Blacklisted! 411

The official hackers magazine

HACK THE SYSTEM...

Telecommunications Hot Drops

Is your landline conversation really safe?

Also inside this issue:

RFID: Chip on My Shoulder

WRT54G/S Expansion

Motorola Phone Modding

VOLUME 7 ISSUE 3

SUMMER 2005

Blacklisted! 411 v7i3

$5.95 U.S. $7.75 CAN

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

All opinions and views expressed in Blacklisted! 411 Magazine are those of the writers of the articles, and do not necessarily reflect the views or opinions of any Syntel Vista, Inc. staff members or it's editors.

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

9035768ABBAJBVJB-0023

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. They were all deeply interested in their Atari, Apple and Commodore computers, electronics, sciences, arcade games, etc. They built projects, hacked into various things, made their own programs, 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 (at the time) without all the cool toys we take for granted today. There was no internet to utilize and nobody had printers which could print anything other than plain text (and didn't even do that well). With a disk based system, text files, primitive graphics/ pictures, and utilities were fairly easy to distribute and it could be copied by anyone who had a compatible computer. At the peak, at least 150 disk copies <per month> of the disk magazine we sent into the world, though there is no way to know how many were copied by others.

Eventually modems caught on and the magazine was distributed through crude BBS systems. Using the power of a Commodore 64, a *Blacklisted! 411* info site, which anyone could log into without handle or password, was created and operated. It was a completely open message center. Using X-modem or Punter file transfer protocols, one 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". There was only one message center, no email capability & only 1 phone line. Primitive, indeed. Effective, however.

Around 1984, the purchase of a 9 pin dot matrix printer that could <gasp> print basic graphics was entered into the mix. Printing out copies of the *Blacklisted 411 monthly* and copying them at the media center at the high school became the new "experiment". The media center staff graciously allowed the production of these copies free of charge which was very cool at the time. The copies were passed 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). Piles of the magazine were left anywhere and everywhere people could see them. One popular location was next to the Atari Gauntlet and Gauntlet II arcade games strategically located at 7-11's all over the place. It's been a longtime myth that people photocopied those original 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 they were left, they were taken - and taken quickly! The feedback was awesome in that people wanted more. The interest was very high, but the inability to meet this growing demand was completely overlooked. The plug was officially pulled on the printout experiment and distribution through diskettes remained the norm. It was really the easiest way to go at the time. 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 disks were still being released at this time.

June of 1987 marked the end of *Blacklisted! 411, the hackers monthly*. The last disk based magazine (# 46) was distributed that month. Since all of us original crew were finally 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, it was assumed that this was the end and *Blacklisted! 411* would never be resurrected in any form.

In the summer of 1993, one member (and the original editor-in-chief), Zachary 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 and he was alone. 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, the will to make it happen, 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. Regardless, the related user meets were packed! The interest in the magazine was great. After a year passed, it was decided to try a quarterly format in an effort to increase distribution. During that year Zachary managed to get in contact with many of the old group members, most of whom which are active staff members even today.

In 1999, what was to be the last issue of *Blacklisted! 411* (Volume 5, Issue 4) was published. It was unknown at the time, but many pitfalls would ultimately cause the demise of the magazine. Officially, it was dead as a doornail. After 4 years of regrouping and planning, *Blacklisted! 411* magazine was resurrected yet again..

To date, Blacklisted! 411 is 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. Hanging onto the very same hacker mentality and code of ethics from the 80's, Blacklisted! 411 stands apart from the rest. Their ideal is that hackers are not thieves - they're curious people who are the makers and shakers of the technology sector. They're not elitist hackers by any means and believe that no question is ever a "stupid" question. Old school hackers and newbie hackers alike, Blacklisted! 411 caters to you.

What' about now…

Community

Over the last year and a half, a lot has been happening. We have become more active in the Hacker Community. As we are based in the Los Angeles area, we have built relationships with the local Hacker groups such as LA2600, SD2600, twentythreedotorg, Irvine Underground and more. We have been attending and sponsoring Hacker Conventions and Conferences such as the Layer One Convention and the ever popular Defcon. You can find us attending these conventions regularly. We usually have a booth at these events where we sell subscriptions, current and back issues of the magazine, and other swag. We also provide 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 for the magazine was to break 100K copies distributed each quarter sometime in 2004 and we surpassed our goal within our timeframe.. Based on orders from distributors and sell through, nobody comes even close to touching us in the hacking arena. We have been 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 now have a whole series of *Blacklisted! 411* themed swag and merchandise. This currently includes stickers and apparel, but will soon include posters, a new DVD 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.....

Greetings everyone! Yes, we've made it to the third installment of this wacky little hacker magazine for 2005. We had to push extra hard to get this issue to print several weeks early so we could have it available by Defcon 13. Talk about cutting it close. This issue was finished with no time to spare. Wow, Defcon 13. Has it really been that long? So much has changed since the early days of hacking. Ahh, the memories.

