must have. With lawsuits so prevalent, not having the proper protection can leave you open for downstream liability.

Software updates - Keep your software up to date at all times. This includes antivirus, email clients, and network servers. You also need to keep all network Operating Systems installed with the latest security patches. Microsoft has done a great job with making these patches available for their Windows distributions. Linux has been said to be more secure, but the patches are less easy to come by. However, SELinux (the NSA's addition to the Linux community) is a great addition to ay Fedora compile. This will give Mandatory Access Control (MAC) capabilities to the Linux community.

Network protection - Using a combination of firewalls and Intrusion Detection Systems (IDS) can cut down on suspicious traffic and can make the difference between logged annoyance and your job. Firewalls should be set to deny all traffic that is not specifically designed to pass through. Integrating IDS will warn you when strange traffic is present on your network. This will assist you in finding and stopping attacks.

Security is not as mystical as people believe. DoS attacks come in many different types and can be devastating if you don't take the proper precautions. Keep up to date and take steps to secure network nodes. Keeping security in mind can minimize damages, downtime, and save your career.

Resources

Security Resources

Black Angels: http://www.blackangels.it/
Cisco: http://www.cisco.com
Microsoft: http://www.microsoft.com/technet/security/current.aspx
Forum of Incident Response and Security Teams: http://www.first.org/
SANS Institute: http://www.sans.org/resources/

cALLEr Id SPooF InG

By The Goldfinger

In this article I will attempt to shine some light on caller ID and ANI spoofing and some of the ways its being done. To be sure there are hackers out there that have a much more in-depth knowledge of the mechanics, but often this technical knowledge is complex, and quite frankly, boring to read. Therefore, I will present it to you, our knowledge-seeking readers in such a way that you won't start drooling as your eyes glaze over in boredom...which is what kind of happened to me while researching this article. j/k

Ok, lets take a look at what caller ID spoofing is in its most simple terms. When spoofing the phone you're calling, it appears you're actually calling from a phone number of your own choosing. In other words, you could pick the number that you want to appear on the recipients phone like pi(3141592653), or some fake movie style number that ends in 5555, then there's the always popular call from Satan (666-666-6666). Whatever you want the number to be, spoof it so. *Spoof it, spoof it good!* *ahem* Sorry, ok, back to spoofing an such. I guess to really understand what's going on here you have to have some background information.

Lets start with ANI. ANI stands for Automatic Number Identification and it's a feature that transmits a directory number or what they call a BTN, or Billing Telephone Number to be obtained automatically. In this case, your number is sent to wherever you are calling to automatically. This feature cannot be blocked, like Caller ID can. ANI can be spoofed though, despite what many telco technicians would say to the contrary. Apparently, spoofing is nothing new, its just becoming more publicized and brought to the layman's attention. We'll come back to this in a minute...but first lets read what the media has to say about all this spoofing stuff.

The New York Times printed a interesting article on Sept 2, 2004 called, "Software Service Aims to Outfox Caller ID". The article was about a California company called Star38, www.star38.com , that is offering a commercial version of this spoofing technology.

For 19.99 a month and as little as 7 cents a minute you can log into their site and type the number you want to call and the number you want to appear on the caller ID screen of the recipient's phone. For an extra fee, you can add a name to that. Bill collectors and their ilk are salivating at the idea. The service will let collection agencies and others avoid breaking laws that prohibit them from using phony phone numbers when they try to collect money. Jason Jepson, founder and CEO of the Star38 service says they will provide them with a legitimate phone number--but one that can't be associated with the actual caller.

"We are providing collection agencies with another option," Jepson says. "Our service will completely document each call, including how long it took, when it was made, and data like that." The service costs $20 per month, plus 7 to 10 cents per minute for phone charges.

Before you get your hopes up about signing up for this service and getting your phreak on, allow me to bust your bubble. First off, its not available to *us*. Its only available to collection agencies, private investigators, and law-enforcement personnel, according to Jepson.

"This is not for public use," he says.

On second thought, that's probably a good thing. Privacy rights advocates wonder how long before angry, disgruntled ex-spouses, stalkers, and fraud artists catch on and use these services to do malicious and nefarious deeds. I wonder as well. Imagine all the havoc you could wreak if you were so inclined? Those are legitimate concerns. "Some people see caller ID as an invasion of their privacy, while others see it as a protection of their privacy," says Robert Atkinson, Director policy research at the Institute for Tele-Information at Columbia University. "Its spy vs. spy." True enough. Just making or receiving a phone call is no simple matter these days. There are definite pro's and con's to this technology. The issue is pretty much divided, with just about everyone weighing in on the issue.

The FCC says there is nothing illegal, per se, in the Star38 system. According to them, the agency's rules require only that telephone companies provide caller ID abilities and the ability to block caller ID. The rules say nothing about add-on services like Star38 provided by commercial companies. Loretta M. Lynch, a member of the California Public Utilities Commission worries that, "People will not trust what their phones tell them. It will spell the end of caller ID as a way for people to protect their privacy." "This is solving a problem that caller ID created," said Mark Rotenberg, executive director of the Electronic Privacy Information Center www.epic.org in Washington. "Most people thought of caller ID as a net privacy loss, but this technology may help customers recapture some privacy." Others say caller ID spoofing is no different and no better or worse than other telecom technology that have allowed people to mask their identities or locations.

For years people have used pay phones to hide their whereabouts, and some companies like Hop-on now sell disposable cell phones that have X amount of minutes and can be discarded afterwards. Btw, those phones are pretty cool and some of them really have a lot of features, plus you can reload minutes if you want, for more info on disposable celly's peep www.hop-on.com Ok, as i was saying, everyone has an opinion on this, so heres my 2 cents.

At first I thought, "oh yea, this is gonna be dope", then when I realized it wasn't gonna be commercially available I was bummed. Then after researching this article and hearing what everyone on both sides of the fence had to say, I've refined my opinion. The technology itself is not bad, its just new technology. How it is used is the issue. After re-framing, I decided that it's a good thing that's its not available to everyone. While you or I might like to use it to mess with our friends and family, some others might be using it to bamboozle people or set them up to be jacked or worse. So I thought it was a good thing to limit its availability. Other than that, I see nothing inherently wrong with it.

As for Star38, when the article dropped, there was quite a bit of publicity and many more articles popped up about spoofing and that company. There was even an article I can't find now that said the CEO changed his mind, due to numerous threats he had received, and was going to sell the company. Something about hiring bodyguards and hiding out in his gated community or something along those lines, don't quote me on that, but after a quick visit to the website, it looks like they are up and running and open for business. It also appears they canned the whole idea for making the service available to collection agencies (ha ha) and PI's. Its only available now *strictly* to law enforcement. That was probably the best bet and a quick way to end all the hassles and drama, at least if you were in Jepsons shoes. *So what's the future of caller ID you ask?*

(Heres an excerpt right off their site.)

What about the future of caller ID? The future of caller ID is safe. The Star38 service is for agencies that are looking for people that have broken the law. The average person does not fall into this category, hence they can still trust their caller ID. Unless you've got something to hide from, there's nothing to worry about. It is important to note, as stated above - that our service is not for consumers, it is specialized for law enforcement agencies.

Now the Man is the only one that has access to caller ID spoofing...well, at least if the Man goes thru Star38 because he doesn't have any hacker friends.

Now lets get back to the in's and out's of spoofing and whatnot. An inquiring fellow by the name of Eric wondered if this particular spoofing system will modify your ANI? Most services for 800's and 911 (E911) capture your info using ANI, not caller ID and ANI is harder to spoof.

Word on the street is ANI info is normally sent by the originating equipment. Caller ID is only accurate when you have a single line to the switch, basically just residential and small commercial customers. Any business with a T-1 or or ISDN connection through their PBX to the CO (i.e. any business with more than 12 lines or so, depending on tariff) can generate any caller ID string they want. Thanks to some guy that goes by the chick magnet handle DV Henkel-Wallace for that info.

Now, lets get down to what you guys really wanna know about.

How to spoof caller ID! We will cover 2 methods, Orangeboxing, and Social Engineering your way into it. Both of these methods are courtesy of a hacker d00d named Lucky225. This kid seems to know his sh*t so I'm just gonna grip his tactics and present them to youz guys.

Go on and test them out, cuz I just don't have the dam time. I'm rappin, I'm kidnappin people out here in Detroit, and I'm writing for this illustrious magazine so as you can see I have a full plate. Go on and test these methods, and if they don't work, complain to Lucky225, *not me!*

J/k. Lets start with Orangeboxing... (excerpts from his site)

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

And here's the Social Engineering part…

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

*placed from and to and because you used a 710 number there were undetermined rates. I was testing to see if the 710 trick also worked with a canadian phone company called Telus. After testing it out my friend in canada dialed *69 and it read back the 710 number I gave the operator, this is how I discovered Caller ID spoofing was possible through Telus and I began to come up with a social engineer to get them to place a call for me without selecting a billing method. I now know that it is also possible to spoof ANI through Telus. Telus' toll-free "dial-around" is 800-646-0000, by simply calling this number with an ANI-fail you can give the operator any number as where you are calling from. As of January 2003, Telus can now place calls to many toll free numbers and the CPN will show up as whatever number you say you're calling from. So by simply causing an ANI-fail to Telus dial-around service you can spoof Caller ID to anyone you want to call, not only that if the person you are calling is in the same area as the number you are spoofing, the NAME and number shows up on the caller ID display. To cause an ANI fail to Telus all you have to do is op-divert to 800-646-0000 or dial 10-10-288-0 and touch tone 800-646-0000 when AT&T comes on the line. You can social engineer the Telus operator to place "test calls" for you which is a free call with no billing, you simply tell the Telus operator at the beginning of the call that you are a "Telus technician" calling from [number to spoof] and need her to place a "Test call" to [number to call]. The social engineer pretext looks like this: You pick up the phone, at dialtone 10102880 AT&T Automated Operator: "AT&T, to place a call" Touch tone 800-646-0000 AT&T Automated Operator: "Thank you for using AT&T" <RING> Telus: This is the Telus operator, Lisa speaking. (or, This is the telus operator, what number are you calling from?) You: Hi Lisa, This is the Telus technician, you should see an ANI failure on your screen, I'm calling from [number to spoof] I need you to place a test call to [number to call] Telus: Thank you from Telus What just happened was AT&T sent an ANI fail to Telus, you told the operator to key in your new number calling from, Telus then places the call and uses the number you gave as both ANI and CALLER ID! NOTE about spoofing ANI to Toll freee numbers: Not all US toll free numbers are accessable from Canadian trunks, so even though you are spoofing a US number the call will not be able to be routed through Telus. Of course, the social engineer will probably become ineffective soon, though I've demonstrated it at H2K2 in July 2002 and It's now 2003 and is still working. The spoofed caller ID also shows up on collect calls(though I think you can only call people in Canada collect with this service), third party billing (would you accept a third party bill call if the caller ID said your girlfriends number and the op said she was the one placing the call? :)), and calling card calls, so you could even legitamatily spoof Caller ID if you had a Telus calling card, however the rates are pretty expensive, though you can get one if you have Telus as your local phone company or if you live outside Canada you can pay with a credit card (you need a Canada billing address though!), call 1-800-308-2222 to order one."*

If I didn't mention before, *and I did*, Lucky225, who can be found at his cool ass site www.verizonfears.com, is the hacker that provided this information, and you can even go to his site and find out a lot more about this subject. To spoof or not to spoof?... that is the question…

The answer can be found within. Look to your phone, is it calling you?

The Goldfinger is also known as Detroits only Octopus-wearing rapper; Mr.Scrillion aka Adam Thick, Mastermind behind Extremekidnapping. The Goldfinger has more than a decade of underground knowledge and experience under his belt, a former social engineering hacker, and when not Rapping & Kidnapping, he is scouring the underground, the black market, keeping his ear to the streets for the rawest and most up to date insider information available.

Visit www.scrillion.com & www.extremekidnapping.com
Coming Soon! www.lapdanceolympics.com
Holla at him > goldfinger@voyager.net

USING LIMITED RESOURCES

Hacking without a real computer, My introduction into the hacker phreaker community.

By BrainPhreak

The Beginning:

In about 1986 I got my first Commodore 64 computer, my uncle who I never really knew, found out I had a PC and I guess he must have been into pirating because he sent me two boxes of games and printing applications. There must have been 200 5" floppies.. with tons of games and apps on each.

Remember "Jumpman", "Marble Madness", "Summer Games", "Print Shop"

I know Commodore came out much earlier.. but I was pretty damn poor.

I found the manuals and read them all, I have always been into getting the most out of everything I own. Didn't get new toys often so must take advantage... Soon I learned that I could make own games or programs. It had examples etc. I had never even heard of programming, I was only 7-8, but I knew commands..

load "*" ,8,1

I saw that this programming was just a series of commands at that very same prompt. I spent HOURS programming every print statement known to man for a demo program listed. I finally finished it and then it RAN!. "It worked! Amazing! But that's it?!! What the #$@! It took all day! I only saw a ball bounce off the edges of my screen." I never programmed again for years.. I only played games and tried my best to get the best quality prints, impossible with the classic printer I had.. Later on it broke down and I was without a computer, but I had things like Nintendo, Sega etc. now, so no big deal.

YEARS LATER:

The Sega Genesis came out, I was the last to get it since I had to save every penny from school lunches. BUT it was the best when I finally got it!!

I was introduced to hardware upgrades and expansion! I wanted to get the most out of the money I spent, so I didn't buy the super Nintendo, it was WAAY expensive. The Sega CD came out! It was MUCH lower than any core system, just attach it to the existing sega genesis, and can even play CD's! I didn't even have a CD player.. and video CD'S! Never even heard of them! No console I ever seen took CD's at that point. Then soon came the "Sega channel"! 30 games a month at your fingertips! Subscribed through the cable system, kind of like the internet.

Sega is really always ahead of their time if you ask me... anyways..

Later I got the 32x, and I was playing a 32bit system "with" CDROM before the Playstation was even out! (which is also 32bit)

When the Saturn was released I lined up, I had been saving every dollar. Unfortunately it advertised a 32 system.. I already had that.. So I read about all the options and in a magazine it said it was actually two 32 bit processors making it "virtual 64". I also read that the new system N64 was really only two 32bit processors also! So this in essence would be better than the first 64bit N64 system! It has a CDROM! And much cheaper!

That shows Sega's bad advertising... they could have said 64bit and got more sales like N64.

Then the magic happened.. I learned that you could go online with a Sega Saturn with a new product called the "Netlink". The net was a mysterious place I had heard about only on TV in countless commercials. "www dot what?" When I had my original Commodore they started advertising connecting online to get games! I tried but would only get to a form requiring a credit card. I just gave up on "quantum link", my mom didn't even have a credit card.. People also had told me that on computers you can "download" games to play. FREE GAMES! No need to buy all the expensive console games anymore!

I never seen a modern computer online. I heard you can obtain pictures of anything and even talk to people from anywhere! So being an artist and a huge fan of games, I HAD to get the netlink to have more inspiration, things to do and draw. No need for the HUGELY expensive PC that I could never afford. I also read it was like a library at your home. Look up anything! I HAD to get online...

MY AWAKENING:

I finally got the netlink and went online where I could find all the info I wanted, needed, or even stuff I never knew existed! Like hack info... I looked up everything.. I mean EVERYTHING! I was the true definition of a "web surfer".

I soon learned I could not save ANYTHING, I was at the mercy of other websites, when one was erased or temporarily down my bookmarks to my favorite images were now dead... I couldn't see the art anymore and only hoped I could find it searching again. There were no games I could download unless I had windows... no java even. My dreams of replacing the PC with the Sega was not exactly what I expected..

I started going to online chatrooms. Sega didn't have IRC, so these were html web chatrooms... I was amazed you can communicate with people in other countries without long distance charges! I noticed some of the more popular people were writing in color at times, it was like a secret to everyone. I finally convinced one of them to teach me how, he showed me my first HTML tags...

 Hey Guy!

"WOW! My text is red! Amazing!"

Later I saw him use a frame around his text. This I found out was HTML tables. Each time he did something I always asked him and begged to learn how. Finally he told me about www.htmlgoodies.com where I can learn ALL about web pages and HTML, the web and how it works etc. It was GREAT! I learned I could make my OWN web page. I didn't have to worry about servers going down. I can finally store my own files! I can create my own online artistic place of expression AND "ANYONE" can get to it from "ANYWHERE" in the world! "Ill make the Ozzy Osbourne, M.C. Escher art, HTML tutorial, blah blah blah blah."

webpage..

The best page on the net...

And best of all it wasn't like the old print statements I learned when I was younger.. Instant embedded images, links to cool places and anything I want. Instant gratification. I already saw what HTML can do in the chatroom, now I learned how powerful it was for a webpage.

The guy on the web was using Linux, I didn't understand what that was anyways... I just finally recently saw windows at school. He told me where I was dialing from etc. by using traceroute, whois, nslookup etc. I asked how he did all his tricks each time. He told me since he knew I couldn't do them anyways, I had no way to do these cool things like ping, traceroute etc. not with HTML. Not with a Sega.. I was now limited... and of course HAD to find a way....

FINDING MY WAY:

I read all about ping and Linux/Unix and the Unix shell. But I couldn't get a shell on a Sega... I was basically just imagining having a shell... having a computer. just writing down notes.. Then, as I was learning about ping, traceroute etc. The win-nuke bug/exploit came out. (bugtraq id 2010)

As most of you know, when Win-Nuke came out everyone and their mother was downloading nukers and knocking people offline.. It was the "thing" to do in chatrooms when someone pissed you off, or to show power. Power trippin' script kiddies..

I however couldn't download anything like a program... maybe make webpages but that's it. No interactive WINNUKE program. I couldn't run ANY program...

I did however learn I was immune to this attack though! Winnuke wont kill a Sega! This was great! I was invincible!

I was fascinated that you can knock a user offline using a simple script, a simple flaw.

I also noticed a few times the entire chatroom would go blank. Or all text would be red. From programming my web page I knew this was due to someone not closing their HTML tags. I had of course made this mistake more than once. I was interested to see you could manipulate the entire chatroom in this way. One flaw can mess up the whole room. I was really getting to know HTML by then, there was no cut and paste on Sega so I knew it all by heart. Fluent.

I decided to try to mess with the chatroom one day by entering a </body></html> tag. This in turn, stopped the interpreter, and displayed the rest of the page in plain text. HTML tags.

I saw the tags:

<meta http-equiv=refresh content="15; url=chatroom.cgi">

I read about these tags and realized it could be used for redirection. I decided to try these tags in the chatroom later.

<meta http-equiv=refresh content="2; url=webpage.com/mypartofsomeoneelsesserver">

IT WORKED! I just forced every chat user to my webpage! (this pissed a few people off)

I could now knock people off the chatroom, and they couldn't do anything to me!

Unfortunately this effected EVERYONE in the chatroom.. I needed the power of Win-Nuke to get a specific person and not my friends.. also this code effected me as a chatter too! I was now on a mission to learn everything about these browser flaws. About nukers..

While learning about the details of winnuke I found a Perl script that would "test" the vulnerability if you type in your i.p. address. Lightning struck! I could now nuke others by typing in their I.P.! I tried it and of course, knocked the victim offline! And I couldn't even be traced, the server did it! and still no-one can nuke "me"!

I really didn't have many people to nuke, but it was a rush finding out how and feeling invincible. (I did find exploits for the Sega browser, but I was the only one who knew). People thought I was the hacker guy now, and I was on a Sega!! Even the guy who taught me couldn't touch me. Unfortunately the winnuke power was short lived as the webpage was taken down due to abuse. I had to learn how to get it back! There were no more webpages with nukers...

I obtained and read the installation of the winnuke script. I was able to install this on my webhosts server and have the nuke ability back! Even better, I now knew about the power of CGI and PERL on someone else's server!

I quickly made the ultimate chat interface. Using frames, I brought the chatroom into my own version of the room. I made forms next to the regular text box that let me type in the i.p., I also added similar Perl scripts for ping, finger, nslookup, whois, etc. as I researched and found these scripts. I also made forms to type in "red" etc. so I didn't need to type the HTML tags anymore (again no cut and paste, so it was a pain).

I found web tools that will read the source of an HTML page for you, upload files from one server to another via ftp, and many other tools all in Perl. All things a regular PC user would take for granted, but I couldn't do. Some things normal windows users don't even have by default (such as traceroute, whois, finger etc.)

I was able now to be perfectly safe on a Sega, no-one could crash me, and I could tell where these people lived, knock them offline etc. through various Perl utilities I could do anything I wanted!

After learning more about vulnerabilities like winnuke, I primarily researched all Perl, CGI, and browser flaws. I ended up finding a flaw in my providers server side includes which allowed me to submit any non-interactive command and get the results displayed..

<!--#exec cmd="cat /etc/passwd">

I let them know and told them how to fix it. They were so nice to me that they erased my entire webpage without notice, since it hosted "hack tools"..... ;o(

A warning to others, don't tell the admin unless you know them, or do it anonymously

Months of work, tutorials I wrote on HTML etc. Perl scripts I customized and used daily..all gone.. I had no backup.. no hard-drive so I couldn't...

Im sure some of you know how this feels when you are actually sick because you lost weeks/months of work... a horrible memory, and wasnt the only time this occurred..

I was taking electronic engineering at this time and started getting REALLY into phreaking, I read several text files online and was amazed.. it didn't require a computer, and I was still mad about the data loss incident so I didn't even have a webpage anymore. I learned EVERYTHING about the phone systems and the phreaks culture. It was the greatest info I ever read! Blue boxing.. captain crunch.. gold boxes, hacking vmb's, answering machines etc.

God bless the PLA for introducing me.

I frequented the Defcon voice bridge (DT!) and built all the boxes I could. In fact just for the record the REDBOX "STILL" works here in San Diego, CA. at ALOT of "Pac-Bell" payphones.. sad but true. (last tested probably mid 2002, but IM sure they are still around). I ended up knowing all the phreaks at the time and was on voice conferences (other than Defcon voicebridge) every night learning more about hacking and phreaking. I was never home to chat anymore, only to research more before leaving on a mission of dumpster diving, beige boxing, scanning for PBX's etc..

I learned about the PHF exploit in CGI, the CGI-TEST exploit, all the classics CGI/Perl string and buffer exploits from some other hackers on the bridge.

At night I learned all about phreaking, I was obsessed with the two subjects day and night. Hack in the day, phreak in the night. I would even be on the payphone during some of my classes at school, missing the entire class if something cool was happening on the hacker/phreaker conference/bridge.

Later on the TIGER-GAME.COM came out and was a touchscreen handheld (http://www.vidgame.net/TIGER/GC.html) It was able to go online and had no browser, it used LYNX and a shell. AWESOME! I could finally get me a unix shell! I bought one as soon as I could, and it was cheap!

As you should know once I had the shell I was unstoppable, phreaking became history after a few phreaks got busted for some huge AOL credit card phish scams. I worried about my activities since I was now 18. On to programming and hacking again full time! My first PC came soon after (a 486) I earned from doing a webpage for a schoolmate who had a ton of extra parts... I of course installed Linux after ALOT of trial and error. About a year later I got some money back from a school grant which I used to buy my first REAL PC of my own. I ran windows for the first time since it came with the PC and I had the 486 Linux box. I of course mastered windows in like 5 minutes.

...well maybe longer but compared to Linux about 5 minutes... I'm still learning Linux of course!

THE POINT OF THIS ARTICLE:

Philosophically: This is just a little story of one mans introduction to the hacking and phreaking society.

Purpose: I have seen MANY people who turn away from hacking, music, etc. because they don't have the right "equipment". This is not true... people hacked with a whistle taken from a captain crunch box... People have played music with rocks and sticks.. the only limit is the imagination. Many newbies think this is all history and the days of innovative hacks, hardware hacks, phreaking in general are history. This couldn't be farther from the truth, now there is even more equipment than ever! I've even hacked more than on kiosk!

Where did all the hardware hackers go? A new Phreak box is almost unheard of! Be inspired and don't be afraid to hack anything! *of course don't do anything illegal*

Technically: You can use ANYTHING to hack. If you use something like a webtv, a Sega, a Playstation, a cell phone or whatever! You still can have the power of a full PC, even Unix!

Utilize what IS available.

Servers are ALWAYS available.

You can run your own programs, through online servers (CGI/PERL/JAVA).

Most game consoles and newer devices like cell phones are all coming with net access.

Tracing these hackers will be even harder now days. Most variables that a browser sends are not sent by these systems, and they are often much more stable than windows online due to less vulnerabilities. They cannot get virus's (YET), and can simply be reset to go instantly back to default and be back online in a few seconds.

There are many advantages... if they are traced, how many people will believe the root of the hack lies back to this kid with a Sega Dreamcast and no PC? Also the trace of I.P. from these hacks/attacks will most originate from the server not the user. Therefore anyone could have executed it if its a public script.

There's a great script that you can use called "commander.pl" which is a command prompt in Perl. It simply executes any command you give it in the unix shell and displays the output on the web. This script actually works on many servers. I have successfully installed it on hypermart.net in the past and was able to look at any users files on the system since they had the same permissions (except root owned files).

Although I couldn't get root access, it allowed me to look at the .htaccess and .htpasswd files on each persons stats directories. As you know the passwd on the stats directory is generally also the ftp passwd for uploading files. Very dangerous.

The capabilities of the commander.pl script and PERL in general are HUGE!

If your ever stuck somewhere, or are unfortunate with no computer, but only have a generic web device with no storage, and preventing you from running your own apps. Find yourself a server with SSI, CGI-BIN, or Perl capabilities. You don't need a real PC to do what you need on the web.

All this could be done on a pre-paid cell phone and be untraceable, or public library etc. Any PC with limited resources, or access. I think we will be seeing more "hacks" like this in the future now that even your hamburger comes with fries and an internet connection. Lets not even think about this paired with wireless access...

WHERE I AM NOW:

Now I have my BA in electronics engineering, and know MANY languages, have written MANY complex programs in every language from EXPECT, TCL/TK, C++, PYTHON, to PERL/CGI and even robotics in ASM (68HC11 etc.). Its amazing how one little thing like a person writing in colored text in a chatroom can help spark your curiosity and turn you into a "hacker". I also now work for one of the biggest telco providers in the world. Supplying high availability unix platforms on sparc and x86 architecture to every major Telco company in the world. From Alcatel and Cisco, to Tmobile, Spatial Wireless, and Ericsson, and I'm loving the new wireless age!

Thank you Al Gore for the internet! MWAHAHA!

And thank you Blacklisted! 411 for helping spread the wealth of information that is available!

Finally, thanks to the support of the hacker community and open source software I still thirst for the knowledge and writing the latest "sploit".

BLACKLISTED! 411 WANTS YOUR INPUT

We want to hear from our readers and get some input on every topic from the articles we print to the content on our website. If you have any ideas, comments, complaints or suggestions, the best way to get something done about it is to contact us and let us know what you're thinking. We are a magazine written for the hacker community. We want to have the best possible magazine with the most fresh ideas and subject matter. This is your chance to help out and get something done. Don't fall prey to the thought, "what I think won't matter" or "let someone else do it." You can make a difference!

We want to hear from hackers, event coordinators, group leaders, graphic artists, writers, creative assistants, magazine editors, system administrators, forum moderators, webmasters, photographers, electronic hobbyists, design engineers, technical writers, field technicians and anyone else who is interested in the hacker community in any way. Here's how to contact us:

Blacklisted! 411 Magazine
P.O. Box 2506, Cypress, CA 90630

Or make contact with us through our website:

WWW.BLACKLISTED411.NET

BLACKLISTED! 411 MAGAZINE

Is proud to announce that our website is now officially open for business.

That's right! It's ONLINE! The website is fully functional, allowing visitors the opportunity of reading about our history and FAQ, learning where they can find our magazine and finding out how they can participate. Further, we have an announcement section where we will list any recent news as well as a guestbook which will give everyone the chance to leave their own comments.

In addition, we have a FORUMS section for everyone to join in and discuss their favorite hacking topics.

Last but not least, our online store is ready and awaiting your order. We have available to our readers both back issues as well as subscriptions.

Please visit our website:

WWW.BLACKLISTED411.NET

Started in October 1983 as a disk based hacker underground magazine (e-zine), Blacklisted! 411 is one of the oldest of the hacker quarterlies available today. Blacklisted! 411 has a mix of the cheerfully basic for the "newbies" who have recently joined the ranks of the hacking community as well as the technically advanced for the experienced hacker. Our effort to appeal to all levels of hackers has not gone unnoticed. In fact, we've been branded "newbie friendly" by several sources which is generally an accomplishment of the impossible kind. Our official Blacklisted! 411 website is intended to complement our print magazine and provide the hacker community with an additional resource. Get online, look around, and join us as we continue to serve the hacker and underground community.

Electronic Surveillance: Introduction by example

Part Three: Intermediate Wireless Networking

A series of articles written exclusively for Blacklisted! 411

By M L Shannon

From Part Two, you now know the basics of wireless networking.

In Part Three we will begin with using Network Stumbler, reviews of several wireless cards and then a review of CommView, one of the best wireless sniffers available at any price.

Then, two real life stories of my own experiences.

Intruder Alert is about how someone was able to access my wireless network, how I discovered their presence and how I handled the situation

A Hacking We Will Go. Also true, how a hacker friend and I explore the technique of getting access to a wireless network, and how we could have easily taken complete control of at least one AP. Could have but did not. Discussed are the methodology and applications used closing with some things you can do to make your wireless network extremely difficult to hack.

Hardware recommendations for wireless networking:

A portable/notebook/laptop with a Pentium II processor. A pentium III is better but a P II with 512 Mb of RAM will probably outperform a P III with only 128 Mb and will cost less money. In either case, get 128 as an absolute minimum. Also, some wireless PCMCIA cards won't work with Pentium I.

The obvious reason for a laptop is portability, but another consideration is weight. My Compaq Presario 2700 with tote bag, accessories like extra battery, cards, antenna, cables, and GPS receiver, weighs way to much to carry around.

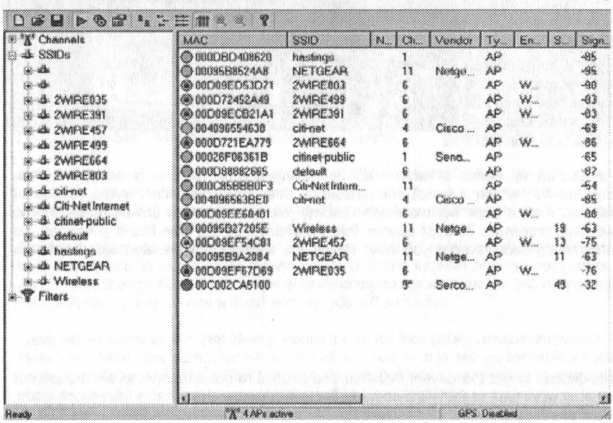
Desktop computers will work, of course, but for wireless cards you can either use PCI which is not recommended, or get an adapter with which you can use PCMCIA cards.

NETWORK STUMBLER

Net Stumbler is an industry standard and is absolutely indispensible for anyone who wants to do more than read the sports page at Betty's Bytes and Bagels. The first step is to go to http://www.netstumbler.com/ and download NetStumbler. It runs on Win 98 and 2000 and other versions and Installation is painless. Make an icon to get it started if you like, reboot your computer and start your card drivers (in case they don't start automatically) and then NetStumbler.

When it starts you will see a screen like this, except that you probably will not see as many listings. As you can see in the screenshot below, it lists every AP as well as wireless cards in Ad Hoc mode that can be detected with your PC card and antenna combination.

On the left is a list of signals which when clicked on will show a graph of signal strength. The colored circles also indicate signal strength. Green is strong so you will probably be able to connect. Red is very weak and yellow is somewhere in between. But these colors are not absolute; you might connect on red but not on green. As the program scans the dots will change to gray except for a very strong or weak signal in which case the color does not change that often. Only a very strong signal will have a green dot that does not change.



Next is hexadecimal code (A system of counting based on 16 instead of 10) This is the 'MAC' meaning Media Access Control, which is a sort of serial number burned permanently into network cards, wireless or wired, as well as APs and other networking devices. After that is SSID, Station Set Identification, which is an arbitrary name you can give an AP. It is also optional; An SSID is not required for the AP to function.

Following that is the Name category

which more than likely will be blank except for Internet Café type places. It, too, is arbitrary so you can name it anything up to fix characters. 'My AP'. My Network'. Joe and Linda's', whatever. The Ch. refers, of course, to the channel that the AP is using. In the US we have 11 B channels and others for A and G. Other countries vary.

The Vendor is the manufacturer of the AP and lastly, for now, is the notation; AP or Peer-to-Peer. If you see this it means you are detecting someone's actual card, which can mean that whoever owns it is using their card - and probably a directional antenna - to look for APs in their area. Your area. Otherwise it is probably an AP but could be a wireless router or switch. There may be a large number of APs appearing on your screen. There may be none. So you can move the antenna around to see if you can find one or more. Now, once you have found an AP, look at the pane on the left. Channels, SSIDs, Filters.

Click the box to the left of SSIDs and a list of them will open. Click the '-' box and it opens, showing the SSID. If there is a little padlock in the circle to the left it means the AP is using WEP; it is encrypted. Find an SSID without the padlock and click the MAC and the main screen changes to a graph showing how strong the signal is. The higher the colored bars - red, purple, green, are, the stronger it is. Now it is beyond this chapter to get into a detailed discussion of signal strength. What matters is what you are able to detect. Later, we will get into making a connection and being able to use one or more of the APs you see in NetStumbler and through them, get Internet access. And, of course, by understanding all this, you will be better able to learn how to make your own AP, if you decide to set one up, secure against others who try to use it for their Internet access.

On Being Detected
At this point you may wonder- if I am using Network Stumbler, can the APs that I see, see me? Do they know - can they know - that I am monitoring them? The answer is not a simple Yes or No. Technically, yes it is possible. NetStumbler sends out a signal with some text within it (The Beacon) that can be detected if someone is looking for it. Normally, the owner of an AP that is for their personal use or perhaps a small business where they don't have an expert security consultant available, then this is very unlikely.

Suggested Reading
There is a FAQ at the Net Stumbler site that explains in detail all that you see, which please read. While it is true that the SSIDs that have a green dot- indicating a strong signal, the SIGN column on the right which is a measurement of signal strength, and the 'S' column which is the SNR or Signal to Noise Ratio are also important to understand. You may see a very strong signal but if there is a great deal of noise present, you may not have very good reception- you might not capture intact packets of data. The lower the SIGN the better and the higher the 'S' the better.

Generally speaking, if the SIGN is in the 60s or 70s you should be able to monitor, capture data from that AP. The 80s are iffy and anything in the 90s will probably not be captured at all. It depends on the card and the software that drives it. CommView, which is reviewed here, will detect weak signals, but if below a certain level, will not capture packets. The Senao card is a little more sensitive than the Orinoco and once again, the antenna is important.

Something else, for future reference: The numbers you see - SIGN and S are not necessarily the same as you will see in other sniffer applications. CommView, for example. We'll see that when we get into the review. Stumbler, again, is one of the most important applications you can have for exploring and learning about wireless networking, but unfortunately, it does not work with all wireless PC cards. Most but not all. I have tested it with Senao, Proxim, Orinoco Gold and LinkSys WPC55AG. It does not work with the LinkSys PCI WMP11.

WIRELESS CARDS REVIEWED

- Classic Orinoco Gold. (B)
- New Proxim card. (B)
- LinkSys WUSB 802.11b Adapter (B)
- LinkSys WPC-11 (B)
- LinkSys WMP-11 (B)
- LinkSys WPC55AG (A B & G)
- Senao (B)

Classic Orinoco Gold.
It is no longer being made and so is becoming more difficult to get. If you can find one, snatch it up. This is an excellent 802.11b card. And, it has an external antenna connection jack, the Allner 31-401A. Orinoco uses the Hermes chipset

Proxim 8420-WD.
A new card, from Proxim or Orinoco or Lucent or Agere or whomever is making it now. Being a new card, it is understandable that there are some programs with which it is not compatable. It does not work with the old version of NetStumbler so you need the new 0.4 release. And, it does not work with CommView, although new drivers may become available. It does work with some other wireless programs. And, of course, this will change by the time this is published, so check with the card manufacturer or software producer before you buy. Uses the Hermes chipset and same antenna connector as Classic Orinoco

LinkSys WUSB 802.11b Adapter
Don't waste your money.

LinkSys WPC-11 card
This is, in my opinion, another loser. It was difficult to get the drivers installed and difficult to get it to work at all. It does not have an external antenna connection, so it may work well at Betty's Bytes and Bagels but other than that, it isn't much good. Some versions use the Prism chipset. Others use RealTek

The WMP11, also from LinkSys surprised me in how well it works, not withstanding that it was, is, a little tricky to get working. When you reboot, sometimes you get an error message stating that some of the needed files were not installed. So, you try to reinstall it and you get another error message stating that the files are already installed. If this happens, all you can do is use the Program Uninstall in Control Panel, then reinstall from scratch.

Now, as you can read elsewhere, I was able to associate, log on to, an AP and actually have Internet access, using only the attached antenna, after I turned the box around to face the open window.

This card uses the Prism 2.5 chipset and the antenna is the standard Reverse SMA, same as the Siemens and other brand routers.

LinkSys WPC55AG (A B & G)
This is a nice card. It started working automatically without installing the drivers, using those that Windows already installed. I traded some stuff for the card which didn't have the installation CD so for a while I just let it run as it was. Later I downloaded the drivers, and installation was painless. Very nice. I like this card as it captures all three bands. I used it in the field trip as described in that chapter, and the sensitivity was quite good. I definitely recommend it, unless you want and can find a similar (A,B,G) card with an external antenna connection.

Before you install the drivers for any PC card, please read the documentation that came with it. There exists the possibility that the application can try to 'burn' or 'flash' the chipset in the card which may not necessarily be a good idea. And it is even remotely possible, though very unlikely, that this could cause permanent damage to the computer.

Senao
This is, in the opinion of many users, myself included, the best overall B card available. The sensitivity is better, the power output higher, 200 mw compared to 30 or so for other cards, and which can be adjusted, and is easily put in "Stealth" RMM mode. CommView, for example does this.

Installing the Senao is easy if you have the factory installation CD. If you do not, you will need to download the drivers and burn them to a CD as trying to run them from the hard disk drive may not work very well. I had difficulty with this as I bought a used card without the CD.

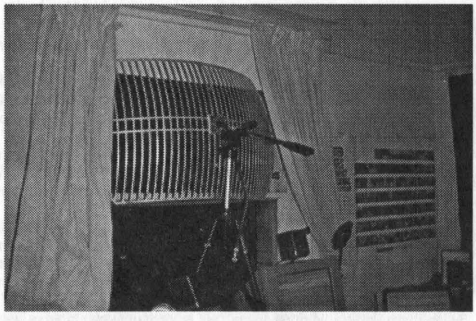
Also, the Senao card works with Knoppix and Auditor; it took off as soon as I started them. Neither the Proxim or the LinkSys WPC55AG did, but it may be possible to get the right drivers- I have not done so as of this writing. Senao has a new A,B,G card but without the external antenna jack. Haven't tried it yet. Senao uses the Prism chipset and MMCX antenna connector

Another card I haven't personally tried but was used in an experiment in the War Driving chapters is made by SMC, and according to the person I was working with, it is an excellent card. Perhaps as good as the Senao, and has external antenna connector. Model is SMC-2532w-b. This card uses the Prism chipset and RP-MMC antenna connector.

There are many other cards available, and some details are on the Seattle Wireless site, http://www.seattlewireless.net although it appears not to have been updated recently. While there is some Windows information, this site is oriented more towards Linux and BSD. A good place to go if you decide to run the Auditor self-booting Linux CD.

HACKING

With what you already know about computers in general and what you have read so far, you should have a good understanding of wireless networking. And if you have obtained and learned to use some of the programs reviewed here included the Auditor self-booting Linux CD, or, the 'Frisbee' Free BSD disk you know how to search for wireless APs and connect to them (associate) so that you can use them to get a free Internet connection. Just keep in mind that while it may not be unlawful to detect APs, it is against the law to connect and use them unless they are known to be free to the public.

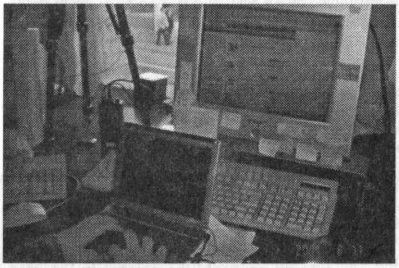


It is also, sometimes, possible to take control of the network. To demonstrate this, a friend from IRC, an Internet Relay Chat channel #SF2600 came over. He set up his portable computer, a Sharp model that runs Free BSD, and an SMC card connected to the big antenna.

Incidentally it was interesting to find out that with this combination, he was able to detect the same SSIDs as I did which allayed my fears that there were many wireless APs that I could not pick up. After a careful scan with Evil turning the antenna around 360 degrees and making a log of what is out there, it was time to get to the business of serious hacking.

For a target, we started with my AP. First, it was detected using a sniffer and from the log file, details were obtained. Evil then tried to connect- to associate to get access to both the Internet and the computers on my small network. He was unable to do so, even though I use DHCP, I programmed my router to allow access only to my own machines.
This was not by any means a dead end, as you will see later.

Next, we selected an AP that clearly stated it was for free public access. However, I will not identify it other than what you will read here. Now, this particular AP is part of a network- it is set up for multiple users, and so uses a router and that router uses DHCP (Dynamic Host Configuration Protocol) which I will explain in more detail than elsewhere in this work, and will repeat some things I have mentioned that will put it all together.



Every computer on the Internet has to have its own unique identifier just as do telephones, otherwise there would be no way to connect directly to them. Now, suppose you have a number of computers and you want all of them to have Internet access. To do so you would need each one to have its own IP and own account and therefore you would be paying for all these accounts. Not a good idea. So what the IT people do is assign each computer with a different IP through a process called subnetting.

I had to learn how this works and to be able to manually, with paper and pencil, actually calculate the IP for each of a number of individual computers in, and also figure the maximum number of machines that can be used, order to pass the Comp TIA Network Plus certification test. Without getting more complicated than necessary, it involves taking one IP in its dotted quad notation (219.123.23.117 for example) and converting each part to binary, then 'borrowing' some bits from one of the four 'quads' (depending on the class of the IP) and using them on another quad. With DHCP, this is done automatically through the programming in the router.

So, when you walk into a wireless cafe, the AP has detected the probe signal from your wireless card, and the router has assigned you a temporary IP so the connection was made. Now you can have a cup of coffee and an overpriced lemon bar, check Email and read The Wizard of Id.

Programming the Router

The Siemens router I have uses a web browser to make and change the settings, including whether or not DHP is used (It is also possible, with most routers, to make the settings manually. Here, you would enter the computers that are permitted access to the network and/or the Internet) and various other things. So from the main (this, the middle one) computer, I type the IP, the address of the router into the location line in Opera; which is 10.0.0.10, and after the user name and password, I get the setup screen.

Now, if I wanted to, I could use either of the other two computers (the left one which incidentally uses 10.0.0.14 or the right one which is 10.0.0.13) to access the router. I believe I know what you are thinking. If we can associate with an AP and find the IP their router uses - and get past their password assuming they even use one, then we could control the router, right? Yep. Most definitely.

In the first example, using my network, Evil didn't attempt to find the IP that the router uses and even if he knew it, there is still the administrators user name and password. Much like a burglar who attempts to get into a home that has strong locks and an alarm system, they will move on, looking for a place that has neither. And in the case of wireless networks, there are plenty of them.

So next, we tried the public access AP. Once associated we had the IP of the gateway- the router- and the brand name. Now, where I use the IP 10.0.0.10 for access to my router configuration utility, this one used 192.168 which you may recall is a block of IPs reserved for internal use.

Many APs use the default 192.168.0.1 which we tried, and indeed it worked. The next step would be to get past the password, and we got lucky- whoever set it up used the default. Which is not that unusual. So, we were able to get in the router and make all the changes we wanted. We could have:

Re-routed all Email to the Sharp computer here at my apartment, copied it and decided whether to let it arrive at its intended destinaton. We did not. Changed DHCP to manual subnetting and controlled who would be able to use this AP and who would be blocked. If we knew who someone, one of the people that use this AP, is from their MAC, we could have arranged to block their access and for them to see a message stating that they were no longer welcome because they spend too much time watching "college girls take it all off". We did not. There are other things we could have done. We did not.

This was an exercise, a demonstration of how easy it can be to take control of some wireless networks. Could we have been caught "breaking into someone's network"? First, how do we define "breaking"? This AP is open, available to anyone who wants to connect. For free. So, by accessing it, associating or connecting to it, we didn't "break" into anything.

As to accessing the router setup menu, what we did was type different IPs into the browser window. The same as anyone would do to log on to any web site except that we used the dotted quad notation (192.168.x.x) instead of the name. We observed what we saw. We looked through the menu selections to see what was there, but again, we didn't change anything. Now, as to being caught, we might have been if the people who own this network had the right software running.

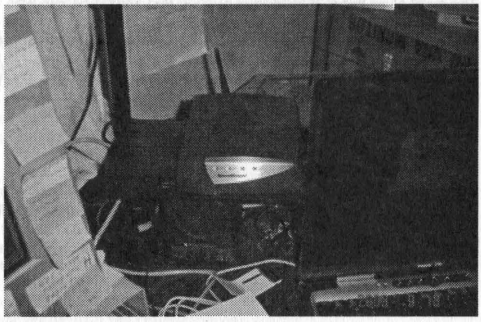
As to them finding who we were, this is very unlikely. Unless we did something stupid. Such as sending Email through their server using one of our real Email addresses or logging on to our own web sites, or accessing an FTP site where we required and used a login name and password; all of which could be traced back to us

And where, geographically we were, my apartment, this is even less likely, as you read in the Intruder chapter. If they even noticed that we were into their router configuration, they would have to take a portable computer like the Zaurus and try war walking to find us. And again as you have read, radio waves do strange things and aren't that predictable, so where would they even start. And: What would they be looking for? The MAC of the Sharp computer? Hell, we can spoof that whenever we want.

So far, we were keeping a fairly low profile. But what if we attempted to take control of an AP where the password was not the default for the brand being used?

Enter some utilities that run on the BSD Evil's computer uses- NMAP, Ettercap and Airsnarf. Running them would give us what we need to take control of the network that the owners, having it password protected, thought was safe.

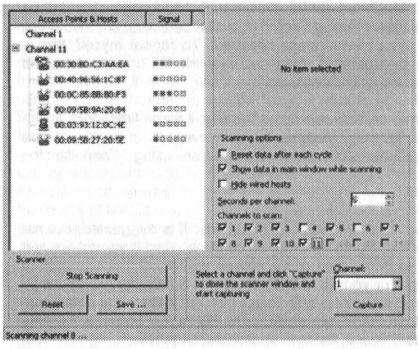
INTRUDER



I am sitting here working on something or other and I happen to notice that the Wireless LED on the router is flashing. Meaning traffic is going into or out of the device and in this case is should not be.
So I double check everything. The Sony (on the left) is not powered on and this machine (center) isn't doing anything. That leaves the Compaq on the right.

But the Compaq isn't doing anything either so the AP is just idling. Only control signals and such should be used and they won't cause the light to be on that much. Someone has found my AP and is using it for Internet connection. Fascinating! I have got to find out who it is and where they are. Not that I am concerned, it is a good learning exercise.