Kudos to Dark Tangent, the maker of Defcon. He's just awesome. The guys over at Defcon are doing a fantastic job in providing the community with the best annual hacker party on the planet. It's second to none. It's difficult to believe that this is the thirteenth incarnation of the greatest hacker summit on planet earth. If you've never been to Defcon, you're really missing out on one hell of a great time. Visit them: www.defcon.org

Shouts go out to the people at Binary Revolution. They put together a great little zine called "BinRev". I've had the opportunity of reading every issue they've put out and I can't say enough good about them. I love what they're doing and fully support their efforts. Way to go guys! www.binrev.com

So, I bet you're wondering what those nutty people at Blacklisted! 411 magazine have been doing for the last few months. Me too. Ha-ha. Just kidding. Yeah, so a lot of things have been going on with Blacklisted! 411 lately. Top of the list has been the astounding increase in our distribution. It's just amazing how many copies of recent issues we've pump out into the world. We had modest goals since our comeback, but we totally blew away even our most aggressive estimates. It's good to be back at the top. You, the readers, are the ones who made this possible. Your voice has been heard and the copy you're holding in your hands is the result of your efforts. Sincerely, my thanks to all of you.

Speaking of distribution, we recently lost one of our distributors (no names) that dated back to the early days of Blacklisted! 411 which was a sharp blow to the various underground communities as well as to the retail industry, but it was no surprise to any of us. We all saw it coming for a long time and we were well prepared for it. However, as a result of this loss, some of you may have a little bit of trouble locating the newest issues at Borders and a few other small chains until all of the kinks are worked out of our shifted distribution chain. We'll get through it. If you want to help, all you have to do is keep bugging your local bookseller to stock our magazine.

We're hiring, people. Yep, we actually pay our staff over here. I know it's probably an unheard of way to do things, but we're west coast, guys. It costs a lot to sustain yourself out here, so we keep our guys paid. Anyhow, to the point. We're looking to fill a few various positions over here.

We need a couple of artists who can work with illustrations and digital artwork, provide this work in a timely manner and work unattended (ie: without much direction). We will provide our artists with the breathing room with respect to creative control over what they do. If interested, please contact myself (Zachary) or my sidekick (Alex) immediately and provide at least a couple samples of your work.

We're also looking for a talented web designer we can keep around for those special times when we need new/updated website content. It's an issue I would like to resolve quickly, so we need to bring in some talent. Again, make contact with us and direct us to some of your sample work.

We currently have an incredible list of writers, both staff and freelance, at our disposal. However, we're always in need of new, fresh material. If you're a tech geek and you think you can write for us, please get in touch with one of us right away. We're always in the market for new writers. Speaking of which, yes, we are a paying market. I can't think of any other "hacker" magazine that actually pays it's writers with cold hard cash. Weird, huh?

We're well into the production of our DVD. It was a mere thought we passed around only months ago, but it's turning into a reality. We have enough of the groundwork set in place, that I'm in a position to tell you more about it. Our "DVD Project" as we've been referring to it as is going to be a top notch production which we have been hard at work on.

Blacklisted! 411 magazine is putting together a brand new DVD about hackers, the hacker community, technology and all related issues. The DVD is arranged as a documentary with a mix of "reality TV" thrown in to capture the interest of a wide audience - old school & newbie hackers, teens, college students and professionals alike. Packed with interviews from the Blacklisted! 411 staff, contributors, real life hackers (both white hat and black hat), celebrities, industry leaders, law enforcement and local government, this won't be your average hacker video. It's the ideal of the Blacklisted! 411 team to bring to the table an informed look at hacking, the reality, the pitfalls and associated amusement. We're serious, but we'd like to keep it fun, too.

If you'd like to contribute to this effort in any way, please contact me as soon as possible. We'll consider any creative ideas or content at this point in time.

You can find out more about this project from our main magazine website (www.blacklisted411.com) or through our main DVD website (www.hackthesystemdvd.com).

Speaking of projects, many of the readers constantly ask us for DIY (do it yourself) projects. Most of our writers have technical backgrounds, but coming up with build-me projects has proven to be difficult at best. We're working on the situation. I just wanted to mention it so I can avoid contacting each of you individually about the subject. Further, if there's someone out there who wants to single handedly take on our project articles, step up. Compensation will be great.