I will elaborate:
The router that the three machines are connected to has a configuration setup in which you can list what computers are allowed to access the network and which have permission to access the Internet. In other words, when the intruder connects to my AP, they can not directly access any of my computers, can not read or copy any files, but since I had allowing Internet access open, the intruder did, in fact, spend hours surfing the Internet through my AP.



I double checked the configuration and once I had verified that I was secure, I opened CommView and scanned the channel my AP was on (9) until I had a list of everything that was operating within range of the AP antenna. Filters were set up so that only certain protocols would be displayed- HTTP and the Emails including POP and SMTP. Then, nothing to do but sit back and wait. So, I watch for a while and see the intruder as they connect to dozens of web sites, mostly universities. North Carolina, Wisconsin... The Intruder was reading files on the physical sciences, physics and some chemistry, and then after a while they spent a couple hours searching through Ebay.

Spoofing the MAC
Over the past several months I have been working on these articles, I have been entering SSIDs and MACs in a database. So, I note the MAC they are using and check my list but it isn't there. Next, I use the CommView feature that provides the manufacturer's name for the MAC.

Spoofed!
There is no listing for this MAC. But the list in CommView may not be complete (it is an added feature and not intended to be a complete database) so I Google it. Again, no listing. So now I know that the Intruder knows how to spoof a MAC. This isn't someone who just happened to find my AP and use it without knowing it is not a free public access service- not an innocent student who bought their first wireless card and was trying it out. Nope. I was dealing with someone who knows their stuff.

They stayed connected for several hours and I watched them go from one site to another and from what these many web sites were about, I began to form a picture. The intruder is a student, oriental, probably Chinese from Taiwan, has college level knowledge of the physical sciences, has at some time in their live lived in Russia or has friends there and can speak that language to some extent.

The arrangement I have, my network configuration is rather inconvenient. If I want to scan for APs, some software will stop on my own AP and not scan any further. But since two of the three network computers work wireless through the AP, if I shut down the AP they lose the Internet connection.

There is no way to turn off the AP except by shutting it down. Something I didn't know when I bought it. So, should you want a setup similar to this one you might consider a separate router and AP. True, I would use CAT-5 cable but that involves changing settings and it is easier to just do without one computer and use dial-up for the other. Meanwhile the main, center, computer is wired to the router so I just unplug the CAT-5 cable from it and connect directly to the DSL modem.

A few hours later, they were gone and they haven't returned. I needed to change my setup configuration to work on a different project, and that required that I disconnect the AP, which meant also disconnecting the router. After I set it back as before, I never saw them again. I don't know if seeing my AP go down caused the intruder to believe they had been detected. Scared them off. I really wish I could have found them and learned where they were located- like I said with the brick wall it couldn't have been very far away. I saved the log files and later when I had time, went through them, but couldn't find anything that would narrow down who my intruder was.

I was hoping like hell that they would do an Email check. Then, I would have them. But alas, no. Anyone smart enough to spoof a MAC isn't gonna do something that dumb. If they had stayed connected long enough, eventually they would have done something that would have revealed who they were.

Now, since they were - had to be - so close, I could have taken a pocket computer or wireless PDA and did some War Walking. But, alas, I don't have either. The Zaurus from Sharp, with a nifty WiFi card, a nice little gadget that runs Linux, fell off my desk all of 2 feet onto a carped floor, and the backlight broke. Cost more to repair than it was worth. And toting the Compaq around isn't practical as it weighs too much - a full size notebook computer.

The point of all this is that serious hunting and finding people who associate with an AP is no trivial matter. I will qualify that: If you have an AP located in a rural area and there isn't but one or two houses or office buildings or whatever anywhere close - within a few hundred yards or so, then you know where the intruder is located. In a large city with hundreds, thousands, of APs operating, well that complicates things. Remember that radio signals -WiFi transmissions are unpredictable and can bounce off buildings and be detected in places that are not in the direct signal path. So, finding an intruder is no trivial matter.

COMMVIEW

Sniffer:
A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal. On TCP/IP networks, where they sniff packets, they're often called packet sniffers. Definition is from www.webopedia.com.

If you happened to read the original series of Cyber-Street Survival articles, you may remember that I had much to say about the wired network version of CommView. An excellent program. The same is true of the wireless version. Of all the programs I have reviewed, and there were many, I consider CommView to be the best, all things considered. So, I will be using CommView for as an example in the chapters on wireless networking as well as a comparison to other programs.

What's so great about it? Features, ease of use, excellent help files, powerful Rules or 'filters' and tech support, yes, but especially the ability to operate totally silent- in Radio Monitor Mode, mentioned earlier. This means your wireless card does not transmit. So, not only will no one know you are using it- there is no signal through which it can be detected, but also if you are using a directional antenna, you will not cause interference to any other wireless network. To repeat myself, this is important as among the many wireless users there are hospitals that depend upon the network for important patient information. And, as I have read, this can include monitoring systems such as in Intensive Care Units.

If you decide to try CommView, you can download the trial version from www.tamos.com. There are some limitations to the trial version, but it is not 'crippled'; you will be able to use the demo in its many features, but only every other packet of data will be displayed. First, search their site to see if CommView is compatable with the WiFi card you are using. Then start the download.

Installation
CommView installs the same as any other program, just run the .exe file and follow the directions. It is suggested, but not required, that you install it in the default directory which is C:\program files\commviewwifi. Once done, start it up and you will see a screen with instructions on configuring your card. Scroll down to the bottom of the screen and check the appropriate box; whether or not you already have the drivers for your card installed, or you do not. If this seems a little confusing- and it might, go back and start over and read carefully what is written and you should be able to get through it OK. If you continue to have problems, open Control Panel from Start/Settings, System then Hardware and Device Manager. Look for the little green icon that says 'Network Devices'. If there is a yellow question mark over it, there is an installation problem.
Right click the icon and click Properties, then Driver and see what is there. There should be a note that the driver is TamoSoft. If not, delete it and start over.

Note that if you already have drivers installed for a different card, that when you install CommView and later want to switch back to the first card, you will need to go back to Control Panel, click 'Install one of the other drivers'. Then select the one for the other card.

When you start it up for the first time after driver installation, click on the triangle button in the top left corner to start scanning and you will see a screen like this.

Select which bands you want to search (A, B, or G, depending on the card you have) and which channels. Turn off (don't check) Reset data after each cycle, and don't check Hide wired hosts. If this is checked, you may miss capturing some APs. Now, click on Start Scanning and let it run for a while, observing the SSIDs that appear in the left pane.

What is all this?
If you are in a place where there is a lot of wireless activity and if you let CommView run long enough, you may well be surprised at the number of SSIDs appear on the screen. As an example, I let it run overnight and on channel 1 are only five that are APs- (icon with the 'rabbit ears' antenna), and 86 others that are either 'Not Wireless Host' (icon without rabbit ears) which are computers that are part of the network, but are connected with CAT-5 cable. The third icon, a portable computer, is a Wireless Host' connected with a WiFi card to one of the APs.

This can be confusing as you may first wornder what kind of AP can have so many wired computers. A fairly big corporation to have so many. In this case, there is Citi-Net, the company that provides wireless Internet to tenants and this neighborhood has dozens of apartment buildings.

But that's only part of the answer. Of you scroll through the list of all channels, you may find that the same MAC is on more than one channel. This may be caused by multi-path distortion as described in the chapter on Wave Propagation. It is also possible that some of the MACs are seen on more than a single channel because the edges of the individual bands overlap slightly. Finally, there are sometimes 'ghost' images that somehow just appear out of nowhere. This is complex and there is no need to go into it here - you can always read some of the books listed in the Appendices, particularly from the ARRL if you want a better understanding of wave propagation. For now, let's go on with CommView.

Once there are some APs listed, select the channel you want to monitor- at first perhaps trying the channel that has the most SSIDs. Click Capture to start capturing packets you will see a screen like this one:

Note: For this example, I have captured packets to and from the Left computer that has the LinkSys PCI wireless card and the Slemens router/Access Point. Only within my own network, and I gave myself permission to do so. Observe that under MAC Addresses are LinkSysPCI (MAC 00:06:25:1D:9F:C9) and MyRouterAP (00:C0:02:CA:51:00). These are aliases. With CommView you can assign an alias of your choosing for MACs and IP addresses. This makes it easy to keep track of what you are seeing and has the added benefit of being able to quickly spot any new ones.

Click on any of the listings in the top window and you'll see the text that is in that packet. What you see above is an Email capture using Pegasus, a free Email program and one of the best. At the bottom is the sentence starting with "This is an example...".

Right click on the line and then 'Reconstruct TCP Session' and a new window opens: This shows the message in plain text without the control characters and formats it for easier reading. If I back up a few lines, the screen would show my login name and password. In this case, the port being used was 110 which is POP or Post Office Protocol.

If it had been port 80 which is HTTP as in browsing a web site, there might have been graphic images included in the packets. At the bottom right is Display type:. Scroll down to HTML and click it and as above, a new window pops open in which will be displayed the graphics. With the right pointing arrows, >> and >>> you can follow the packets, to some extent you can follow along and see what the person who made this WWW web site connection was seeing.

Here is another example of capturing wireless packets. This is the IRC channel #SF2600 on EFnet. We were yacking about The DaVinci Code book.

OK at this point you have a good basic understanding of how CommView works, and with that you will have a good start on how other wireless packet sniffers work. But that's just the beginning. The CV Capture screen is in three parts and you can use the little dots and bars at the extreme bottom left corner to arrange how they appear. You can have all three parts stacked vertically or the bottom part can be on the left or right of the screen.

It seems easier to start with it on the left. That way you can slide the divider bar to the left so that you see only the top and bottom frames. We can get into what information is on the left frame later, but it is rather technical and you may not even want to use it; it depends on how far you want to go with this versatile program. Now, please click Help and read Using the Program. Read it carefully, and while you probably will not absorb all that is there, it will help you understand what you see on the screen.

OK, now look at the lines of text and scroll through them, observing the different IP addresses and MACs. Again, depending on how much wireless traffic there is where you are, there might be thousands of lines from hundreds of different APs. With hundreds of MACs and IP addresses. Any number of people connected to the various APs, reading the comics, checking the stock market, sending "confidential" Email... CommView is logging everything that is being transmitted within the channel you selected. It can be mind boggling as you look at the very bottom of the screen and see that CommView has captured several million packets.

FILTERS

In order to zero in on only the specific information you want, you have to learn about filters, or 'rules' that control what data gets through and what is blocked. (Actually CommView captures all of it, the filters control what appears on the screen and lets you save only the packets you want).

Filters can be the most confusing aspect of wireless networking. Some applications, sniffers, have a simple 'off-or-on' and don't clearly show what is passed or what is blocked. Some don't actually have filters built in, so you have to create (write) your own or copy those someone else has written. And for a beginner, that would require a fair amount of searching the web. And then, the syntax of filters for one program aren't necessarily the same for another. Capsa has a nice filter set, and Ethereal also although not as easy to understand.

CommView has the most versatile set of filters of any program I have ever used. So let's get started.

At the top of the screen are three buttons. D, M, and C. They stand for Data, Management and Control. And if you click the Rules at the very top, you will see Ignore Beacons. (See glossary) For now, engage only D for Data and don't check Ignore Beacons. This means that, so far, you want only packets of data that may contain useful information to be displayed in the bottom part of the screen. Once you have done this, clear the packet log to get a blank screen, and watch what is happening. Pause and examine some of the data by selecting one line in the top window and viewing the contents in the bottom window. You might find something interesting, but for now, let's continue with using filters.

*** Beacons**

All access points ship with a wireless beacon signal so that wireless PCs can find them. In effect, the beacon signal is shouting every tenth of a second or so, "I'm here! Log on!" With Ignore Beacons not checked, you will recieve - depending on how many APs are operating on the channel you are monitoring, many thousands of packets that you do not need. At least not yet. Now, click on Rules and look at the tabs on the left side of the screen.

*** IP:**

Internet Presence of a particular computer- or the IP that a computer is connected to. Here, you can pass or block IPs.

*** MAC.**

As explained elsewhere, MAC is Media Access Control, a hexadecimal number that is unique to every computer network card (NIC) as well as other networking equipment.

*** Ports**

A port is like a door or portal through which information is sent and received in a computer. There are 65535 ports available but only the first 1000 or so are actually normally used, that is up to 1023. Beyond that they are Registered (1024 to 49151) and Private, 49152 to 65535. There is no need to study this long list of ports as only a handful apply to filtering in wireless networking.

Click on those that you want to pass or be blocked. Port 80 is Hypertext; the World Wide Web. Port 25 is Simple Mail Transfer Protocol, used for sending Email through a server. Port 110 is Post Office Protocol, for receiving Emai. Others are FTP, Telnet, IRC (Internet Relay Chat) and on and on.

*** Protocol and Direction**
This is advanced and will require some study that is beyond this chapter, with one exception: Click on ARP to avoid having the screen flooded with useless characters.

*** Text**
Text is just what it implies. Enter a string of characters and select whether they are to be Captured (displayed on the screen) or Ignored.

*** Advanced**
Here, you can make a list of APs by their MAC (based on their SSID) and individually select which ones are to be Captured and which are to be Ignored. In this neighborhood there are, as previously mentioned, a couple hundred APs. Many of them are from something called Citi-Net which is a company that provides wireless Internet to the tenants living in the buildings that they own. They operate on several channels and so there is a great deal of data passing through this sophisticated system. Most of it control and management. So, to eliminate traffic from this organization, I wrote these advanced filters.

Block Citi=not((smac=00:0C:85:BB:B0:F3 or dmac=00:0C:85:BB:B0:F3))
Block Citi-Net Wireless=not((smac=00:0C:CE:0C:E9:2A or dmac=00:0C:CE:0C:E9:2A))
Block CitiNet=not((smac=00:02:6F:04:77:5B or dmac=00:02:6F:04:77:5B))
Block citi-net-public=not((smac=00:02:6F:05:EF:72 or dmac=00:02:6F:05:EF:72))
Block citi-net=not((smac=00:0A:41:7D:43:A6 or dmac=00:0A:41:7D:43:A6))

The first filter, "Block Citi" is just one of the SSIDs they use. 'not' obviously means do not display these packets on the screen. Then, smac is source, dmac is destination. So what it all comes down to is that with the use of filters, you can let every packet that is being broadcast from all of the IPs that are within range of your computer, to be displayed on the screen and/or saved as a file, or you can narrow this down- fine tune it. Suppose, for example, you are an upper level manager at a company that has hundreds of employees and dozens of APs. You have reason to believe that some workers are browsing Ebay on company time and you want to find out who they are.

You can start by running CommView to capture APs on a particular channel and then use the Text filter to set off an alarm whenever 'Ebay' is captured, and within the captured data will be the MAC of the computer that it is being sent to. And, that employee is then invited to an interview with the office manager.

Advanced filters can get much more complex than just blocking certain MACs from Citi Net. This one:

((sip from 192.168.0.3 to 192.168.0.7) and (dip = 192.168.1.0/28)) and (flag=PA) and (size in 200..600) //

It captures TCP packets the size of which is between 200 and 600 bytes coming from the IP addresses in the 192.168.0.3 - 192.168.0.7 range, where destination IP address is in the 192.168.1.0/ 255.255.255.240 segment, and where the TCP flag is PSH ACK.

Again, it is complex and requires some study, but the possibilities are virtually limitless in what you can do to narrow down incoming (Source) and outgoing (Destination) packets of data. And, you can save any rule set you have built; as many as you want. So, if you have a set for watching one particular employee, you can save that set as the person's name, or save a set for a specific MAC, and then load, on the fly, the set you want to use at any given time.

WEP and WPA-PSK Encryption
CommView can display encrypted traffic from APs in real time, if you have the right keys. Under Options, check 'Forced WEP decryption'. Note that this does not mean CommView can crack encryption or derive the keys that are being used. It means that if you have and are authorized to use the keys, then you can read data as it appears on the screen rather than having to save them, save the packet buffers, and decrypt them later.

Just as there is no limit to what information goes out into that vast mind boggling series of wires and satellites, routers and gateways that we call the Internet, there is virtually no limit to what anyone with the right equipment and software can intercept.

Questions:

Q: I do a scan and, on a certain channel, see a number of APs and a lot of wired hosts. But when I Capture, how can I tell which host goes with which AP?
A: Those listed directly beneath the AP usually are within the network that the AP is operating from. But not always. As mentioned before, some signals may appear on more than one channel. But it is, or can be, more complicated than that. Like Citi-Net that you read about in Filters, which has many APs and hosts within your range, so there could be any number of wireless devices, computers, routers, bridges where many computers communicate with others. You could go crazy if you tried to keep track of all that you see. Use filters and concentrate on one AP and it's hosts.

Q: I wrote down some of the wired hosts, but I don't see any packets from some of them.
A: First, did you make note of the signal strength? Some of them will be too weak to be captured. The "Capture damaged packets" option might make a difference.
But remember that not every computer in a network is transmitting all of the time.

Conclusion:
All things considered, CommView is one of the best and most useful applications available. True, it isn't cheap at $500 but it is well worth the price- it does what other programs costing several times the price do not do. And of course you have the advantage of running in Radio Monitor Mode.

Spend a few hours learning CommView, monitoring, and working with the versatile filter combinations and you will realize what an excellent program CommView is.

Next, some other wireless programs are reviewed.

Most of the cards, PCI which plug into a slot on desktop computers, or PCMCIA for portables, are for 802.11b which transmits on 2.4 GHz. There are some for 802.11a which seems to not be used much and works on 5 GHz, and then there is 802.11g which also use 2.4 GHz but transfer data much faster. Then, there are cards that may work on b and g, or all three. Something to consider before you decide which one to buy. Several cards will be reviewed in the next article.

Wireless Network Monitoring and the Law

Radio waves, signals of all types, cover the entire surface of this planet. Radio, TV, International short-wave, and of course wireless networking. In a metropolitan area, there are so many of them that were they to become visible, they would blot out the rays of the Sun. And even if you lived in an ice cave somewhere in Antarctica, you are still inside a web of radio signals.

Now, there are people who say that since these radio waves pass through my home and my body, then I should have the right to know what they are and what they are sending- what information is being transmitted. It doesn't work like that. There are laws - many of them that state what you can or can not "listen" to, what frequencies you can tune your radios to. But you don't necessarily have control over that with wireless networking. You have a portable computer with an 802.11b PC card. You go to an Internet cafe, and you are instantly tuned to their AP. Their Access Point, on whatever channel it happens to operate. Probably.

But, supposing there is some big corporation in the same building, up a few floors, that has a wireless network, and because of the way that radio waves behave - especially at microwave frequencies which is where 802.11 systems operate, instead of seeing on your screen a list of the kinds of coffee you can order, you see pictures of naked people engaged in sex acts. Middle managers are goofing off and browsing porno sites on company time. Or maybe you see a confidential message sent from the CEO to the Chairman. About a merger that they would rather no one else know about.

Hey, all you wanted to do was go have a cup of house coffee, check your Email and the stock market.

So what do you do? There really isn't anything you can do; your portable computer has connected to the strongest signal that it could detect, unless you make the effort to connect only to what you reasonable believe you are allowed to. And how many of the millions of WiFi users do so? Or even know how?

If you want to know exactly what the law says about monitoring wireless networks, I suggest that you consult an attorney. Assuming that you can find one that knows about wireless networking. And, you can check out the Electronic Privacy Information Center (EPIC) and the Electronic Frontier Foundation (EFF) and other related sites.

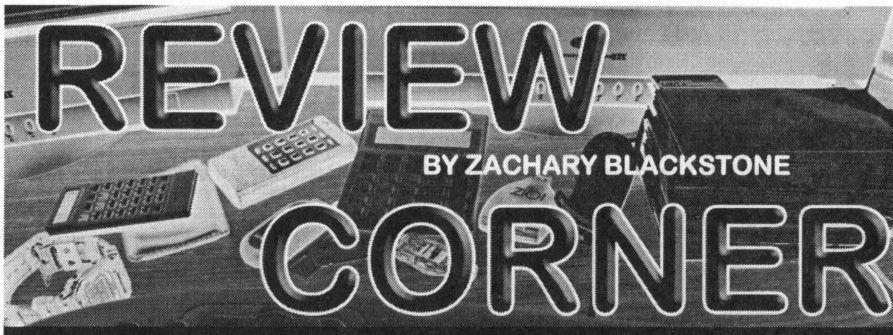
What the law seems to say is that there are no restrictions on detecting transmissions from an AP using Network Stumbler or other 'sniffing' applications, which again you have no control over, but that it is against the law to connect, 'associate' with any AP unless you know it is open to the public, to use an AP to get Internet access, and to intercept any data from such a wireless network.

OK, troops, you now have a pretty good understanding of wireless networking. If you practice using Network Stumbler and CommView, especially learning the filters, you can fine tune your system so that it intercepts exactly what you want, leaving out everything else.

Then, maybe you will want to try out different locations and should you have a GPS receiver and mapping software you will soon be adept at making site surveys. Ordinarily I hesitate to recommend any Microsoft product but Streets and Trips is an exception. An excellent and affordable application.

Meanwhile, I hope you will take the time to become more familliar with networking terms and technology, and read the articles on sites such as slashdot. Then you will be in a better position to use the bootable Linux CD called Auditor, which will be reviewed in a coming article.

M L Shannon is a SF writer, author of several books on electronic surveillance from Paladin Press. ...graduate of a 2 year college in electronics, former countermeasures sweep technician, has been guest speaker and made a few radio and TV appearances...



Ok, so we're getting back into reviewing hacking related items again. Several people have suggested ideas and submitted material for us to check out and to comment on, hoping to make the items known to the rest of the community. So, with no further adieu, here's our review content for this issue of Blacklisted! 411.

CIDPad
Classifications: Software
Cost: $34.95
URL: http://codegods.net/cidmage/

Remember back in the day when we had "Phoneman" for the Commodore 64? It produced Red Box tones, Green Box tones, Blue Box, Silver Box, etc. Well, CIDPad is somewhat the same, except that it addresses a whole new technology that has since emerged (oh and it doesn't run on a Commodore 64 either). Caller ID technology has eluded most people for over a decade now, people not knowing how it works or ways to circumvent it's use. The people over at Whirlwind Software have created this awesome little program which can use your computers sound card to produce the caller ID signals. Yes, this is exactly what you would use to "Orange Box" with. Orange Boxing is ineffective in my opinion, but interesting nonetheless. CIDPad is actually the economy version of the more expensive (and more powerful) CIDMage ($49.95), but don't let this fool you into thinking it's not powerful. This program should be classified as a tool considering it's possible use. There are an endless number of uses for this program. Aside from the obvious use of prank calling, on a more serious note, this could be used to generate specific name/number information on a Caller ID unit for use in the film industry for instance. CIDPad will generate MDMF Name and Number Caller ID signals, Call Waiting Caller ID signals and Number Only Caller ID signals (which is used with the oldest of the Caller ID equipment). Additionally, you can create WAV files with your caller ID data streams. It will run on any Windows OS from 95 on up. The only "extra" you'll need to purchase (or construct yourself) is a phone line interface/isolation unit. Radio Shack comes to the rescue with model number 43-228 "Recorder Control" (just use it to pump sounds INTO the line). At $25.99 it's pretty inexpensive. Of course, you could opt for the premium model (43-2208) at a cost of $29.99. Either way, these will allow you to get the job done. So, what's my final word on this? Two thumbs up. Way up.

Touch Tone Decoder Model 930
Classification: Tool
Cost: $139.00
URL: http://www.vikingint.com/tel2.htm#.

This is a really nice touch tone decoder with a 16 character display, 1K of memory and includes a serial port. I really have a thing for tone decoders, so I pay extra attention to the details. What I like about this one is the case that it's installed into (it's easy to open up and modify). The unit is simple to use and very effective. It lacks the refinement of some of the premium models I've seen before (ie: much better menu, larger memory, etc), but this one makes up for everything with it's no nonsense approach which can be much appreciated in a situation where the user has little time to do his or her job. It's pretty solid for field use which is a BIG plus in my book. If you're looking for a unit which has all the bells and whistles, this isn't your answer. However, if you're looking for a rugged tone decoder to drop in your tool box, it's a decent choice. Overall, I still believe this is a very useful tool and I'm going to hold onto mine for a long time to come. I'll give it a thumbs up.

8 Minute Digital Audio Board #DAB8
Classification: Tool
Cost: $121.00
URL: http://www.dschmidt.com/digaudio.html

If you're anything like me, you've run into situations (more than once) where you've needed a device for your project which would record audio. The uses for this are endless. First thing that comes to mind is Amateur Radio. This would be perfect for an automated call sign. Or how about an automated alarm system call out feature? One of the guys over here used several of these for some Museum displays and they worked out perfectly. Yeah, I'm sure you have better ideas and that's good. Keep thinking! Well, this unit will record up to 8 full minutes of audio in a single recording or anywhere from 1-8 recordings from 2-4 minutes each. The unit is extremely simple to operate and has a user selectable option to auto-play upon power-up which I thought was very cool. You can record audio from three different input sources (a built in microphone, or two 1/8" inputs). It also comes with a 1/8" stereo speaker output and 1/8" mono output. The downside? Unfortunately, there is a problem. The audio quality is good, very good, but it's not good enough in my opinion. The plus side. The unit has nonvolatile memory which means your recordings will stay intact for many, many years to come, even without power. I still find this item of great use, so you may also find it of use. On a slightly different note, the people over here at Dschmidt Technologies offer several other items of interest. You should check them out and see what interesting items they have. You might actually find something useful.

Doug TV
Classification: Video [Underground]
Cost: Free
URL: http://www.dougtv.org

This is a hacker TV show done by "Doug" and also spotlights the goings on of Lucky225, a well known local hacker in California who's phreaking skills are quite the topic of many conversations as of late. Anyhow, I got my hands on episode 1 and 2. I watched them both in their entirety. The intro to the show is amazing. I love it. The effects are great. The video quality sucks from time to time, but overall, it looks good for a self produced show. The antics that go on are both entertaining and educational. I don't know about the trips at the drive through, but it reminds me of similar times from years ago when it didn't matter what we were doing — we had fun doing anything. If you enjoy watching some real life, no frills hacking, here's your show. When they do manage to film some hacking in the form of phreaking, it's actually quite educational. You may actually learn something from this show. I'm going to give this show two solid thumbs up and I suggest to all readers that they take the time to watch these shows and support their efforts any way you can. Note: As of this writing, the above link seems to be down. I don't know if this is a permanent situation or not. It would be a shame if Doug decided to cut the show.

Whitesword TV
Classification: Video [Underground]
Cost: Free
URL: http://www.athnex.com/whitesword

Yeah, ok, so there's another hacking related show out there called "Whitesword TV". Sixteen episodes strong, it's definitely solid. The show is pretty much all about urban exploration which has always been associated with social engineering which in turn has always been associated with hacking. So, you can see how this is remotely geared towards hackers. I'll admit that I sat and watched every episode. Some bored me to tears, others entertained me, some of them made me say "WTF?!". Though, I really did enjoy all the crazy places this guy visited and captured on camera. I wish more people would record this kind of stuff so people like me can go through it and pick it apart. All in all, I think this guy is onto something and I believe others will agree with me. All I can say is go watch this yourself and see what you think.

10Hz to 3GHz Deluxe Handheld Frequency Counter Model #104
Classification: Tool
Cost: $229.00
URL: http://bkprecision.com/www/np_searchmodel7.asp?lf=Handheld+RF+Counters

Ok, so I'm sure all of you know how much I like my tools. This one is no exception to the rule.. The Model #104 from B&K Precision is simply awesome., or "dope" as some of the others around here might word it. Yeah, it's $230, but it's money well spent if you have it. You might wonder what use something like this may have. Well, I have one. Snatching frequencies from mobile radio equipment in use. All you have to do is have this sucker running in proximity of a radio transmitter and it will indicate the frequency transmitted. Nice! This unit has a 10 digit display and has a range of 10hz to 3GHz, which is pretty amazing. The unit comes with a rechargeable NiCad battery pack and an AC Wall charger. It even has a display backlight for use in low light situations. It's small, lightweight and easy to conceal. The only downfall of this item is that it only works with analog signals which is somewhat of a bummer, but aside from that, I love this device. Into the toolbox it goes.

Note: For a similar unit which also handles digital signals, try model # 106 from B&K. It's $219.00 , but has fewer digits on the display and a smaller frequency coverage (30MHz - 2.8GHz).

BLACKLISTED 411 WANTS YOUR ARTWORK

Are you an artist? Do you like Blacklisted! 411? Do you hate Blacklisted! 411? Well, if you're looking for work, it doesn't matter if you like us or not, does it? If you'd like to show off some of your talent, why not send us some samples on PAPER or send us a disk with your sample artwork. We'd be happy to show off your work, give you a free subscription or make some other arrangement if you'd like. If you're interested, take a look through the magazine and make note of the existing artwork. Think about it and try to come up with something completely original which coincides with the general theme of the magazine. A few ideas to consider: Pirates, Skull & Crossbones, Einstein, Computers, Electronics, Phones, Cable TV, Satellite TV, Radio, etc.

Here's who you send your artwork to:
Blacklisted! 411 ARTWORK
P.O. Box 2506, Cypress, CA 90630

We WANT to hear from YOU....**don't delay - just send us what you have. We prefer freehand artwork on PAPER, but will accept in high resolution (if at all possible) computer graphics formats: TIF, TGA, JPG, GIF, PSD, PCX and most other popular image formats.**

Vigilante Social Engineering: Is it Black, Gray, or White Hat?

By Erik Giles

The growth in use of PC's and the internet during the past decade has made it easier and cheaper to service thousands of customers in all kinds of businesses. But these very technologies also make it easier and simpler for criminals to dupe these same customers with social engineering schemes. The internet has allowed a new wrinkle in the world famous Nigerian 4-1-9 advance fee fraud.

It's my job to contend with and reduce the impact these crimes have on the company I work for and the customers we serve. I use all the creativity I can muster, but must operate entirely within the limits of the law to defend against bank fraud. But on occasion, I let the 'dark side' of my creativity take over, and dream up ways to counter these schemes if I was allowed to use illegal vigilante tactics. Of course, I cannot execute, recommend, or condone this kind of behavior. But it does make for a very interesting 'thought-experiment', as Einstein would call it.

Could one steal from the fraudsters? I think so. Read on.

Nigerian Advance Fee Schemes

The Nigerian 4-1-9 (or West African) schemes date back to the 1960's. It's pretty simple. The crook begins his crime by posing as some kind of desperate individual, such as a high ranking government official, an oil baron, a princess, or even an heir to a rich fortune. Often this charade is quite impressive, complete with office meetings with well dressed and official looking, but phony government leaders, military officers, and banking officials.

The crook sends out thousands of messages, proclaiming that there is an untold fortune waiting for them, if they could first only pay off a few key officials with small bribes. They need your help; just a few thousand dollars from you to make the requisite bribes, then the fortune of a hundred million dollars is theirs. And of course, for helping them they will share 15% of this incredible fortune with you.

Of course, these big fortunes never materialize. The crooks continue to string the victim along and bleed him for every cent that they can, saying that the next bribe is sure to be the one that will free the fortune. When the scheme is over the victim has nothing left and can even find himself in physical danger. A number of victims have had to flee Nigeria in fear for their lives, and I am aware of at least one American victim who was executed in grisly fashion.

It would be fun, poetic justice to turn the tables on these guys. And I wonder, though it's probably illegal, could one ever get into real trouble with the law for doing it? Like money stolen from a drug dealer, what law enforcement officer would bother trying to arrest someone for stealing money from a Nigerian 4-1-9 fraudster? The important thing would be to make sure that the crooks don't send their own goons after you. Fortunately, the internet offers the anonymity needed to pull this off.

Vigilante Tactics and 4-1-9

If you have an email address, you have likely received a message like this at least once. I received this one earlier this year.

My Dear Friend,

It is with hope that I write to seek your help in the context below. I am Hajia Mariam Abacha, wife of Nigeria's former head of state; Late General Sani Abacha, whose sudden death occurred on the 8th of June 1998. Since my husband died, I have been thrown into a state of utter confusion, frustration and hopelessness by the present civilian administration. The security agents in the
country have subjected me and my family to physical and psychological torture. As a widow that is so traumatized, I am hopeless with my present faith.

You must have heard over the media, reports on the recovery of various sums of money deposited by my late husband with various security firms. Some companies willingly gave up their secret and disclosed our money confidently lodged there, while many, embarked on outright blackmail. In fact the total sum discovered by the government so far is in the tune of $700 Million USD and they are not relenting to make me poor for life.

I came in contact with your name and address through my personal research and would want to have faith and confidence in you as I view you to be a responsible personality. I have no doubt about your capacity and goodwill to assist me in receiving into your custody(for safety) the sum of US$40.3 Million USD willed and deposited safely in my favor by my late husband. This money is currently kept in Safe Deposit Box (SDB) at a security firm within Europe.

As it is legally required, the administration of my late husband's estate is under the authority of the family's Attorney

Mutalib Inuwa (Senior Advocate of Nigeria). The investigative teams set up by the present government have submitted their report after freezing almost all our account.

Fortunately, our family lawyer had secretly protected the personal will of my husband from the notice of the investigators and has strictly advised that the $40.3m USD be urgently moved to an overseas account of any trust worthy but ANNONYMOUS foreign family friend without delay, for security reasons. All our traveling papers have been seized by the government thereby preventing us from traveling and all the local and international outfit of our business empire seized. This sum of money is our only hope to stay alive.

I have therefore agreed to compensate your goodself with 30% of the total deposit when you finally receive the deposit box from the security firm and its contents safely lodged in your account. You are equally guaranteed a 100% risk-free and smooth transfer. If you are interested in assisting me, please reach me immediately through this email address hajiamariaba@netscape.net sending to me your confidential telephone and fax number(s) so that I can reach you as soon as possible.

For obvious security reasons, it is imperative that you keep all our communication very secret. Do not mention my family's name or disclose the transaction to anybody. If you are not interested in assisting me, still get in touch so that I can make alternative arrangement as time is of
the utmost importance. I beg that you, do not expose me to my government as this will have grave consequences on my family.

Regards,

Hajia Mariam Abacha.

When I received this email, I decided to have a little fun with the fraudster. Here is the message I sent back.

Dear Madam:

It just so happens that I will be traveling to Switzerland early next week on business. I am the owner of a large automobile dealership located on the eastern coast of the United States and I will be happy to help.

Let me know what I need to do next.

Erik Giles

Of course they responded back. The crook told me to pay thousands in fees to the security company, and then they would open deposit box. The forty million would be released and I'd get my huge cut. All I had to do was travel to Switzerland with the money in hand.

Now this is getting interesting! So I sent this message:

Dear Madam,

Unfortunately, due to an emergency, I will not take my scheduled trip to Switzerland. However, would it be possible for me to wire the money to yourself or a representative. Please send me the appropriate wire transfer information, including a contact name and account number.

I will then wire the money to you, which you can use to pay the security fees. If this is acceptable, please let me know the correct amount and the account number to which I should wire the money.

Thank You,

Vigilante Thought Experiment

And to my utter shock, the crook sent me a name and an account number. Now this was getting a little scary, so it's where I stopped. But what if I took it a couple of steps further? Let us proceed with the 'thought experiment' I mentioned above.

What if I used the account number they sent me, created a fake check, wrote several checks out to myself, and deposited into another bank account? Preferably an anonymous account in the Caribbean. Then I could cover my tracks by reporting the fraudster.

To make this work, I would do all of the following:

1) Determine exactly what bank the account number corresponds to, and make an excellent copy of one of their checks. Not all countries in the world allow people to make home made checks like in the United States.

2) Since you don't know how much money is in this crooks account, (it could be nothing, it could be a few thousand, or maybe even a hundred thousand), it would be smart to deposit several checks of varying dollar amounts. The checks that are too big would bounce, and the smaller checks would clear.

3) Follow up with a wire transfer to the account they gave you. Send a small sum, like $50. You are doing this so you can proceed to step 4.

4) Report the fraudster to the correct authorities, claiming theft of the small sum you wired. The local police officers would likely pursue the crook, or at the very least, close the bank account. By getting the fraudster either arrested or scared off, you reduce the chance that he would be able to recover the money to stole in step 2.

Remember to execute step four only AFTER the checks you wrote to your anonymous bank account have cleared.

Hmm. Is this kind of vigilante justice legal? Of course not. But it might be 'effectively legal', in that I find it very unlikely that any law enforcement officer would ever bother to help the fraudster get his money back.

If enough people did this kind of counter attack, this might deter future 4-1-9 schemes, and save some people a great deal of money, as well as possible bodily harm. And to satisfy your conscience, you could always donate your proceeds to a charity, possibly one that benefits Nigerian children.

I might use this concept in a future book. *Vigilante* would be a good title.

Hacking the XMDirect Cable

(How you can build it yourself cheaply)

An XMDirect cable will give you the ability to control a XMDirect device with your computer. In this article, you will learn how this cable works, how to build and use the cable out of components you may already have at home, and how you can do come cool things with your XMDirect using free software applications, such as turning your XMD1000 into a XMPCR.

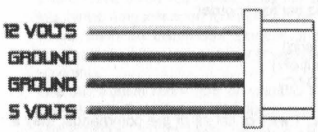
Before we get started, I would like to thank http://www.hybrid-mobile.com, sonnik, dbroome, and dobbz for all the reverse engineering they did on this project.

In this article the following terms will be used, so take a second to become familiar with them:

XMDirect
The XM Receiver used to connect to the computer. Model number XMD1000

XMPCR
(**XM** Personal Computer **R**eceiver) is a small USB device with an antenna. It connects to your sound card's line-in via a 1/8" stereo cable. It was released in May 2003 by XM as a lower priced alternative to gain a wider audience to XM radio. However, as of August 2004, retailers started pulling these units off the shelf due to controversy over the unit. Although XM will not comment, it is believed XM was worried the RIAA would claim it was a device to aid in music piracy (which is not the case).

Male Molex
A standard 4-pin computer power supply plug (see pinout below) you will use the +12V (yellow) and -12V (black next to yellow). For clarification, the male connector cannot be plugged into a hard drive, that would be considered female (look at the pins to differentiate)



Ok, enough with the terms, let's get to the article.

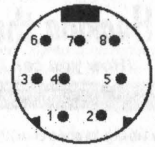
Now why do we want to use our computer to control our XMDirect? Why would we want to tie this unit down to a computer? There are several reasons, but probably the biggest draw is using it in a Carputer setup. Building a Carputer is a totally different article but the basics are that you replace your current car stereo with a computer. This enables you to listen and watch all your mp3's, music videos, movies, DVD's, etc., in your car. Connecting a XMDirect cable to your Carputer will enable you to control and listen to your XM using a simple and unified interface such as FrodoPlayer (www.frodoplayer.com). Other examples of uses are: watch for and record your favorite music, time shift (like Tivo) radio, publish "What your are listening to RIGHT NOW" to a website, setup rules for Artists you like and don't like, see song history, schedule times to listen/record, and the list goes on and on.

Lets build our cable. You will need the following to build it.

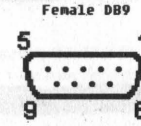
- **(1) 8-Pin Mini-din cable.** A great source of these is old Apple Printer cables. I will be using a 10' Belkin Gold Series Apple Printer Cable (Model F2V024-10-GLD)
- **(1) Female DB9 Connector and Hood**
- **(1) 4-Pin Male Molex connector & wires.** A good source for these is a Molex Y-Adapter, or your local radio shack.
- **15-30 watt Soldering Iron & Electronic Solder**

First you will need to cut off one of the ends of our 8-Pin Mini-din cable. Again, in this article I am using the Belkin Gold Series Apple Printer Cable (Model F2V024-10-GLD). The cable pinouts are below, however for ease of use I will be stating the color of wires used inside this particular cable, if you are using a different brand, model, or just building your own, you will need to use a multi-meter to check each wires pin location. (You may want to double check even if using this specific cable)

Cable Pinout:
8 pin mini-din to db9
pin 1 = pin 3 Data Receive
pin 2 = pin 2 Data Transmit
pin 3 = pin 5 Ground
pin 6 = 12v
pin 7 = 12v
pin 8 = gnd



Cable



As viewed from back of board

Using my Multi-Meter I find that Pin 1 is Brown, Pin 2 is Black, Pin 3 is Yellow, Pin 6 is purple, Pin 7 is blue, and Pin 8 is green. Once you have identified these cables you can cut off the un-needed wires (Red and Orange)

Tech Tip: *To figure out which color of wire corresponds to each pin, Strip 1/16" off each wire, and then set your multi-meter to continuity. Locate the pin you want to test, hold the black lead to this pin, and then use the red lead to test each of the wires. When you hear a beep, you know which wire corresponds...*

So to create our cable, we connect Brown (Pin 1) to DB9 Pin 3, Black (Pin 2) to DB9 pin 2, and Yellow (Pin 3) to DB9 pin 5. To connect the power to the cable, solder Blue (Pin 6) and Purple (Pin 7) together, and then solder them to the yellow wire on the male molex connector (+12v). Finally solder Green (Pin 8) to the black wire on the molex connector (ground). Use your multi-meter to double check everything and then stuff it all into the hood. Make sure that you insulate the power connections using electricians tape or heat-shrink. If you don't want to use a molex connector, you could connect these wires to a DC power connector and use a 12v power adapter to power it.

Testing our cable

Now that you have made your cable and double checked everything, lets test it out. We will need to download some software that is compatible with this cable, and that knows how to control the XMDirect. I suggest using the TimeTrax demo available at: http://www.timetraxtech.com. Connect your XMDirect cable to a spare molex connector in your computer, and then connect the DB9 to COM1 on the back of your computer. Run TimeTrax and select COM1. In a matter of seconds you should get a listing of all the channels you have access to. If you have not subscribed, you will see 2 channels.

Now that you have a working cable, try out some of the freeware apps that are available. A good listing of apps can be found at http://www.xmfan.com/viewtopic.php?t=7459

How this works and writing your own software

You might be wondering how such a simple cable is able to control the XMDirect unit. Short answer is, It doesn't. The software behind the scenes is doing all the magic. The cable just provides a transport of data between your computer and the XMDirect. When the XMDirect is powered up, it expects to be contacted by a controller. We will need to emulate this controller in order for our software to work.

The XMDirect unit requires a 3-step handshake before enabling as follows, in this particular order:

{0x5A, 0xA5, 0x00, 0x03, 0x74, 0x00, 0x01, 0x01, 0x77} (Controller contact, Hello)
{0x5A, 0xA5, 0x00, 0x04, 0x74, 0x02, 0x01, 0x01, 0x01, 0x7B} (Turn on power supply)
{0x5A, 0xA5, 0x00, 0x03, 0x74, 0x0B, 0x01, 0x01, 0x81} (Turn off soft mute on DAC)

Once these are sent, the XMDirect will accept the standard XMPCR commands. I will not list all of the commands; they are available several places on the internet. However Nerosoft has released XMPCR Object 2.0 which is a .dll that "Encapsulates the complex protocols used to communicate with the XMPCR radio. Now it is possible to operate the XMPCR using only a few lines of code! The object can be scripted from Visual Basic, C, VBScript, or even ASP pages." This object is available to download at http://www.nerosoft.com/XMPCR/index.asp. Using this .dll makes it absolutely simple to code up your own application if none of the freeware applications above fit your need.

I hope you have enjoyed this article. Remember to keep information free, if we as hackers unite and share our information with each other, we will all benefit. If you are interested in hardware hacking, I invite you to stop by my website, http://www.i-hacked.com for other interesting articles.

About the author:
Nick: hevnsnt
I have been in the underground community for years. My interests have moved to more hardware hacking, and I currently run the website http://www.i-hacked.com. This is my first article to BL411 and I hope you enjoyed it, hopefully there will be plenty more in the future.

The Hacker Chronicles

An accounting of the life and events of a real honest to goodness old school hacker.

PART III

**** A series of articles written exclusively for Blacklisted! 411 ****

By Cactus Jack

Inspired by the recent re-discovery of Blacklisted! 411 magazine and at the request of my wife, I've agreed to write a quasi-autobiography of some of the goings on in my life that relate to hacking <both directly and indirectly>, from as far back as I can recall. Amazingly enough, I recall everything from the time I was a few months old up until right now, thirty some odd years later. Very few people have a memory like mine, but those who do should use their gift to teach, instruct and entertain others. If anything, simply detailing experiences and providing a lesson in history would be more than adequate in helping the cause. With this in mind, I intend to detail as much of my life as possible, noting the many hacker related experiences I've had. I hope you enjoy the read.

Welcome to the third installment of my ongoing article.

The High School Years

Ok, so it's the first day of my freshman year of high school. Besides the typical butterflies in my stomach, it was anything but typical for me. It was that day that I had my first real class in electronics. Of course, I was way beyond first year electronics, but this was the first time I was able to flex my academic muscles in the electronics field. I quickly became close friends with our shop teacher, which proved to be an excellent move on my part with future events in mind. I also noted that nobody else in the class had no idea what they were doing in the classroom — the thought it would be an easy "A". Well, maybe for me.

Over the course of the first month of high school, I noticed several items of interest.

- There was a small room in the English Dept. full of Commodore 64 computers setup for use, each complete with a 1541 floppy drive, monitor and dot matrix printer. I found out that nobody ever used these machines for any reason — they just sat there, collecting dust. I schmoozed my way into getting the room opened/unlocked during lunch and after school so I could use the machines. It was a useful find.
- There were three full classrooms full of Apple II computers, setup for use. They also had a "closet" full of broken machines they intended to throw away.
- There were an enormous amount of phone lines going into the school. I found the utility room where the lines terminated. After some minor investigating, I found that many of the lines had a dial tone but were not connected to anything.
- The electronics room had an unused side room connected to it, complete with door/lock, power, phone lines and an access panel which provided full control of the school's intercom system.
- The intercom system was two-way. It was a common misconception that you could only hear what the office was announcing over the intercom system. In reality, you could access any the intercom of any room from any other room and listen in on them (or speak to them if you so choose). The system was very powerful, yet untapped.
- The vending machines in the P.E. locker rooms were new and hi tech, complete with bill acceptor and an advanced menu system for programming it.
- Attendance ran everything through a primitive networked computer system (with modem access) which had an easy to discover "back door". The personnel in attendance had no way to verify information in the system (ie: no hardcopy of tardy or absences to check against)
- There was a single master key that would open any door at the school. I heard rumors that the very same key would open any door from any school in the same district, but I never verified that rumor.
- The only room in the school which had an alarm installed was the metal shop.
- Every teacher I knew had something they needed to have repaired and was willing to pay to have it done.

Anyhow, reading the above notes of interest, I'm sure you can see for yourself that this high school was a hackers dream (at the time). Can you say, "easy access"?

Within no time, I had the spare room in the electronics room all to myself and had my own lock installed. I ran a few unused phone lines into the room somewhere near the end of my first year. I would find a use for them later on. I set up shop and started repairing devices for all of my teachers; everything from TV's and Stereo's to Commodore 64's, Atari 2600's, 800's, 1200's and Apple II's. At first, I was only charging them for the parts and eating some cost from time to time. Eventually, this turned into a full time job while I was at school during 4th period Electronics and Lunch break. My Electronics teacher condoned the operation and even sent new prospects to me on a regular basis. It was a sweet situation that only blossomed as I made it through my 4 years of high school.

One of the cool things about my endeavors at school was that I was "in" with the entire school staff. They allowed me to do things that a student could only dream of doing; the whole time just turning their heads the other way while I was happily enjoying my freedom to explore just how far I could go with this. The principal, the dean of students, the school board, they

all loved me and why wouldn't they? I was fixing all their electronics for nearly nothing at all. To me, it was nothing more than some more experience to put under my belt. To them, it was an incredible savings and worthy of "owing me one". It's nice when people, a lot of people, owe you favors.

Eventually, I started moving all of the Commodore 64's from the English Dept. into my private room. Nobody seemed to care, but they knew where the computers were going. I set up all of the machines and ran a BBS out of the school. Technically, I ran 9 different self contained BBS's, but I consider it one BBS after I devised a way to allow each of the computers to communicate with each other through primitive means. In essence, I created a chat board out of 9 Commodore 64 machines, running my own BBS software. There were no file transfers, only message capabilities, both public (forum style, or "message base" to the old school) and private (email style - but we did not call it "email"...yet).

After a short time, other various electronic devices ended up in the electronics room, waiting for me to pack it away. Yes, I got all of the Apple II's (and I fixed them). Somewhere along the way, I became the school's resident computer expert and had teachers asking me for advice on programming and troubleshooting. That was kind of cool getting that kind of recognition, but it ate into my time to create and explore which was a downer.

One day during my Sophomore year, two pallets of old IMSAI computers were delivered to the school as a donation. They were in my hands within minutes. I was called out of my math class by the dean of students and he took me to my surprise gift. Hell, I was thrilled beyond belief! These machines were fully loaded and came with all the peripherals, including acoustic modems and "voice boxes" (voice synthesizers). I still have these computers in my own personal collection to this day. That was one of my more memorable experiences in high school.

So, you know I had to dive into that intercom system. In a word: FUN. I was able to listen to ANY room in the school without them having any clue they were being monitored. Interestingly enough, verbal quiz's were quite easy to listen in on. Aside from that, the only other entertaining thing was talking to a class and hearing their disbelief when they realized we could actually have a conversation through the intercom system. The system was quite sophisticated and totally underutilized.

With the help of my electronics teacher, I was able to get free commercial samples of all sorts of equipment. Everything from test gear and tools to computers and entertainment equipment. Back then, you could do almost anything with the right letterhead! Later in life, this very experience allowed me to create a loss prevention program for a well known manufacturer. Apparently, they were getting duped out of a lot of commercial samples and thus, losing "millions". That was an easy gap to close up for them and for what they would have considered a very, very small cost. Yeah, I know what you're thinking. But, I'm one of the good guys, so I had to use my skills for the greater good.

I bet you're wondering about that attendance computer, huh? Well, if you're thinking "Ferris Bueller's Day Off" you're not too far off....and it was that easy! People may look back at that movie and think, 'no way, it's not that easy"... They would only be half right because it was easier. Since the school kept no paper records, they couldn't go back and compare, a la Rooney. Speaking of vital school computer systems, even the grading system was vulnerable on several points. From a completely social engineering aspect alone, there was a major problem. The teachers were assigned to give out grades which they did in the form of "grading sheets". They used pencil! These sheets would end up under lock and key (uh, yeah, the same master key!!) and they had unsecured blank grading sheets available from any number of sources throughout the school. They had someone, usually a computer user from attendance, go through the sheets and enter in all the grades, one by one. This was done at a machine that was in fact "wired" in the form of a dialup modem. Bad, bad. You can use your imagination based on the information above. It was a very imperfect process.

I have to admit that one of the most interesting rooms I explored at my high school, didn't have the least bit to do with technology. It was the groundskeepers room. I guess it was like a janitor room, but bigger and had more equipment (ie: ride around lawnmower, mini electric cars, etc). What was interesting was the stash of confiscated goods that were kept in this room. Think back to when you were 15, 16 or 17 and in high school. What kind of crazy things did you bring with you that ended up getting taken away? Well, if you can think of it, it was probably in this room as well. I had hours of fun looking through all of the interesting items. For the record, I never took (or borrowed) any of it.

During my Junior year of high school, I was a third year electronics student (the only one) and I was given complete and total immunity over every assignment in class. I was dropped into the same classroom with first and second year students and since they had no curriculum for third year students, I was able to just wander around and do whatever I felt like doing. This was the same year I met in that classroom who was to become my best friend. I was able to get the teacher to cut my buddy some extra slack as well so I had someone to help me explore the school.

This year was particularly fun for me because I was able to try out my more elaborate projects on many new and unwitting students who wanted to hang out with the guy who had all the connections. For some reason I was fascinated with high voltages that year. I made the standard Van De Graffe generator, a Jacobs Ladder, a Tesla coil and a large assortment of other gizmos who's sole purpose was to generate high voltages and discharge them in various manners. Many people suffered through my endless pranks.

During these high school years, I was doing much more than hanging out at school, but it was such an important learning experience, I seem to be focusing on the school aspect alone. Aside from school activities, I also took the time to go from building to building in my city to explore utility closets which was a whole experience by itself. Many technicians managed to leave behind tools, wire, fittings and notepads which I gladly collected. This is about the time I discovered what was referred to as a "hot drop". I also explored many office buildings, disassembled elevator control panels, located security rooms and went on ride alongs with the police, paying close attention to their communication devices and computer systems. Nice!

I also revisited my earlier fascination with fireworks and applied new ideas I had come up with over the years. The first thing I devised was a magnesium "flare". Getting the powered magnesium hot enough to ignite was tough enough. I then refined the mixture to magnesium power and "rust". I was working towards making a batch of thermite. I was somewhat successful in my experiments, so I took notes and kept working. I then set my sights on making a bigger and badder smoke bomb. I'll have to admit to a complete success on that project. I then moved to rocket propellants. First it was solid rocket propellant which proved to be a capable (and non-messy) solution to model rocketry (which I was way into). This was a lot of trial and

error, all the while taking notes so I could adjust the ratios for the next batch. The I moved to liquid propellants. Myself and three buddies constructed a 15ft long model rocket which ran on liquid fuel. We launched it out in the desert. The fist mix produced a dead on, powerful thrust.....and we never saw the rocket again. We supplied liquid fuel to many of the local model rocket enthusiast for years until they figured out how to do it themselves. It was only a matter of time, so we saw it coming.

The model rocketry spurred an interest in telemetry and wireless communications. I picked up a dead cordless phone at the local swapmeet and turned it into a "portable phone" which I carried around in a small briefcase. The inside of the case was a very refined looking product, finished with a brushed aluminum panel and a nice keypad mounted to the panel, with a handset from a regular corded phone installed. Under the panel, was the original cordless handset circuit board, Frankensteined into a monster high power transceiver. I had greatly extended the already hefty power of both the base and the headset to allow communication over a greater distance, but the look on the faces of my friends when I opened that case and pulled out a handset and got a dial tone made it worth the time and effort. The official (and tested) range of my design was 5 miles, give or take depending on large buildings.

From that, I moved onto high power covert listening devices (ie: bugs). I made a few different versions, the last one working just above the normal FM radio band. I took an old Sanyo portable radio and adjusted the range up enough so it was capable of receiving the signal from the bug. After messing around with this, I quickly lost interest in it and moved to lasers. I was interested in modulating audio/video on a laser beam over great distances. I was able to get the audio modulated, transmitted and receive with little trouble. The video was a bastard to work with, but I was able to get it done eventually. It was exciting for only a short time.

It was the lasers that turned my attention to surplus electronics and sent me off in a whole new direction. I suddenly found that I could get mounds of electronic components for less than wholesale. Which, of course, fed my need to constantly build projects. I found this awesome place by the name of "ECSC" which I see advertised in Blacklisted! 411 and became fast friends with the owner, Barry Gott. He was happy to reveal many other similar places to that of his own which also had much in the way of electronic surplus.

With all of this surplus electronics all around me, I dove head first into microprocessor technology, microcontrollers, embedded devices and automation. I had always been heavily involved with these fields, but now I was in the market to build something new and interesting. The first thing I constructed was a automation device that inter-connected phone, central air/heat, lighting and alarm system to my home computer. However, the unit would operate stand-alone on a 68000 microprocessor.

I went on to many other hacks, including building devices for my then brand new Amiga computer. The Amiga computer as well as the Commodore 64 computer were great learning platforms. I think some of the best hackers in the world got their start with those ancient machines. Since there wasn't much processing power or available memory, power users were required to be resourceful and creative. We created our own peripherals if one wasn't commercially available. A perfect example would be the lack of a rock-solid multi-serial board for the Amiga. Yeah, the A2232 eventually came out but it was a huge disappointment at best. Before the A2232 8 port cards ever came out, I had already managed to design, prototype and run off a limited batch of 16 port high speed serial cards. The local BBS operators were thrilled to get their hands on one of these babies. I believe this creation spurred the local chat board phenomenon. Eventually, Comports made an offering which was pretty solid, but had some issues. GVP came out with a two port version which was too little way too late, but still greeted with open arms considering the fact a Comports board was nearly impossible to get ahold of. Eventually, I revived my BBS and moved it up to the Amiga platform, at the same time relocating it to my home. I got a copy of CNET Amiga and started modding it until you couldn't even recognize it. I tweaked it into a killer chat board.

Anyhow, as you can see, this time of my life, I was really jumping into technology, getting my hands dirty creating new devices and modifying other existing items. I was exploring my surroundings and making everything work for me. The best part was learning to network with people to get the things I needed to make my ideas take shape.

I'd have to say that high school was a monstrous social event for me. I honed my people skills down to a science and learned the ropes with regard to doing things in plain sight without being noticed. In essence, I was taught the evasive art of social engineering without even realizing it at the time.

In fact, all of my social engineering allowed me uneventful and overlooked access to the school's pool during the summer, late at night after the school was closed. I was allowed a certain number of "guests" to join me. It was greatly appreciated. However, it also allowed me the opportunity of exploring the school even more so, but completely without any supervision whatsoever. This was the real treat that gave me the access I had been waiting for. Armed with my key and a good sense of direction, I quickly explored that school inside out. There were no more secrets to be learned at that point, so I used my knowledge to nestle myself in good with the staff, the students and anyone else who passed by. It really was a learning experience, social as well as technical, that prepared me for real life situations.

In the next installment, I'll take the reader on a tour of my experiences from my college years on up. Standby.

What the hell is a baud anyways?

A look at BBSes and how it's a resource for your Amiga!

By MobbyG

Many of us old timers remember BBSes. The community feeling, the discussions, BBS user get togethers, file leaching and more. For those of you that don't know what I'm talking about, I'll tell you what a BBS is, a little on how it works and how it can be a resource for your Amiga.

What is a BBS

BBS is short for Bulletin Board System. Back "in the day", before the internet, computer users and hackers allowed other users and hackers to call their computers using their modem to post messages and software as well as upload and download files at the blazing fast speeds of 300 bps or better. Basically they were self contained intranets. Some were even members of message networks, which allowed them to send messages to other BBSes using Fidonet, a store and forward messaging system. Now a days, BBSes are not as popular thanks to the internet, but they're still very much alive and kicking and still a good place to meet up with current and past Amiga users for info and software.

Message Bases

Just about all the BBSes that ever were had message bases. Much like the web forums we see on many websites, they allowed you to post a message and reply. If the message bases had a high amount of traffic on them, some BBSes would allow you to bundle up the messages in a format called QWK or Bluewave, and allow you to read them offline using a mail reader that supported that format. One for them Amiga was AmiQWK, which you can still download on Aminet today.

It isn't hard to find someone that used to or still has an Amiga and is more then willing to talkbout their adventures using one. Many are still very knowledgeable about Amigas and will be more then happy to answer questions and share info. You might even be able to get older software from them (We'll also talk about that in the files section of this article). In the past few weeks on my BBS, Amiga-Z, talk has been around running the CNet BBS software in an emulated Amiga using WinUAE. Myself and a fellow sysop, Black Phantom, have done a lot of work compiling info on doing this. Even to the point on getting help from the WinUAE developers to get the smtp daemon for CNet running under WinUAE. Other info you might gleen from someone in a BBS message base is current contact info for developer of an old program you used to use a lot. Or find someone that has managed to get another program running where you have been having nothing but problems.

Files and Software

Maybe there was an old program you loved, but you just can't seem to find it on Aminet or your old Fred Fish discs. I have from time to time, found old doors and programs that I used that are no longer available anywhere, but someone has managed to find a copy on an old floppy or hard drive and posted it to a few BBSes. I myself recently got a copy of a program I needed to run a door on my BBS. You could also find original software that a sysop or another user wrote, only on a BBS, that may work better then something you already have or could find on Aminet.

Text Files and E-Zines

Maybe you remember an article you read in an e-zine like Amiga Report. Some BBSes have old copies of e-zines and text files for you to read and download. Or even, files with recipes from Chili to home-brew beer. I myself first read the Anarchist's Cookbook on a BBS called RIPCO in Chicago, along with a slew of other informative textfiles. If anything, now days, they prove to be great reference items. If you like writing, you could always whip something up and post it. Or even update an old article or text file and post it for others to learn from. With a little digging, you can find some real hidden treasures that can take you back in time or even motivate you to update the information and teach someone else what you have learned.

Doors and Games

Perhaps the main draw of BBSes was and still is, the doors or games. I've received many requests for me to put old games that users could play that they used to play all the time, such as Hack & Slash, Lords of Irongate, Tradewars or even the old infocom text adventures. While you won't find a lot of info in the game section of a BBS, it is a good time waster if you're grabbing messages from message bases using AmiQWK or something like it.

Modern BBSes

Many current BBSes have the ability to be connected to the internet. For some that is the only way to connect to them while others can still be dialed up on a landline. Most allow you access to other internet services such as IRC, FTP or even WWW using a console-based browser. Some, like mine also offer usenet newsgroup access.
There are instances of BBSes becoming full-blown ISPs. Bluemoon BBS, run by the famous door coder, Dotoran, has turned his BBS into a full-blown ISP, as well as Moonstar in Virginia. So you could say that BBSes help make the internet more of what it is today.

Where to find a BBS

BBSes are pretty easy to find now days. Using our old friend Google, I have found many webpages about BBSes but for some reason many are very out of date and the BBS inaccessible. But in the last few months, a couple sites have started up that help you not only find

BBSes, but if you were a user on an old BBS and would be interested in finding old friends from them, you can. The first one is *BBSFINDER.COM.* This site let's sysops list their BBS while they are up and active using a client they can download and install. At last look, there was about 14 BBSes up and active, 2 of which were Amiga BBSes, one being mine (Shameless plug I know).

The other site where you can find old BBS friends is *BBSMATES.COM.* Here you can find old BBSes and new ones for that matter, that you were a member of sign-up on their list. You can also find currently active BBSes in their listings as well.

And another site you can visit for a list of telnet accessible BBSes is *DMINE.COM/telnet/.* You can find about well over 200 BBSes, but I can't say as to how up to date this list is. I have found a few that were down, but for the most part finding one that is still active shouldn't be a problem for you.

Even though most of this information could work for either PC/Mac or Amiga, it can still be a great source of information for the current Amiga user. Like I stated before, there are still hundreds of old Amiga users that are still out there and more then willing to share their info.

What software to use

If you're currently using a PC with "Winblows", I would recommend a telnet client called MicroTelnet. It displays the ANSI on almost all BBSes beautifully, plus allows you to upload and download using z-modem, which is still used by BBSes. For Mac, I don't really have anything, but would love to hear from a few Mac users as to what they use. I'll soon have access to a Mac so I'll be able to try them out and print an update in a future article. Amiga users, AmiTelnet or even an old copy of JrComm works great!

Conclusion

So hopefully, I piqued your interest in either getting back into the scene or maybe exploring it and becoming a member. I think if you try it, you'll see what the interest was about and how addicting it was, or better yet, want to start one up yourself. If anything, it's a great way to remember the early days of hacking.

Hey! I need your help!

For future articles, I want to write about the new OS4 and Amiga One. But with the cost being kinda high right now, I can't afford one. So I'm asking for your help. Please visit my BBS' store and support me by purchasing something from it. You can visit my store at http://www.cafepress.com/amigaz/ . Or if nothing tickles your fancy, but still want to help by making a small donation, visit my website at http://www.amigaz.org and click on the PayPal button and make a small donation.

(My BBS store and website is in no way affiliated with Blacklisted 411! Magazine.)

MobbyG is also know to radio listeners in the Rapid City, SD area as Rich Lawrence, on Classic Hits! Q92.3 and their sister station Star 106.3. When not on the radio he's been known to play on his ham radios and runs a telnet BBS

Editors note: This article really hit home. Anyone who was with us back in the early years of the magazine will undoubtedly recall the infamous BBS "meets" (that would be a kick ass hacker party to the new breed of hackers) we used to host. Those were the days.

CYBER EXTORTION & BLACKMAIL: THE NEW FRONTIER

BY: THE GOLDFINGER

Remember when things were simpler? Back in the day, when a gangster or criminal type wanted to extort money from you, he would show up at your place of business, and threaten to burn down the building, or chop off your employee's digits until you coughed up his cash. Weekly payment that is, this is extortion afterall. Gotta keep up with those payments don'tcha know? Yea, things were more personal back then.

You could see up close and personal the guy that was giving you a hard time, and probably gonna rob you regardless. Not anymore.

Its no big surprise that crooks have migrated on-line. Black hat hackers have been conducting their misdeeds on line for some time now, what is surprising is who else is getting on-line now.

Organized crime syndicates like the Russian mafia for one. They realized that the internet is a vast landscape where they could ply a trade that was once limited by geography. The internet has opened up criminal enterprise in ways not seen since the wild wild west. Extortion and blackmail are nothing new, its just a new twist on an old crime. Now instead of "reaching out" and extorting money from say 10-20 local businesses, you can bulk mail your threat to 100,000 or 1,000,000 companies...or why stop there? *How big are your cyber-coolyons anyway?*

The new threats go something like this; "Pay up or we'll destroy your site." The most common and effective ploy being used by these criminals is the threat of a distributed denial of service attack (DDoS), which can take down a site by bombarding its servers with emails from a network of PCs all breached by a Trojan. If the flavor is more of the blackmail variety, its more like this, "Pay me X amount of dollars, or I'll sell your data to someone else", or "pay me, or I'll install child porn on your pc", or "pay me, or I'll delete your files." Experts say it usually starts with a threatening email in which the author claims to have the power to take over a worker's computer through a loophole in the corporate network.

The email usually contains a demand that unless a small fee is paid, the blackmailers will attack the PC with a file-wiping program or download images of child pornography on to the terminal.

Police however warn if a person pays the small amount, the blackmailers may simply demand more. It depends on who is being extorted or blackmailed. The crooks will tailor the threat to maximize effectiveness. For example, last October, blackmailers warned UK-based on-line bookmaker Blue Square http://www.bluesq.com to pay 7,000 euros or they would send out emails in Blue Square's name containing child porn.

The threat followed a more traditional denial of service attack, taking Blue Square's site down for five hours. The email was sent to Blue Square by a 'Bohan Krascevic' from a Yahoo! web email address with a '.se' Sweden suffix. It stated: "You have time until 5 Pm your local time. I will now start an attack for 1 hour. This will be 1/20 of the power I can do. Answer me and I will give you my e-gold account number which must be funded ASAP, 7000 EURO. Waiting for answer."

The CTO at Blue Square, Pete Pederson said the latest threat ups the ante from the traditional denial of service attacks.

"The thing that has distinguished this is the seriousness of the threat. He's threatened to send mass email containing child porn from Blue Square accounts. That changes the stakes of these things from being apparently financial extortion to something that has a different kind of impact," he said.

The NHTCU (The UK's National Hi-Tech Crime Unit) arrested three suspected ringleaders of one of the online extortion gangs in Russia earlier this year, confirmed this is a new tactic being used by the criminals. A spokeswoman for the NHTCU said: "We are investigating it. It is not a threat we have seen before."

Earlier this year, hackers targeted online bookie William Hill with similar demands.

"We did have a DoS attack, but we don't know where it came from," said a spokeswoman for William Hill. "We are building in software to prevent this, but it's a technology game.

The NHTCU is aware and we've had quite a good relationship with them in the past."

The director of research for security organization SANS said that every online bookmaker was receiving similar denial-of-service threats. The crooks struck on the eve of the Cheltenham Festival, a big horse racing festival, one of the biggest betting weeks of the year. Britain's second-biggest betting chain was hit by a barrage of data which disrupted its gambling website on March 11. Police and security experts say organized crime is behind the growing crime wave, which typically intensifies in the days leading up to big sporting events. The culprits targeted a variety of sites before the Super Bowl in January, each time demanding money or threatening to take out the sites with a crippling data barrage. "The level of intensity is higher than any we've seen before. They are increasing the force and frequency and sophistication in these attacks," said Richard Starnes, director of incident response for Cable & Wireless. (UK)

Many ISPs are working with victimized sites and law enforcement to track down the culprits as larger and larger sites are being taken out for longer periods, experts said.

Both police and security experts believe gangs in Eastern Europe and Russia could be behind some of the attacks. William Hill's Sharpe added that after the attack the company received an email the following day demanding $10,000 to avoid a repeat. "We had and continue to have no intention of dealing with demands made by blackmailers," he said. He added the extortion demand made no mention of the Cheltenham festival as a reason for the attack. He added, to his knowledge, it was the first time the site was hit. The race festival attracts high-rolling gamblers who fearlessly take on the bookmakers with stacks of cash. On the course alone, ££2m pounds are bet on every race. On the net, the betting is just as high. Online betting has been an important new growth area for high street gambling firms such as William Hill and Ladbrokes, plus a bunch of new dot coms that have emerged to pounce on the market. www.Betfair.com, one of the world's largest online gambling operations, takes in more than ££50m pounds per week in betting volume. "This is probably our biggest week," spokesman Hugh Taggart said.

A sustained outage could cripple a young betting site's business operation for the year, and deflate a multi-billion-pound business sector still trying to establish the public's trust.

The crime wave, which dates back at least three years, has yet to yield any arrests.

Part of the problem with these kinds of crimes is that its almost impossible to gauge the full extent of the problem, because many companies would rather pay up and avoid the negative press which their case might attract if they reported it to police - and shareholders.

Cyber extortion attempts, once the industry's dirty little secret, is now being reported to the police more often which will increase the odds of arrests.

Neil Barrett, technical director at Information Risk Management, who is an advisor to the UK police on high-tech crime, said: "Nobody knows the full extent of this problem. There has certainly been a significant increase in the number of denial of service attacks and the only sensible reason would seem to relate to extortion." Barrett highlighted the problem of non-disclosure, stating that many companies may opt to comply with "pay up and don't tell the police"-style demands. He said among the sites targeted previously include internet gambling sites. But in theory any company conducting cash transactions with clients or customers is a target - criminals know many will look upon paying the ransom as the lesser 'evil' compared to running the risk that clients lose faith in the sites security. As for who is committing these crimes, Barrett is convinced its not a new breed of criminal.

"It's the same criminals, just with new tricks," he said, stating that previous investigations have implicated the Russian mafia. Who else is getting in on the act? Brazil and Romania.

When I think of Brazil, I think of miles of beaches, blazing hot sun, and bronzed babes clad in thongs swishing and shaking thru the sand as I heft another tropical drink to my mouth and, ah... *oh yea*, cyber crime, sorry, got lost in the image. It seems Brazil has become a hot-bed of cyber criminal activity. Brazil is currently the global capital for online hacking and fraud and is home to eight out of 10 of the world's hackers. whoa. Brazil loses more money to Internet financial fraud than through bank robberies, and *two-thirds* of online child pornography is said to originate in the country. For about the past two years, Brazil has been the most active base for shady Internet characters, according to mi2g Intelligence Unit, a digital risk consulting firm in London. Last year, the world's 10 most active groups of Internet vandals and criminals were Brazilian, according to mi2g, and included syndicates with names like Breaking Your Security, Virtual Hell and Rooting Your Admin. So far this year, nearly 96,000 overt Internet attacks - *ones that are reported*, validated or witnessed - have been traced to Brazil.

That's more than six times the number of attacks traced to the runner-up, Turkey, according to mi2g. The authorities hands are somewhat tied since legislation dating back to 1988, well before most brazilians even heard of the internet, states that a hacker cannot be arrested

merely for breaking into a site, or even for distributing a virus, unless they can prove the action resulted in a crime. Police there have their hands full with violent crime in cities like Sao Paulo, Rio, and Brasilia, and keeping up with hacker gangs is difficult. Sao Paulo has about 20 officers in their electronic crime division and they bust about 40 suspected cyber crooks a month. Those cases only account for a small fraction of the ever increasing number of cybercrimes.

The country is becoming a laboratory for cybercrime, with hackers specializing in identity and data theft, credit-card fraud and piracy, as well as online vandalism. Across the globe, hackers like to classify themselves as white hats (the good guys) or black hats (the bad guys), said a Brazilian expert, Alessio Fon Melozo, editorial director of Digerati, which publishes a hacker magazine, H4ck3r: The Magazine of the Digital Underworld. "Here in Brazil, though, there are just various shades of gray," Melozo said. "They say they have their own security and prefer to turn a blind eye," he said. "But Brazilian hackers are known for our creativity. If things go on like this, there'll be no more bank holdups with guns. All robberies will be done over the Net." Although the cost of owning a PC is difficult for most people in Brazil, getting information about hacking is easy. H4ck3r magazine, available at newsstands, sells about 20,000 copies a month.

And then theres Romania. Law enforcement documents obtained by The Associated Press portray a loosely organized but increasingly aggressive network of young Romanians conspiring with accomplices in Europe and the U.S. to steal millions of dollars each year from consumers and companies. Their specialties: defrauding consumers through bogus Internet purchases, extorting cash from companies after hacking into their systems, and designing and releasing worms and viruses.

"Frustrated with limited employment options offered in Romania, some of the world's most talented computer students are exploiting their talents online," the U.S.-based Internet Fraud Complaint Center, run by the FBI and the National White Collar Crime Center, says in a new report. Computer crime flourished in Romania because the country lacked a cybercrime law until earlier this year, when it enacted what may be the world's harshest. The new law punishes convicts with up to 15 years in prison - more than twice the maximum for rape. Dam. That is harsh. Too harsh if you ask me. Thats messed up on more than one level. How is a computer crime more serious than rape? It just goes to show you that at this point in time, a crime of finance; read MONEY, is more important than a person or a persons welfare. A truly f'd up state of affairs, but I digress, the new law is tough on computer crime. Concerned with the nation getting a bad online rep, Varujan Pambuccian, lawmaker and former programmer helped to draft the new law in an attempt to speed up efforts to join the European Union by 2007. "We want a good name for our country," he said. "I'm very angry that Romania is so well-known for ugly things - for street dogs, street children and hackers." Pambuccian said there was a noticeable decline in criminal activity in the first three months since the law took effect. Well no shyt. With those kind of consequences, hackers better think long and hard, or they'll be learning new meanings for long & hard. No pun intended. (ok, pun intended) More than 60 Romanians have been arrested in recent joint operations involving the FBI, Secret Service, Scotland Yard, the U.S. Postal Inspection Service and numerous European police agencies. Although the Russians are better known for online extortion, Romanians have become major players in the scam, as well as by criminals from Bulgaria, Poland and Slovenia.

Information technology is a Romanian forte dating to the former regime, when the late dictator Nicolae Ceausescu saw computers as a way to advance communist ideology. Software piracy took hold during the Cold War era, when Romanians too poor to buy licensed software simply copied it. Today, Romanians get their first computer lessons in nursery school. Universities have top-shelf IT programs whose graduates are heavily recruited by Western companies like Microsoft Corp. But all that know-how has spawned a dark side: Internet sheisters who prey on victims half a world away.

The classic scam: Offer high-end electronics or other goods for sale or auction, take the order, confirm the "shipment" - and simply vanish the moment the consumer has wired payment. The Internet Fraud Complaint Center said it gets hundreds of complaints daily from

defrauded Americans. Many cases trace to Romania, where crooks use Internet cafes to prevent tracing them back to their own pc's. Some have developed Web pages that look like legitimate sites such as eBay, diverting them into the cyberspace equivalent of a back alley. Buyers think they're dealing with eBay, but their money ends up in dirty hands and the goods are never shipped.

The boldest hack into protected corporate databases, where they copy proprietary information and demand cash on threats of publishing the findings on the net. This past summer, authorities aided by FBI experts arrested six young Romanians in the Transylvania town of Sibiu after they successfully extorted $50,000 from several leading American corporations, which were not identified.

With all this scheming and scamming going on, you would be right in assuming the Feds were gonna get involved, and in a big way. **Operation Cyber Sweep** made arrests or convictions of more than 125 individuals and the return of over 70 indictments in a coordinated nationwide enforcement operation designed to crack down on the leading types of online economic crime.

Criminal schemes included in this initiative include: International re-shipping schemes, auction fraud, spoofing/phishing, credit card fraud, work at home schemes, cyber-extortion, Intellectual Property Rights (IPR), Computer Intrusions (hacking), economic espionage (Theft of Trade Secrets), International Money Laundering, Identity Theft, and a growing list of ""traditional crimes"" that have migrated on-line.

Taken from press release:

*"The ongoing operation, known as **Operation Cyber Sweep**, was coordinated by [35] U.S. Attorneys' offices nationwide, the FBI, the Postal Inspection Service, the FTC, the United States Secret Service, and the Bureau of Immigration and Customs Enforcement, together with a variety of state, local and foreign law enforcement agencies. "The operation targeted a variety of online economic crimes that involved schemes including fraud, software piracy and the fencing of stolen goods. The investigation exposed the ways in which economic crimes are becoming increasingly global and multijurisdictional in nature. "Online criminals assume that they can conduct their schemes with impunity," said Attorney General John Ashcroft. "Operation Cyber Sweep is proving them wrong, by piercing the cloak of anonymity that the criminals adopt and prosecuting them in whatever jurisdictions their schemes may affect." "More than 125 investigations have been opened since Operation Cyber Sweep began on Oct. 1, 2003. Investigators have uncovered more than 125,000 victims with estimated losses of more than $100 million. More than 90 search and seizure warrants were executed as part of the operation, and prosecutors have obtained more than 70 indictments to date. The charges have led to more than 125 arrests or convictions."*

And more recently, **Operation Firewall** busted another ring of hackers and various cyber crooks in another global sized operation of epic proportions. Its obvious to me and should be obvious to anyone pursuing on-line crime, the feds are on it, and they have new agreements in place with countries all over the world to co-operate, and jointly prosecute anyone in their jurisdiction found to be committing these types of crimes. If theres money to be made, on-line or off-line, the crooks will find it. And if there are people making money, getting rich, and not paying taxes, then you can be sure Uncle Sam will be stepping in to take his bite of the pie. Just follow the money trail, you'll find cops & robbers doing what they've been doing all along, now its just on-line, the same old game, with a modern twist.

The Goldfinger is also known as Detroits only Octopus-wearing rapper; Mr.Scrillion aka Adam Thick, Mastermind behind Extremekidnapping. The Goldfinger has more than a decade of underground knowledge and experience under his belt, a former social engineering hacker, and when not Rapping & Kidnapping, he is scouring the underground, the black market, keeping his ear to the streets for the rawest and most up to date insider information available.

Visit www.scrillion.com & www.extremekidnapping.com
Coming Soon! www.lapdanceolympics.com
Holla at him > goldfinger@voyager.net

A new Style for Windows XP

by Robert Peloschek aka MacOS X

You are bored of the three old Windoze XP styles and don't want to use crappy 3rd party "XP style" software to change the look of your Windows Installation? Well, I guess I have a solution for you…

Since 10/11/2004 Microsoft offers the new "Energy Blue Theme Pack" for Win XP Tablet PC Edition 2005 on *microsoft.com/download* for free. All you have to do is to download *[1]* it to your hard disk and install it following the instructions in this article.

You may ask why you can't install the Theme Pack on XP Standard or Pro by simply using the installer Microsoft provides. Well, that's because M$ seems to penalize "normal" XP Users. If you try to install the Theme Pack using the original Microsoft install routine the only thing you get is the error message: "The Energy Blue Theme Pack can only be installed on machines running Microsoft Windows XP Tablet PC Edition 2005". So what you'll have to do to get this friggen theme workin' is some manual work.

The first thing you have to do is to extract the content of the install file. To do this go to "Start → Run", type in "*C:\WindowsXP-TabletPC-EnergyBlueTheme-x86-ENU.exe /x*" (I assume the install file is lying directly on "*C:*") and extract the content into any directory you like (for example "*C:\New Theme*").

Now that you have the extracted files, you have to create some new folders (and subfolders) in "*C:\WINDOWS\Resources\Themes*":

- \Royale\
- \Royale\Wallpaper\
- \Royale\Shell\
- \Royale\Shell\Homestead\
- \Royale\Shell\Metallic\
- \Royale\Shell\Normalcolor\
- \Royale\Shell\Royale\

Next you have to copy the extracted theme files (from your "*C:\New Theme*" folder) into the new created folders in the Windows directory.

First copy "royale.theme" into "*C:\WINDOWS\Resources\Themes*". Then copy "royale.msstyles" into the "*\Royale*" subfolder. Next copy "energybliss.jpg" into the "*\Wallpaper*" subfolder. And last but not least you have to copy the "shellstyle.dll" into all "*\Shell*" subfolders ("*\Homestead*","*\Metallic*", "*\Normalcolor*", "*\Royale*"). That's it. ☺ Time to check out what you have done…

Simply go to Start → Control Panel → Display, select "Energy Blue" from the Theme drop down box, and enjoy your new XP style (***Fig 1***).

***Fig 1**: Win XP Royale Style*

Links:

[1] http://www.microsoft.com/downloads/details.aspx?FamilyID=86268ffa-70b1-4814-bd00-2d380dc5a89d&DisplayLang=en

Shout outs: … all fellow Hackers who help to keep the Underground strong …

Securing Grub

Written By USTLER

In today's world, boot security is essential. It is the first line of defense for all users that require decent security. In the case of theft, this can be one of the easiest means in preventing a user from accessing confidential information.

To start off we must understand the computer boot process, which is rather simple. When the computer is first powered on the CPU is initialized, then the BIOS(Basic Input Output System) begins POST procedure and then passes the process to the boot loader. One of the most widely used bootloaders for a multiboot environment is the GRand Unified Bootloader, or more commonly known as GRUB. Traditionally distributed with Linux, this bootloader can be used with a multitude of operating systems and hardware configurations. Unlike the windows boot loader, GRUB is more flexible when dealing with multiple operating systems.

Security within GRUB has an important part in secure your PC. Unfortunately boot security is one aspect that is often overlooked by administrators and security personnel. A simple BIOS password always seems to suffice most users, but this is not always the best option. In the following section I will present a layered security model and how each layer plays an important part in today's world.

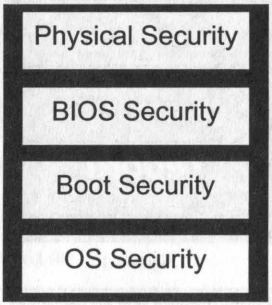


Diagram 1.1

The diagram above displays how boot security should be modeled. In the following section we will quickly go over each layer and its benefits.

Physical security

Physical security is one of the most important aspects of security. Preventing a malicious user from accessing ones motherboard is essential to locking down a box. If one can gain access to the BIOS reset pins or hard drive the security model begins to crumble.

BIOS Security

The BIOS controls one important aspect of security, boot order. This is the order that the PC looks for bootable media during the initial boot process. Although not the only security feature some manufactures provide, this is the most common one. If the BIOS is not secured properly, one could simply boot off of a CD-ROM, or floppy with something like DOS, or Knoppix and gain access to password files and other damaging information. Many laptop manufactures now offer a BIOS password along with a embedded hard drive password. Implementing these can provide a good barrier against unauthorized use of the PC.

Boot Security

Boot Security covers securing the bootloader and its components. For those who have no idea what a bootloader is, it is program that usually lives in the MBR (Master Boot Record) and transfers control to the operating system. Bootloaders like the one that Windows uses by default do not offer any security features or any that compare to what GRUB has to offer. Bootloader security is another line of defense that provides an administrator the ability to limit the bootable OS options and prevent unauthorized users from booting.

OS Security

OS or Operating System Security provides the final and most important layer of boot security. OS Security provides one or more authentication methods to ensure that only authorized users are able to authenticate and gain access to the system and its resources through the Operating System. OS security covers ACLs (Access Control Lists), encryption, and policies used to control user privilages.

Grub Security

This article does not encompass the installation of GRUB, but does cover the configuration and security aspects. In the following sections we will examine GRUB configuration files and show you how to tweak them to further your overall security.

A Quick look at GRUB

Grub has come along way from just being a text based bootloader. GRUB in todays *nix systems include a full graphical user interface along with built in commands for troubleshooting boot problems. For those of you that are unfamilar with GRUB, figure 1.1 shows the GRUB bootloader that is bundled with Fedora.

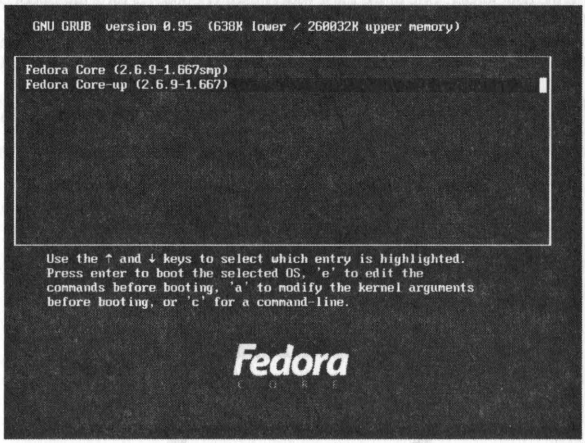


Figure 1.1

As we stated above, GRUB has added many features that go above and beyond what the windows bootloader offers. Figure 1.2 shows GRUB's command line that offers a wide variety of tools and options.

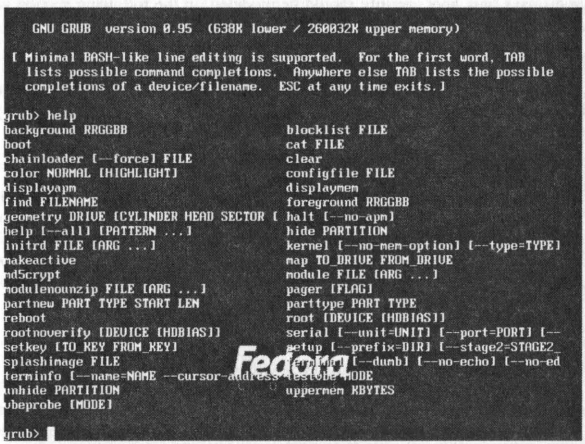


Figure 1.2

GRUB also includes the ability to modify boot options and kernel arguments without having to boot into linux to modify the grub.conf file. Figure 1.3 shows a Fedora OS ready to be edited before we boot

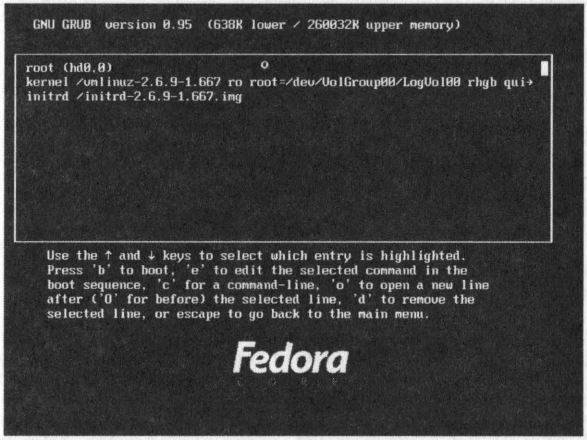


Figure 1.3

As you can see, GRUB is no longer a simple bootloader, but a flexible tool used in a multiboot environment. Although this flexibility adds functionality, it also creates a huge security hole as we will see later.

Introduction to grub.conf

Grub.conf is the main file that grub uses to define Operating System choices and bootloader settings and resides in /boot/grub/ . Menu.lst is not a configuration file for GRUB, but rather a symbolic link to grub.conf. (Common misconception)

Let's take a look at a standard GRUB config file

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this #
file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,2)
#          kernel /vmlinuz-version ro root=/dev/hda5
#          initrd /initrd-version.img
#boot=/dev/hda
default=1
timeout=20
splashimage=(hd0,2)/grub/splash.xpm.gz
hiddenmenu
title Fedora Core (2.6.9-1.681_FC3)
            root (hd0,2)
            kernel /vmlinuz-2.6.9-1.681_FC3 ro root=LABEL=/1 rhgb quiet
            initrd /initrd-2.6.9-1.681_FC3.img
title Windows XP Pro
            rootnoverify (hd0,0)
          chainloader +1
```

This is the GRUB configuration file from my laptop. In the following section, I will cover each option, explaining its main purpose.

Default = 1 ← This option sets the default OS.
Since grub starts counting with zero, Windows XP Pro would be default OS.

Timeout=20 ← This sets the default timeout. This is timer before GRUB boots to the default OS.

Splashimage=(hd0,2)/grub/splash.xpm.gz
The above sets the splash image that is used in the GUI. Note it is in gz format.

Hiddenmenu ← This option hides the menu from a dumb terminal, and waits to boot to the default target.
Title ← Defines the title of the boot option
Root ← Specifies the root partition which would be hd0 partition 2
Kernel ← The kernel is location
Rhgb ← This option is passed to the kernel and tells it to boot via the graphical mode.
Initrd ← This is the RAM disk that the Linux kernel uses

The Windows XP Pro is rather self explanatory.

Rootnoverify ← Specifies the root directory but does not attempt to mount it.
Chainloader ← This simply hands the boot process over to windows.

This is a typical dual boot configuration file with no security settings implemented. Now that we stepped through the regular configuration lets start by adding a password to prevent unauthorized users from accessing the GRUB's options menu. This prevents a malicious user from modifying arguments that could allow a user to boot into single user mode or change the boot partition/drive. To do this, we must encode the password that we want to use using md5. Grub includes its own password creation tool called grub-md5-crypt which we will use in the following example. Please note that the grub-md5-crypt program is located in /sbin/ and is only accessible by root. The following example escalates a standard user's privileges and creates the password "mypass".

```
Sh-3.00$ Su ñl
Password:
Sh-3.00# grub-md5-crypt
Password:
Retype password:
$1$Q5lWi0$P.7z9OmKbTDt52cTFXCZa.
```

Now that the password is created, we can insert it into the grub.conf file. To do this open grub.conf up and insert the following before the first title statement.

```
password --md5 $1$Q5lWi0$P.7z9OmKbTDt52cTFXCZa.
```

Example:

```
default=1
timeout=20
splashimage=(hd0,2)/grub/splash.xpm.gz
hiddenmenu
password --md5 $1$Q5lWi0$P.7z9OmKbTDt52cTFXCZa.
```

One important aspect of GRUB security is to provide limited access to different operating systems. For example, if you had a Windows XP installation for your regular users, and a Slackware or Fedora installation for administrators, you could specify the lock command to prevent unauthorized users from accessing it.

```
title Fedora Core (2.6.9-1.681_FC3)
          lock
          root (hd0,2)
          kernel /vmlinuz-2.6.9-1.681_FC3 ro root=LABEL=/1 rhgb quiet
        initrd /initrd-2.6.9-1.681_FC3.img
```

The lock command specifies that only users with the password you specified will be able to boot. To authenticate, the user will need to press 'p' and enter the password.

There is one problem with this setup. If multiple users need to boot to the locked operating system, this setup does not prevent them from modifying arguments in GRUB that could compromise the system. The other option is to add a separate password for each operating system as needed. The following grub.conf example shows a Windows and Fedora operating system, the Fedora OS is locked with an md5 password "fedora", and the menu options are locked with "mypass". This will allow anyone to boot into Windows, but limits the users allowed to boot into fedora.

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this #
file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,2)
#          kernel /vmlinuz-version ro root=/dev/hda5
#          initrd /initrd-version.img
#boot=/dev/hda
default=1
timeout=20
splashimage=(hd0,2)/grub/splash.xpm.gz
hiddenmenu
password --md5 $1$Q5lWi0$P.7z9OmKbTDt52cTFXCZa.
title Fedora Core (2.6.9-1.681_FC3)
                        password ñ-md5 $1$yMnWi0$suM0qj7x77BdWEbkf21yI0
          root (hd0,2)
          kernel /vmlinuz-2.6.9-1.681_FC3 ro root=LABEL=/1 rhgb quiet
          initrd /initrd-2.6.9-1.681_FC3.img
title Windows XP Pro
          rootnoverify (hd0,0)
            chainloader +1
```

But lets say we wanted to the hide a operating system selection from anyone but a small administrative group. Using the password command, we can create a menu that requires a password. While grub.conf/menu.lst is the default for grub, we can specify another menu accessible only by entering a password. Below is the command syntax.

Password --md5 *password* /boot/grub/*mymenu.lst*

To create this new menu, we must first copy the contents of grub.conf. Then we will rename it, and add the Fedora Linux option to our file. The following will demonstrate this

sh-3.00$ su
Password:
sh-3.00# cd /boot/grub
sh-3.00# cp grub.conf admin.lst

The only difference is that the Fedora OS is listed in admin.lst but not in the original grub.conf. As seen below.

```
title Fedora Core (2.6.9-1.667)
          root (hd0,2)
          kernel /vmlinuz-2.6.9-1.667 ro root=LABEL=/1 rhgb quiet
          initrd /initrd-2.6.9-1.667.img
title Windows XP
          rootnoverify (hd0,0)
          chainloader +1
```

Although not a access security feature, a simple disclaimer or warning can inform users that by trying to access unauthorized resources, they will be punished with strict legal actions. We can do this with the pause command. Using the pause command is rather simple, it displays a message the waits for a user to press a key. So if you wanted to notify all users that the fedora OS was for administrators only, you could use the following.

```
title Fedora Core (2.6.9-1.667)
          pause Warning for Administrators Only!!
          password -md5 $1$yMnWi0$suM0qj7x77BdWEbkf21yI0
          root (hd0,2)
          kernel /vmlinuz-2.6.9-1.667 ro root=LABEL=/1 rhgb quiet
          initrd /initrd-2.6.9-1.667.img
```

The example above will display the message and then wait for user input before prompting for the password "fedora".

The last and final aspect of grub security that will cover is the hide and unhide commands. These are useful when you're trying to prevent a Windows PC from accessing another partition. Please note that this is only useful with Windows partitions.

The following example has 2 DOS partitions hda0 and hda1. With the hide command, we will "hide" the other DOS root file system from each other. Please note that if you hide a partition, you must unhide it to use it again.

```
title DOS PARTITION 1
          hide (hd0,1)
          unhide (hd0,0)
          rootnoverify (hd0,0)
          makeactive
          chainloader +1
title DOS PARTITION 2
          hide (hd0,0)
          unhide (hd0,1)
          rootnoverify(hd0,1)
          makeactive
          chainloader +1
```

One last thing to consider is file permissions in /boot/grub for the configuration files. Grub.conf can safely be changed to 600 (Read and Write access), and the owner should be root. This will prevent any users from reading or writing to grub.conf. The rest of the file structure is considerably safe at 644 (Everyone can read and only root can write).

The scope of this article ends here, but a few other things to consider is changing the default grub image file and replacing it with your own customized one. Encrypted disks and other security measures also play an important part in security. Remember that security expands far beyond boot security. Boot security should never take the place of proper encryption, security policies, and restrictions.

INTERVIEW WITH A HACKER

LUCKY225

By The Goldfinger

As part of a new series, I'll be hitting the streets and the web to find hackers and phreakers of all types to interview and find out *who's who*, and who's doing what in the underground world of Hacking. My first interview was with a young cat that goes by the handle Lucky225. I caught up with Lucky and heres what he had to say…

Q: Word on the street is your a hacker. How did you get that rep?

A: I've been playing with phones, electronics, and computers since I was a very young child.

Q: What kind of "hacker" are you?

A: The kind that doesn't believe in labeling. Hackers think differently than most people, they find ways to circumvent systems and how to secure systems so that they can't be circumvented. This usually requires something most people don't have -- Logic, and common sense.

Q: There are many sub-genres or classifications of hackers...how do you > classify yourself? Refer to question 2

Q: What areas of hacking do you specialize in?

A: "Phreaking", telecommunications, telephony, etc..

Q: How old are you?

A: I'm 21

Q: What do you do? (outside of hacking)

A: Nothing, I'm unemployed. My employer fired me for downloading putty, which they seem to think is 'installing software', and they claim I used it to transmit confidential company files to my computer. If I wanted company files, I would have used this thing called a photo copier. Secondly, they wanted to hire me on for their IT department, but I took a different position, the person who DID get the IT position downloaded a copy of putty on every computer in the office. Employers tend not to have logic or common sense.

Q: What do you want to do?

A: Anything that puts a roof over my head. But seriously, anything in the technology, telephony, telecom area I would be pleased with.

Q: Whats the best hack you've done so far? > (It doesn't have to be anything grand, but what was the most fulfilling, or > one your most proud of?)

A: Blueboxing is the most fulfilling 'hack', it's nostalgic.

Q: What was your favorite hacker movie or movie with hackers in it?

A: Wargames and Sneakers

Q: Why do you think hackers get a bad rap?

A: One word; Media.

Q: What do you think about 'black hat' hackers? what hat do you wear?

A: I don't think hackers wear hats. People that commit crimes are criminals, yes some hackers also commit crimes, but intentionally exploiting a system to commit crime is criminal activity, not hacking.

Q: What real life hacker would you like to meet?

A: Lance James and RMS

Note: Lance James is a security expert that's released a couple caller ID spoofing vulnerability advisories. RMS is Richard Stallman.

Q: What's your dream hack?

A: Owning SS7 :)

Note: SS7 is Signaling System 7. SS7 is the signaling system currently used by our phone system

Q: What are you currently working on?

A: Telephone entry systems. www.dkaccess.com -- EVERYTHING IS ALWAYS ON DEFAULT (hint: 9999)

Q: Do you have a nemesis? Any enemies?

A: No nemesis, of course there are always haters, but no real enemies.

Q: Would you rather have the 6 screen super computer as seen in Swordfish, or a Ferrari(or insert your own pimp ride)?
I'd rather have a car, so I could get to the secret layer that contains the 6 screen supercomputer and bone the fuck out when I'm done hacking :P

Q: Tell me about your website and what you offer.

A: www.verizonfears.com Verizown is a socal phreaking group, the website offers information about privacy, caller ID, telephone phreaking, and links to other websites, however at the time of this interview the server is down, but hopefully by time this is in print the site should be back up.

Q: Ever run afoul of the law during your hacking activities?

A: Only once was I contacted by Verizon Fraud department and we settled out of court. One time I called a courtesy phone at the airport (which isn't really hacking), the ones they let people getting off the planes use to get a hotel or rental car, and the recipient freaked out that this phone was ringing, I just wanted to talk to people as they got off the planes, anyways, the guy who freaked out said I was a terrorist, long story short the Ontario Airport police came out to my house and made a report that I was a non-credible threat. The interesting thing about this story is the same day this happened I happened to be moving to Austin, TX the following day, so they asked to search my house and were very curious as to why everything was in boxes, and one of my drawers was filled with telephone equipment and wires, which they assumed might be to make a bomb or something, but I convinced them that there was no threat and none intended in the first place, but supposedly they made a report to the FAA and FBI.

Q: Where are you from,where do you live?

A: Guasti, California 91743

Q: Is there a hacker scene near you, or do you roll solo?

A: There's a scene, but it's underground.

Q: What is a tip/trick you can show the readers about how to hack or > bypass something. (can be anything)

A: As for the trick, sign your freeworlddialup account for Washington state phone number where people can call your FWD voip line direct at www.ipkall.com, your ipkall number will trap CPN information, even if the caller ID is blocked. This means you'll have a Washington state phone number that no matter who calls it you will always know who's calling.

Q: What do you think the future of hacking is going to look like?

A: It will evolve with new technology, just as phreaking has with voip.

Q: Whats something you want the readers to know about you.

A: I'm an open person, I get many emails and instant messages and I try to reply to all of them. If there's something you'd like to know that you think I could help you out with feel free to contact me.

Q: Any final words or thoughts....

A: If freedom is to be outlawed, only outlaws will have freedom.

And there you have it folks. Lucky225 is out there, puttin it down, and you can too… Wanna be famous? Got Hacking cred? Wanna be immortalized in Blacklisted411? *Holla at the Goldfinger!*

If you're a hacker or phreaker that is interested in being interviewed, you can contact me at goldfinger@voyager.net I can't guarantee I'll interview you, but drop me a line, tell me what kind of hacker you are, what you specialize in, what you've done, and your plans, *and who knows?* Maybe you'll be the next "Interview with a Hacker" story. pz an I'm out.

The Black Market

LARGE SELECTION of items of interest to the hacker community. Surplus, stun guns, pepper spray, hobby supplies, electronics, survivalist, spyware, too much to list here. Huge selection of FREE ebooks, Succeed With Women, Guerilla Web Promotion, many others, some for purchase, the cream of the crop. Come check us out! www.hacksupplies.com

URBAN EXPLORATION! Phone obsessions! Pointless conversation! And a slight chance of hacking! It's Doug TV baby http://www.dougtv.org

THE WORLDWIDE WARDRIVE is an effort by security professionals and hobbyists to generate awareness of the need by individual users and companies to secure their access points. The goal of the WorldWide WarDrive (or WWWD) is to provide a statistical analysis of the many access points that are currently deployed. http://www.worldwidewardrive.org/

LOCKPICKING101.COM Open forum discussion to educate yourself and others about lock picking and lock security.

HACKER ART WANTED! We're actively recruiting people to submit artwork to us. We're looking for freehand as well as computer artwork of technology, people using technology, events, devices, utility personnel, utility vehicles in action (or doing nothing at all), tradeshows, technology swap meets and hacker meets, comics, etc. If it's related in any way, we want artwork!! Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

LOOKING FOR HACKERS AND PHREAKERS! We're looking for hackers and phone phreakers to work on a new community based WWW project. If you're interested and would like to know more, email keynet@spoonybard.org or visit http://spoonybard.org/keynet.html

INFOSEC NEWS is a privately run, medium traffic list that caters to the distribution of information security news articles. These articles will come from newspapers, magazines, online resources, and more. For more information: http://www.c4i.org/isn.html

I'M RAFFLING my original APPLE-1 computer I have no use for it anymore so im giving any one who wants a chance on owning a piece of history all I ask is for a one paragraph letter telling me why you would want my computer, and $2.00 cash or money order to: MY RAFFEL, 567 W. channel Isl. Blvd., Port Hueneme CA, 91341 suite 416

HACKERSHOMEPAGE.COM - Your source for Keyboard Loggers, Gambling Devices, Magnetic Stripe Reader/Writers, Vending Machine Defeaters, Satellite TV Equipment, Lockpicks, etc...(407)650-2830

HACKER STICKERS Geeks, Coders and Hackers get your stickers, shirts, hardware and caffeine from www.hackerstickers.com

CELLULAR PROGRAMMING CABLES: For Motorola Flip Series $100, 8000/Brick Series $150, Mobile/Bag: $100 (includes handset jack, the only way to program Series 1). Panasonic and Mitsubishi Cables $100. All cables are high quality, professionally assembled and guaranteed. Guide to Cellular Programming, everything you ever wanted to know, correct wiring diagrams, troubleshooting, etc.: $45. Other accessories and programming software available. Inquiries to: (714)643-8426, orders only to: (800)457-4556. C.G.C.

HIGHLY COLLECTIBLE INTEL 4004 Processors. We have these available in NEW OLD STOCK condition. Ceramic as well as plastic. Ceramic "D4004" $70. Plastic "P4004" $40. Shipping cost of $6 not included. We also have P4001/P4002 support devices available @ $26 each, shipping included. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

GET YOUR FREE AD IN BLACKLISTED! 411 Reach thousands of readers in the US, Canada, Japan, the UK, Australia, and elsewhere. Join our long list of satisfied clients who have made Blacklisted.411 their vehicle for reaching customers. Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

SCANNER MODIFICATION HANDBOOK. Big! 160 pages! More than 20 performance enhancements for PRO-2004 and PRO-2005. Restore cellular, increase scanning speed, add 6,400 memory channels, etc. Step by step instructions, photos, diagrams. Only $17.95, + $3.50 hipping ($4.50 Canada). (NYS residents add $1.38 tax.) CRB research, Box 56BL, Commack, NY 11725. Visa/MC welcome. (516) 543-9169.

HIGH-TECH security/survival books/manuals: Computers, Internet, Phones, Energy, Physical Survival, Financial, Law, Medical/Radionics, Mind Control, Weird/Paranormal. Free Online Catalog at: Consumertronics.net (PO 23097, ABQ, NM 87192), or $3 hardcopy (USA/Canada, $7 foreign). See display.

SIX DIGIT LED CLOCKS (with seconds); AC powered, highly accurate. Several models. Free catalog! Whiterock Products, 309 South Brookshire, Ventura, CA 93003. (805) 339-0702.-9169.

CELL PHONE cloning for the guy who has (two of) everything. Must have current service contract. For more info, call Keith (512)259-4770. 6426, Yuma, AZ 85366-6426.

BUILD A RADAR JAMMER out of your old radar detector. No electronic knowledge needed. Only $9.95 + $2.50 S&H Call 24fr. for easy step-by-step plans. 1-800-295-0953 Visa/MC/Dis.

BOGEN FRIDAY FR-1000 all digital answering machines. An excellent all-purpose digital answering machine with 8 mailboxes (4 announcement only). Has a total recording time of 18 minutes. $52 each including shipping. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

ALL YOUR 802.11B ARE BELONG TO US Unlike any other database system that exists since or during the period of "the collective" (2002), none other has given a return of the entire collective back to the submitter. The collective is not a mapping database system. It is a mechanism to exchange data in a cumulative fashion for such interested parties through anonymous assimilation. http://www.allyour80211barebelongtous.org/

BLACKLISTED! 411 MEETINGS We know some of the diehards kept the meetings going while we were out of print. Thanks guys!! You need to contact us and let us know the details of your meetings so we can list you in the magazine. For everyone else. Would you like to start up a meeting, yourself? It's fun, it's easy and you get a free subscription out of it. Tell us where you want it held and give us a contact name and number or email address. If you want your free subscription, you'll need to provide an address, of course. Think about starting a meeting yourself. Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

SCIENTIFIC ATLANTA 8580 $225, 8570 $250, 8550 $150, 8500 $120. Will program your 8550, 8500 EAROMS for $7.50. Cable security key gets past collars $25. Add $5 shipping. No TX sales. Send money order to: K. Perry, PO Box 816, Leander, TX 78646-0816. Phone: (512)259-4770.

HEAR NON-COMMERCIAL SATELLITE RADIO programs right in your area without the use of a dish or any other expensive receiving equipment. Thousands of these programs are operating today across America. Programs may include talks shows, weather, sport events, news feeds, financial reports, music programs and data ports. This technology is received through a high tech. SCSRT1 card. Find out today what you have been missing! (800) 944-0630. Credit card orders accepted.

USED CELLULAR HANDHELDS: Panasonic EB3500 portables, includes a battery (but no charger) forty number alpha memory, good working order, available as an extension to your existing line for $279, or as is for $129. Orders only: (800)457-4556, Inquiries to: (714)643-8426. C.G.C.

HOME AUTOMATION. Become a dealer in this fast growing field. Free information. (800)838-4051.

TIRED OF SA TEST KITS with marginal or inconsistent performance? 21st Century Electronics and Repair guarantees peak performance with 40-pin processor kits. New, more flexible program with additional features puts others to shame. Price $49 each or 5 for $233. 1st time offered. (404)448-1396

FEDERAL FREQUENCY DIRECTORY! Kneitel's "Top Secret" registry of government frequencies, New 8th edition. 268 pages! FBI, DEA, Customs, Secret Service, BATF, Immigration, Border Patrol, IRS, FCC, State Dept., Treasury, CIA, etc. & surveillance, bugs, bumper beepers, worldwide US military, 225 to 400 Mhz UHF aero band, Canadian listings, & more! Ultimate "insider's" directory! Standard reference of law enforcement, news media, private security, communications industry & scanner owners. $21.95 + $4.00 shipping ($5.00 to Canada). NY State residents add $2.21 tax. CRB Research Books, Box 56BL, Commack, NY 11725. Visa/MC welcome. Phone orders (516) 543-9169 weekdays (except Wednesday) 10 to 2 Eastern.

TV CABLE/SATELLITE ("GRAY" MARKET) DESCRAMBLER EXPOSE, 160pp, illustrated, with vendor lists for chips, parts. Law, countermeasures, much more! $23.95 + $3 S/H. Check/MO. INDEX, 3368 Governor Dr., Ste. 273, San Diego, CA 92122. Credit cards only: (800) 546-6707. Free catalog of "insider" books on scanners, cellular, credit, eavesdropping, much more.

TOP SECRET SPY DEVICES Home of the Worlds' Smallest Digital Voice Recorders and Spy Cameras. We stock many items including: Transmitters, Bug Detectors, Audio Jammers, Telephone Recorders, Lock Picks, Voice Changers, Keystroke Loggers. www.spydevicecentral.com (305)418-7510

EUROZINES AND OTHER CULTURAL HACKER ZINES! A one-stop, cutting-edge mail-order source for over 1,000 titles. Beautifully illustrated 128-page catalog includes: alternative/ fringe science, conspiracy, Forteana, sexuality, computer hacking, UFOs, and much more. Send $3.00 to Xines, Box 26LB, 1226-A Calle de Comercio, Santa Fe, NM 87505.

WEB SITES We have a list of hundreds of interesting and unusal web sites. Some of the sites are related to this magazine and some are not. Hacking, phreaking, breaking the law, sovereign citizenship, lasers, electonics, surplus, credit, etc.. You have to check this out! Save hundreds of hours of time by getting our list. We will provide the list on 3-1/2" disk and you can load it directly into your web browser and click on the links OR we can provide the list on paper - whichever you prefer. Send $5 to TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

FM STEREO TRANSMITTER KIT. Transmitter broadcasts any audio signal from a CD player, VCR, or cassette player to FM stereo radios throughout your home and yard. Uses the unique BA1404 IC. Tunable across the FM band, runs on 1.5 to 12 volts CD. PC board/components, $24. Visa/MC. TENTRONIX, 3605 Broken Arrow, Coeur d'Alene, ID 83814. (208)664-2312.

CALLING ALL WRITERS! We want YOU to write for us. We're looking for articles related to the hacker "scene", technology reviews, opinions on issues, etc. If you submit an article for print and we use it, we'll pay you $25-$600, depending on length, content and the use of additional material such as (diagrams, photos, pictorials, schematics, etc). We require all photos to be 3.0megapixel or greater. JPG format is acceptable. Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

TRUE TAMPER-PROOF Security Screw Removal Bits. The super torx kit includes: T-10, T-15, T-20 & T-25. Complete set for $19.60. TOCOM 5503 bit $8.95. TOCOM 5507 bit $19.95. Zenith PM/PZ-1 bit $10.95. Jerrold Starcom bit $19.95. Pioneer (oval) bit $23.95. Oak Sigma (oval) bit $23.95. Security Screws available. Tamper-Bit Supply Co. (310)866-7125.

CELLULAR RESTORATION on your 800 Mhz scanner performed expertly for $40 including return shipping. Guaranteed. Offer expires soon. Keith Perry, 607 Osage Dr., PO Box 816, Leander, TX 78641. (512) 259-4770.

6.500 MHZ CRYSTALS $4 a piece, 50 for $115, 100 for $200. Add $3.00 for shipping. Send checks to C. Wilson, P. O. Box 54348 Philadelphia, PA 19105-4348

SPECIAL SALE amd 2400+ system with 256mb ram, 40gig hdd, 64meg int video w/agp slot and extremely portable case w/handle $450.00 + shipping handling. for details send email to xteraco@yahoo.com w/ subject special sale??

OBSOLETE COMPONENTS Are you looking for an old IC you can't seem to find anymore? We have a very wide variety of hard to find and obsolete components available. Check us out. Odds are, we have the part you need or can find it for you. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

COIN-OP VIDEO ARCADE GAMES. Parts, boards, and empty cabinets available for your projects. Cabinets available for $75. C.J. Stafford, (301)419-3189.

WANTED: FEATURE FILM JUNKIE who can access up-to-date FAX numbers for hot agents and/or producers & directors. My objective: to bring to their attention my action-thriller script. Can pay by the hour. (909)275-9101

THE BLACK BAG TRIVIA QUIZ: On MSDOS disk. Interactive Q&A on bugging, wiretapping, locks, alarms, weapons and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining and VERY educational. Includes catalogs of selected (no junk) shareware and restricted books. Send $1.00 for S.25 disk, $1.50 for 3.5, plus two stamps, to: MENTOR PUBLICATIONS, Box 1549-W, Asbury Park NJ 07712

6.500MHz or 6.5536MHz CRYSTALS Your choice. $4 each. No shipping charges. Send to TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

ANARCHY ONLINE A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers and phone phreaks. Scheduled hacker chat meetings. Encrypted E-mail/file exchange. WWW: hhtp://anarchy-online.com Telnet: anarchy-online.com Modem: 214-289-8328

WAR DRIVING IS NOT A CRIME The benign act of locating and logging wireless access points while in motion - Wardriving is NOT a crime, being stupid should be. http:// www.wardrivingisnotacrime.com/

ARE YOU A PHOTOGRAPHER? With the increasing number of high resolution digital cameras in the hands of our readers, we're actively recruiting people to submit photos to us. We're looking for 3.0megapixel or better digital photo's of technology, people using technology, events, devices, utility personnel, utility vehicles in action (or doing nothing at all), tradeshows, technology swap meets and hacker meets. If it's related to hacking in any way, we want photographs!! Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

HACK THE PLANET A new and exciting board game in which 2-4 players race to complete a hacking mission. Please send $3.00 check or money order payable to CASH. Hand-scanned 99XX exchanges in 516 AC. Included may be data kit modem numbers, WFA/FA, SSCU, TSAC(SCC), CO#'s, etc. Send $2.00 check or money order payable to CASH and specify exchange. "MCI-Style" Phone Patrol hats are now available! Just $18 check or money order payable to CASH. 2447 5th Ave, East Meadow, NY 11554.

ATTENTION HACKERS & PHREAKERS. For a catalog of plans, kits & assembled electronic "TOOLS" including the RED BOX, RADAR JAMMER, SURVEILLANCE, COUNTER SURVEILLANCE, CABLE DESCRAMBLERS & many other HARD-TO-FIND equipment at LOW PRICES. Send $1.00 to M. Smith-02, P.O. Box 371, Cedar Grove, NJ 07009

PRIVACY ACT AND SOCIAL SECURITY NUMBER LIMITATIONS, How anyone can win $10K fine for this simple violation of your rights. Open a bank account without a SSN $5 plus 3 F/C stamps. Obtain a major credit card without a SSN (making it impossible for a bank or any institution to check your credit history or records) $25 plus 5 F/C stamps. For info send $1 and LSASE to: Know Your Rights, c/o R. Owens, 1403 Sherwood Dr., Bowling Green, KY 42103. NO CHECKS PLEASE. M/O or FRN's only.

HARD TO FIND 6502 6800 68000 Microprocessors. We have a wide array of very hard to find microprocessors and micro support devices available. If you need it, we probably have it. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

VOICE CHANGING ACCESSORY. Digital voice changing: male to female, female to male, adult to child, child to adult. Use with any modular phone. 16 levels of voice masking. Connects between handset and phone. STOP THOSE ANNOYING TELEPHONE CALLS! Sound older and tougher when you want to. Not a kit. Fully assembled. Use with single or multi-line phones. 30-day refund policy. Ask for free catalog of our products. VISA/MC ok. Xandi Electronics. 1270 E. Broadway, Tempe AZ 85282-5140. Toll Free order line: (800)336-7389. Technical Support: (602) 894-0992

MAGENCODERS.COM Manufacturer of the World's Smallest Portable Magnetic Card Reader & Point of Sale Data Loggers. We also have Magnetic Stripe Reader/ Writers, Smart Card Loaders & Copiers, etc... (407)540-9470

UNDETECTABLE VIRUSES. Full source for five viruses which can automatically knock down DOS & windows (3.1) operating systems at the victim's command. Easily loaded, recurrently destructive and undetectable via all virus detection and cleaning programs with which I am familiar. Well-tested, relatively simple and designed with stealth and victim behavior in mind. Well-written documentation and live antidote programs are included. Priced for sharing, not for making a ridiculous profit. $10.00 (complete) on six 1.44MB, 3.5" floppy discs. Money orders and checks accepted. No live viruses provided! Do NOT ask. Satisfaction guaranteed or you have a bad attitude! The Omega Man. 8102 Furness Cove, Austin, TX 78753

NO SOUND ON PREMIUM CHANNELS? It will happen sooner or later on your Jerrold DPBB-7 Impulse. Ask Manhatten! Soundboard brings the sound back. Best sound fix on the market. Easy to install soundboard $24.95. Easy to build soundboard schematic, parts list and common chip number $34.95. Send us your unit and we will install the soundboard for $59.95. SOUNDMAN, 132 North Jardin St., Shenandoah, PA 17976. (717) 462-1134.

BAD CREDIT? WANT/NEED A VISA CARD? If so, send us $19.95 (cash/check/MO) and we will send you a very useful list of addresses and phone numbers of banks and financial institutions that *WILL* work with you. Most will give you a VISA credit card regardless of your credit rating. We even include a few banks that will require a deposit, just to "round out" the list a bit. For an additional $10 we will include a small "how-to" program showing you step-by-step how to improve your credit rating and dealing with creditors. You might think that your bad credit doesn't mean anything right now.. Wait until you need to buy a house or a car, then you'll see how much you REALLY need to have GOOD CREDIT. So, get back on track. Buy our list and the how-to program and start your way back into a good credit status. Cash or money order. TCE Information Systems. P.O. Box 5142, Los Alamitos, CA 90721.

SINGLE DUPLICATION OF CD-ROMS Send your CD and $25 and you will receive your CD and an exact copy. Want more than one copy? Send a additional $15 for each duplicate. Make checks or money orders Payable to/Mail to: Knoggin, 582 Merket Street Suite 616, San Francisco, CA 94114

LOOKING FOR A BLACKLISTED! 411 MEETING IN YOUR AREA? Why not host one yourself? It's easy. Tell us where you want it held and give us a contact name and number or email address. If you want your free subscription, you'll need to provide an address, of course. Think about starting a meeting yourself.

FIND PIRATE SOFTWARE Learn how to find pirate software on the Internet. Get thousands of dollar's worth of programs for free such as Office97 and more games than you can play. Complete guide includes background, tools, techniques, locations, and shell scripts that will find software for you! Send $5.00 money order or CASH (no checks) to The Knoggin Group, P.O. Box 420943, San Fransisco, CA 94121-0943, USA.

RAM DRAM SRAM GALORE We have many hard to find memory devices available. If your project requires old RAM not available any longer, check us out. We have a very wide selection of RAM to choose from. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

CB RADIO HACKERS GUIDE! New! Big 150 pages; pictorials, diagrams, text. Peaking, tweaking and modifying 200 AM and SSB CB radios. Improved performance, extra capabilities! Which screws to turn, which wires to cut, what components to add: Cobra, Courier, GE, Midland, Realistic, SBE, Sears, Uniden/President. $18.95 + $4 S&H ($5 Canada.) NY State residents add $1.96 tax. CRB research, Box 56BL, Commack, NY 11725. Visa/MC accepted. Phone order M-Tu-Th-F, 10 to 2 Eastern time. (516) 543-9169.

S-100 BUSS CARDS for sale. I have piles & piles of S-100 cards I'd like to sell off at $15 each. Vector, Corvus, SpaceByte, Cromemco, Heath, etc. Please contact me for a complete list of available items. techgathering@comcast.net

AUCTIONS! You hear about them all the time, but you've never been to one? You gotta GO to one. You can buy just about anything for pennies on the dollar! Cars, trucks, boats, houses, electronic equipment, furniture, etc. Forget that "cars for $100" crap. That's a load! But, you can get some pretty awesome deals for small amounts of cash.. Our favorite auctions (and many of the BL411 staff) include the arcade auctions and the car auctions. Remember those arcade games you played as a kid in the 80's? Man, you can get some bitchen deals on those! This is only the tip of the iceberg. There's SO MANY things you can get for a small fraction of their worth. Send $5 and we'll send you a booklet loaded with names, numbers and places to go...You NEED to do this! You'll find out how you can attend the non-advertised auctions, which will mean better deals for you. Don't miss out on all the great deals! So send $5 right NOW: TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721.

WE WANT WRITERS! That's right! We want YOU to write for us. The people at Blacklisted! 411 are currently seeking freelance writers to increase the quality and scope of the magazine. We're looking for quality articles related to the hacker "scene", events, technology reviews, opinions on issues, etc. If you submit an article for print and we use it, we'll pay you $25-$600, depending on length, content and the use of additional material such as (diagrams, photos, pictorials, schematics, etc). We require all photos to be 3.0megapixel or better. JPG format is acceptable. Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

NULL MODEMS - Download laptop: or upload to your pc the easy way! w/ direct connect, or (DOS 6.1) Customized setup, no bulky adapters, MAC or IBM compatibles. Send $18.95 for 6ft cable, specify 25 or 9db ends, custom ok. Instructions included. P.O. Box 431 Pleasanton, CA 94566 (510)485-1589

NEW BOOK FOR CABLE HACKING. All about the industry and how to install test chips in nearly every model of decoder. Test chips available, Etc. (408)581-2380

SECURITY SCREWDRIVER BIT SET Our best selling 30 piece screwdriver bit set is now available for $40 including shipping to anywhere in the U.S. The set includes 9 security Torx bits from TT7 through TT40, 7 security Hex bits from 5/64" through 1/4", 4 Scrulox bits from S-0 through S-3, 8 standard pieces, covered plastic case w/ a nice handle for all of the bits. This is an extremely handy toolset you'll wonder how you ever did without! TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

DON'T BUY A MODIFIED CABLE CONVERTER! I'll show you what to do. Where to get parts, everything. Call 24hr.. 1-800-295-0953 Only $9.95 + $2.20 S&H Visa/MC/Dis.

SPEECH CHIPS - WE GOT 'EM Yes, we have hard to find speech chips. We have General Instruments SPO250, SPO256, Votrax SC-01, Harris HC-55532, Texas Instruments TMS5220NL, TMS5220CNL and more. Come and check us out. We have a wide selection to choose from. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

HACKERS '95 THE VIDEO by Phon-E & R.F. Burns: See what you missed at Defcon III and Summercon 95! Plus, our trip to Area 51 and coverage of the "CyberSnare" Secret Service BUSTS. Elec Cntr Measures, HERF, crypto, and more! Interviews with Eric BlookAxe, Emmanuel, and others. VHS 90 min. Only $25 - distributed by Custom Video 908-842-6378.

HACKERS SCREWDRIVER BIT SET Brand new for 2004! Our newest selling 60 piece security screwdriver bit set is now available for $55 including shipping to anywhere in the U.S. The set includes 3 Spline bits M5 through M8, 4 scrulox (square) bits S0 through S3, 3 torq-set bits 6 through 8, 12 security torx T-5 through T-40, 13 security hex bits 2mm through 5/32", 5 tri-wing bits 1 through 5, 3 posidrive bits PZ0 through PZ2, two flat bits 1/8" and 3/16", 3 phillips bits 0 through 2, 5 spanner bits 4 through 12, 3 bowtie bits C1 through C3, triangle bit 2mmx2mmx2mm, wing nut driver, 1/4" x 60mm bits holder, bit holder socket, socket adaptor, ratchet screwdriver and a covered plastic case. This is an extremely handy toolset no hacker should be without! TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

SPEECH CHIPS - WE GOT 'EM Yes, we have hard to find speech chips. We have General Instruments SPO250, SPO256, Votrax SC-01, Harris HC-55532, Texas Instruments TMS5200NL, TMS5220NL, TMS5220CNL and more. Come and check us out. We have a wide selection to choose from. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

A TO Z OF CELLULAR PROGRAMMING. Programming instructions on over 300 phones in a software database. Also back door and test mode access instructions for all the popular models; manufacturer's contacts, system select, lock/unlock info. Just $59.95. Orders only: (800)457-4556, inquiries: (714)643-8426. C.G.C.

WE NEED ARTISTS! We're actively recruiting people to submit artwork to us. We're looking for freehand as well as computer artwork of technology, people using technology, events, devices, utility personnel, utility vehicles in action (or doing nothing at all), tradeshows, technology swap meets and hacker meets, comics, etc. If it's related in any way, we want artwork!! Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

GAMBLING MACHINE JACKPOTTERS We offer a complete range of gambling products designed to cheat gambling machines as well as other games. Our products are designed to demonstrate to gambling machine owners the vulnerabilities of their machines. Our product line consists of Gambling Machine Jackpotters, Emptiers, Credit Adding Devices, Bill Acceptor Defeats and Black Jack Card Counting Devices. Please visit www.jackpotters.com

ADVERTISE IN BLACKLISTED! 411 Classifieds are now FREE for everyone. Reach thousands of readers in the US, Canada, Japan, the UK, Australia, and elsewhere. Join our long list of satisfied clients who have made Blacklisted! 411 their vehicle for reaching customers. Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

KEYSTROKEGRABBERS.COM Manufacturer of discreet keyboard logging hardware. Our devices capture ALL keystrokes on a computer including user name and password. PARENTS---Monitor your child's internet, e-mail, instant messaging and chat room activity. EMPLOYERS---Monitor employee computer usage compliance. Employees will spend less time browsing the internet and sending e-mails if they are being monitored. EXECUTIVES & SYSTEM ADMINS---detect any unauthorized access of your PC. If someone uses your computer after hours, you will know. (305)418-7510

ADAPTEC SCSI CARDS for sale. We have AHA-2940, AHA2940UW, AHA-2944, etc. $20-$30 each. We also have brand new 3' and 6' SCSI cables $2-$4 each. DB25-to-SCSI, SCSI-to-SCSI II, etc. We also have brand new Belkin 15' IEEE printer cables $3 each. Shipping extra. We have a wide selection of SCSI products to choose from at low, low prices. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

INTEL SDK-85 SYSTEM DESIGN KITS available here. I've been collecting this stuff for years. They're in GREAT condition. $100 each plus shipping. If you're interested, please contact me ASAP. techgathering@comcast.net

HACKING, PHREAKING, computer security and education on the First Tuesday of every month in the Detroit area. Meeting is at 7pm at Xehdo's cafe in Ferndale. Bring your open mind and positive attitude. **MAKE MONEY NOW, HACKERS!** Have an interesting story to share? Write for us and make some money. Have some cool photo's of something nobody has seen? Send it to us and get PAID! Doodle on paper all the time and wish you could catch a break...along with a paycheck? Draw for us and make $$$! Blacklisted! 411 Magazine, P.O. Box 2506, Cypress, CA 90630 www.blacklisted411.net

ZINE PUBLISHER RESOURCE BOOK If you're thinking about publishing or already started publishing a zine, you need this resource booklet. Discover who you can distribute your zine through and make more money. Send $14.95, cash or money order only. TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

NEW BOOK ON HACKING We're going to put together a hard cover book full of interesting stories from hackers, crackers and phreakers. If you have a story to share, please send it to us along with some contact information (ie: name, address, email, phone number - we won't publish this information), your handle/alias/pen-name for print. The longer the story, the better. We'd like factual stories, but we'll consider fictional stories as well. If you have any suggestions on the topic of this book, we'll consider your ideas. Once the book is complete, each person who submitted material we use will get a FREE copy of the book. Please send your material to: Blacklisted! 411 Book Project, P.O. Box 2506, Cypress, CA 90630.

CHIP COLLECTOR / SALVAGE SOURCEBOOK Have you ever looked online for some collectable components or vintage electronic equipment, only to find out that it's cost is way too high? This sourcebook will provide you with the ability to locate the same items at only a small fraction of the bloated online cost. Buy collectable gold chips (Intel, Motorola, Zilog, National Semiconductor, etc) for $20-$40/lb. Do you have any idea how many chips are in a single pound? More than enough to make this sourcebook worth a peek! Find that Intel C4004 you've been looking for and pay pennies, not hundreds of dollars. Grab a few thousand EPROMs and pay a few bucks a pound, not a few bucks per EPROM!! Find older high end EPROM programmers for $20-$30, not $200-$300! The deals are many, the price is minimal. You'll be glad you got yourself a copy of this sourcebook and wonder how you ever did without! Send $19.95, cash or money order only. TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

A SHOW ON URBAN Exploration. WhiteSword TV http://WhiteSword.tk

INVESTOR NEEDED to assist InEvitableGlobalDomination $25000 startup cost required for Textile Industry. Contact croz@consultant.com For further details. Market Analysis Report available to interested investors only.

I WANT TO OFFER my playstation 2 game burning service. Any game that you would like for a back-up or just for fun. Or maybe that Japanese game that just won't be out in the United states for a few months.. I have bundles that you can choose from if you want handfulls depending how much you order. the games are $25 each !PLEASE NOTE THAT YOUR PLAYSTATION 2 NEEDS TO BE MODDED i ALSO HAVE THAT SERVICE BUT YOU CAN ALSO GOOGLE SEARCH FOR PREMODDED SYSTEMS TO BUY. EMAIL IF YOU HAVE ANY QUESTIONS AT ALL.

ACCUSED OF A COMPUTER RELATED CRIMINAL OFFENSE IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in the defense of alleged cybercriminals, including but not limited to, hackers, crackers, and phreaks. Not a former prosecutor seeking to convince defendants to plead guilty, but an idealistic constitutional and criminal defense attorney who helped secure a total dismissal of all charges in Los Angeles Superior Court for Kevin Mitnick, who was falsely charged with committing computer-related felonies in a case with $1 million bail. Please contact Omar Figueroa, Esq., at (415) 986-5591, at omar@aya.yale.edu or omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Complimentary case consultation for Blacklisted 411 readers. (Also specializing in medical marijuana and cannabis cultivation cases.) All consultations are strictly confidential and protected by the attorney-client privilege.

DO YOU WANT MORE underground information? Are you ready to go to a whole new level of knowledge? Then you need to check out "Binary Revolution" magazine.
 is a printed hacking magazine put out by the DDP that covers hacking, phreaking, and other assorted topics from the computer underground. For more information on the magazine, forums, HackRadio, HackTV, or any of our other numerous projects, come to www.binrev.com and join the revolution. "THE REVOLUTION WILL BE DIGITIZED."

I-HACKED.COM is a hardware hacking based website and it currently looking for articles! Membership is limited to contributing members, so come and share your knowledge with other hackers around the world. Topics we are currently looking for include: DVD "Dual-Layer" Firmware hacks, CD-RW / DVD+/- Speed Hacks, Video Card Hacks, Motherboard Hacks, IDE Card / Raid Hacks, Xbox Hacks, Playstation Hacks, cell phone tricks, or anything else you might have. Check us out @ http://www.i-hacked.com

NEW HACKING WEBSITE: Hackit.org has hacking guides, forums,tools and more. Much more. Check it out!

I RECENTLY GOT HOLD of a service that will allow me to make a call via the internet and have the caller ID appear to be whatever number I want. Not cheap but i really like the idea. I would like to find away to do it and be able to do it directly via my phone/cellular. If you know how I could do it (any way possible) please contact me.

BLACKLISTED MEETINGS will begin in Greece as the new year arrives, They will be held every 3rd saturday of the month and they will begin at 7pm. Meeting point will be the centre of Athens at the metro station Panepistimio by the fountains. Also check the webpage www.blacklisted411.gr.

A+ CERTIFIED TECHNICIAN offering cheap repairs in Louisville Area. Will make house calls or take home with me. I do everything from virus and spyware removal to networking. Send an email to alanb6100@gmail.com with your name and phone number as well as a description of the problem. Also I have Gmail invites available for a reasonable price. Louisville area only unless you want to Western Union me some money! Thanks!

THE NEWEST DEVICE on the market it the new Sony PSP. Already there are numerous hacks out to make it do your bidding, whether it be surfing the net, or using memory sticks to watch movies the sony psp is powerful. These are a hot comodity. Get them before they are gone.
Get them from Phreepsps.com

BUILD YOUR OWN REPLICA APPLE I 8-bit computer! The replica 1 is a functional clone of the first Apple computer. Prices start at $129. See www.vintagecomputer.tk for more details.

HI, MY NAME IS RICK. Me and my friend Rob where looking for a low cost rackmount server one day to use for a web and mail server that we could have racked at a local datacenter, Not finding anything real cheap we decided to start our own company building fast cheap servers for you also. www.cheap1u.com was born. Mention this ad and get 10% off any server order. Also since I am the owner, if you mention this ad buy 10 servers and I will throw in the 10th server for free! Thats right even our $399 AMD powerhouse!

SELLING USED HIRSCH SCRAMBLEPADS that retail new for around 500$ for your best offer! They are for very high security places, every time you press the START button on the keypad it randomizes the digits so that any onlookers cannot find a pattern in the digits you press. Also, you cannot see the numbers from the side, so for anyone to see your code they would have to be directly behind you. Email me for more information. guiltyspark414@netscape.net

TUNE IN TO CYBER LINE RADIO on the internet, on the USA Radio network. We can be heard Saturday Evenings 9:00 pm to 12:00 am (Central). Heard Exclusively On The USA Radio Network & Via The Internet! We discuss Technology, Space, Hacking, Linux and more. For more details meet us at www.cyber-line.com.

ATARI/BALLY/WILLIAMS ARCADE PARTS We stock hard to find parts for your arcade games. We have custom ROMs, PROMs, custom sound and speech chips (AY-3-8910, AY-3-8912, AY-3-8913, HC-55532, TMS5200, TMS5220, SC-01, SPO250, SPO256, LM379, etc), custom video chips (TMS9928), custom Atari chips (AVG, SLAG, SLAPSTIC, POKEY, etc), custom Namco chips, custom Williams "Special Chip 1", D-to-A and A-to-D converter chips (AD561JD, AM6012, AD7533, ADC0804, ADC0809, etc), Atari LED buttons, Keltron brand Cinematronics flyback transformers, trackball roller repair kits, 6500, 6800 and Z80 series CPU's and support chips. We even carry manuals and schematics. We have a wide selection of arcade parts to choose from. GI Electronics www.gielectronics.com P.O. Box 11029, Westminster, CA 92685

CELLULAR EXTENSIONS, SEND US YOUR PHONE or buy a new or used phone from us! Proof of line ownership required. We have phones from $129. Call for a list of available models, we program many different brands including all Motorola, same day service. Orders only: (800) 457-4556, inquiries to: (714)643-8426. C.G.C.

WANTED: OLD COMPUTERS for my collection. Looking for Commodore, Atari, Amiga computers, accessories, books, cables, software. If you have something like this that you no longer want, please contact me ASAP. techgathering@comcast.net

Marketplace classified advertising is currently FREE to anyone. It's a first come, first served offer, limited only by space constraints within each issue. If you'd like an ad placed within Blacklisted! 411, you should send it in as soon as possible. We accept both commercial as well as personal ads. We may decide not to publish any ads which are inappropriate or have no connection with the hacker community.

CONTACT US AT: www.blacklisted411.net

MONTHLY MEETINGS

Interested in meeting up with some of the Blacklisted! 411 readers? We will list all hacker meeting information that is provided to us. We will list "Blacklisted! 411" only meetings as well as "independent" meetings open to all.

California

(949 Area Code) - Irvine

iHop - By Airport (Upstairs Room), 18542 MacArthur, Irvine, CA. 92714 - Meeting is not Blacklisted! 411 specific. The meeting date may change from month to month. For specifics, check here: www.irvineunderground.org
Hosted by: Freaky

New Mexico

(505 Area Code) - Albuquerque

Winrock Mall - Louisiana at I40, food court, east side doors under the security camera dome.
First Friday of the month, 5:30pm - 9:00pm
Hosted by: Mr. Menning

(505 Area Code) - Albuquerque

The computer room in the Grand Reserve Apts. at Maitland Park
Last Friday of the month, 12:00pm - 1:30pm
Hosted by: Whisper

Wyoming

(307 Area Code) - Rock Springs/Green River

White Mountain Mall—Sage Creek Bagels. The last Friday or every month from 6:30pm until 9:30pm.
Hosted by: Phreaky

Colorado

(719 Area Code) - Colorado Springs

DC719 - Hack the Rockies. Meetings held on the 3rd Sat. of every month. 8pm-11pm @ Xtreme Online, 3924 Palmer Park BLVD
Hosted by: DC719 POC: h3adrush

(303 Area Code) - Centennial

We meet the first Friday and third of every month at 5:00pm at the Borders café on Parker in Arapahoe Crossings.
Hosted by: Ringo

Mexico

(666 Area Code) - Tijuana, B.C.

Café Internet, Calle 12, Felix M. Gomez #844, Col. Libertad. In back room by payphone. First Friday of the month, 5:00pm to 8:00pm
Hosted by: Tom

YOUR MEETING HERE

Want to set one up? Contact us and give us your information in a similar format to the meeting info. listed here.

G.I. ELECTRONICS

YOUR BEST SOURCE FOR HARD TO FIND AND OBSOLETE COMPONENTS
WWW.GIELECTRONICS.COM

DRAM/SRAM

1101	$15.00
1103	$15.00
2016	$5.00
2101	$8.00
2102	$10.00
2104	$8.00
2107	$15.00
2114	$5.00
2115	$15.00
2117	$12.00
2128	$6.50
2147	$7.00
2148	$8.00
2149	$9.00
X2212	$35.00
27S03	$5.00
4016	$6.50
4027	$4.00
4116	$4.00
4118	$10.00
4164	$4.00
4416	$5.00
4801	$10.00
5101	$10.00
5114	$25.00
6116	$6.00
6264	$7.00
9101	$8.00
9128	$6.50
74S89	$5.00
93415	$15.00
93419	$10.00
93422	$15.00
82S09	$15.00

SOUND/SPEECH

AY-3-8910	$15.00
AY-3-8912	$15.00
AY-3-8913	$15.00
CO12294B	$15.00
LM379S	$25.00
MB3730	$35.00
SC-01	$45.00
SPO250	$35.00
SPO256	$35.00
TDA1004	$25.00
TDA2002	$15.00
TMS5200NA	$25.00
TMS5220NA	$25.00
TMS5220NL	$25.00
TMS5220CNL	$30.00
HI55532	$55.00

Z80

Z80	$2.00
Z80A	$4.00
Z80B	$6.00
Z80-CTC	$2.50
Z80A-CTC	$4.50
Z80B-CTC	$6.50
Z80-PIO	$3.00
Z80A-PIO	$3.50
Z80B-DART	$3.00
Z80A-DART	$3.00
Z80-SIO/0	$4.00
Z80A-SIO/0	$4.00
Z80B-SIO/0	$4.00
Z80-SIO/2	$4.00
Z80A-SIO/2	$4.50
Z84C00-4	$8.00
Z8530 SCC	$6.00
Z8603RS	$20.00
Z8613RS	$25.00

6500

6502	$5.00
6502A	$6.50
6502B	$8.00
65C02	$8.00
6504A	$8.00
6507	$8.00
6510	$8.00
6512	$8.00
6520	$8.00
6522	$6.00
65C22	$8.00
6525	$8.00
6526	$7.00
6529	$7.00
6532	$8.50
6551	$6.00
6551A	$6.00
65C51	$6.00

PROM

82S23	$15.00
82S123	$8.00
82S126	$8.00
82S129	$8.00
82S130	$9.00
82S131	$8.00
82S137	$9.00
82S140	$16.00
82S141	$16.00
82S147	$20.00
82S153	$25.00
82S180	$12.00

6800/68000

6800	$4.00
6802	$10.00
6803	$9.00
6808	$12.99
6809	$8.00
6809E	$8.00
6810P	$2.99
6810	$9.99
6821	$5.00
68B21	$5.00
6840	$6.00
6850	$4.00
68000P8	$4.99
68000P10	$5.99
68000P12	$6.99
68000L8	$14.99
68000L10	$16.99
68000L12	$17.99
68008	$10.00

EPROM/EEPROM

2516	$10.00
2532	$16.00
2564	$15.00
2708	$15.00
2716	$10.00
27C16	$8.00
2732	$12.00
2732A	$10.00
27C32	$8.00
TMS2732	$11.00
TMS2732A	$11.00
2764	$4.50
2764A	$4.50
27C64	$2.00
27128	$3.50
27128A	$3.50
27C128	$2.50
27256	$4.50
27C256	$2.00
27512	$5.50
27C512	$2.50
27C010	$5.00
27C010A	$5.00
27C020	$8.00
27C040	$9.00
27C080	$9.00
27C1024	$6.00
27C2048	$8.00
27C4096	$10.00
NC7055	$35.00
ER2055	$35.00

SPECIAL SERIES

MC1495	$8.00
AM2901	$8.00
AM2903	$20.00
AM2907	$8.00
AM2909	$8.00
AM2910	$8.00
AM2911	$8.00
AM2914	$15.00
AM2960	$15.00
AM2964	$14.00
AM29116	$20.00
AM29516	$20.00
AM29701	$8.00
TMS9927	$35.00
TMS9928	$45.00
DG201	$4.50
LF13201	$4.50
LF13331	$9.95
CD4016	$1.50
CD4066	$2.00
LM324	$6.50
LM3900	$6.50
TL081	$3.50
TL082	$3.50
TL084	$4.00
WD1010	$15.00
WD1014	$15.00
1771	$15.00
1791	$15.00
1793	$15.00
1795	$15.00
1797	$15.00
2793	$21.00
2797	$21.00
DSP32010	$15.00
TMS32020	$15.00
TMS38010	$15.00
TMS4500A	$15.00
TMS5501NL	$45.00
TMS5502NL	$45.00
8X300	$15.00
8X305	$15.00
G171S-35C	$10.00
N3002I	$35.00
NS32201	$10.00
NS32203	$10.00
P4004	**$40.00**
D4004	**$70.00**
INS4004	**$60.00**
P4001	**$20.00**
P4002-1	**$20.00**

WWW.GIELECTRONICS.COM

GI ELECTRONICS, P.O. BOX 11029, WESTMINSTER, CA 92685

Blacklisted! 411 Magazine
The Official Hackers Magazine
P.O. Box 2506