I'd like to take a moment to mention one of our staff members, The Goldfinger. He's what I have been referring to as the "go to guy" over here. If we need it, no matter what the hell it is, we go to this guy. He gets the job done and he does it quickly, with great precision. Over time, he's moved up from a freelance writer to a full blown staff member. In fact, he's doing a lot of the footwork on our DVD project. I consider him an awesome creative talent and recommend to any of you interested in helping out Blacklisted! 411 magazine in any way, to give him a shout so you can discuss how you may be able to help. If you're not sure, he can figure it out for you. :-) Give him a shout. Goldfinger@voyager.net

So, finally bringing this to a close, the magazine is doing great, the people running the show over here are in high spirits and we're all having one hell of a time doing what we love to do — producing a cool little hacker magazine that gets noticed. We're west coast hackers. We left the attitude at the door. Join us and have a great time. Until the next issue, be safe and hack the system!

- 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 4 is October 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.

Letters and comments from our readers…..

Dear Blacklisted! 411,

Hey, it's nice to see another hacker magazine! I found your magazine for the first time at Tower Records. I really like what you guys are doing.

My question involves payphones. Now, I know what you're thinking, but no I don't want to know how to get free calls. When I was a kid, we had a payphone in our apartment complex which was used quite heavily. One day I noticed that the conduit which housed the wiring to the phone had been tampered with and the wires were pulled out, providing bare wires. There were four wires (red, black, green, yellow). Upon a little investigation, I found that the red and green provided a dialtone if you hooked up a regular phone to it. I also immediately noticed that you couldn't complete a call because the line was different. I figured it was a special payphone line and you had to use a payphone to make it work.

Now, I was discussing this very thing with a person at a local hacker meet who shall remain nameless. He told me that I was wrong and that you could hook up any phone to the line and complete a call without doing anything overly creative. Granted, I'm not a hacker per se, but I know what I know. Can you provide any insight on this subject to satisfy my own personal curiosity? Thanks

Sky M.
Routed: Snail mail

Hello Sky. Well, you're both correct. I'll make the distinction for you. The phone you were dealing with was a phone company owned payphone which actually connects to the switching office quite differently from a "normal" phone. It requires tones which are generated from the phone to tell the switching office to allow the call to go through, etc. This is where the red box usually comes into play. Having a normal phone connected to this line will prove useless in your situation. Anyhow, your hacker buddy is referring to a COCOT (customer owned coin operated telephone) which is a completely different beast from a normal phone company payphone. The COCOT is actually connected to a normal phone line and does all the money calculations itself. If the wires it's connected to were accessed, a normal phone should be able to place any call to any location.

Dear Blacklisted! 411,

I just crashed my computer and decided to build a whole new machine rather than try repairing this old POS. I've been using Outlook (not Outlook Express) on XP and I want to copy over all of my email information from my old PC to the new PC. For the life of me, I can't figure out where the data files are located. It's nothing like Outlook Express. Can you help me?

Jason J.
Routed: Snail Mail

Hi Jason. We get this question a lot. The solution is easy. As long as you have access to the hard drive of the crashed machine, look in the following directory:

Documents and Settings\<username>\Local Settings] Application Data\Microsoft\Outlook\

The copy the two files over:

extend.dat
outlook.pst

That should do it. Note: <username> in the above refers to the name of the windows account you're trying to access.

Dear Blacklisted! 411,

I have a question regarding data recovery. One of my hard drives died on me recently and I've been trying to find a reputable company which can recover my data and not rip me off at the same time. Do you guys have a recommendation for me?

Scarface
Routed: Internet

Hi Scarface. Sure, I can recommend a place to you. We've been using this place on and off for the last 20 years. They have decent pricing and they negotiate. If you're not in a hurry, they will take that into consideration and lower the price accordingly. By the way, they have a 100% full recovery success rate with us. Incredible! Here's their information:

DriveSavers Data Recovery,Inc.
400 Bel Marin Keys Blvd
Novato, CA 94949
800-440-1904 voice
415-382-2000 voice
415-883-0780 fax
http://www.drivesavers.com

We love these people! Good luck with your hard drive woes. Been there and know how awful it can be.

Dear Blacklisted! 411,

I've made the switch to firefox (version 0.8) upon your recommendation. I love the browser, it's so much better than the other one. Anyhow, I was trying to find the bookmarks, but I have no idea where they are stored. Can you direct me? Thanks guys.

Rowdy Rob
Routed: Internet

Rob, you should upgrade to the newest version of firefox ASAP. I believe it's up to version 1.0.5 now. Anyhow, here's where you can find the bookmarks. It's contained in an HTML file here:

Documents and Settings\<username>\Application Data \Phoenix\Profiles\default\nv3rnqaq.slt

The filename is bookmarks.html

Enjoy.

Dear Blacklisted! 411,

I absolutely love your magazine. I've been reading the other one on and off for a few years but I couldn't get into their political agenda. Anyhow, I've read your last two issue and think you're doing a great job. I have a question for you. I've finally jumped on board with the MP3 craze and I want to convert my entire CD library (1200+ CD's) into MP3's for my own personal use (iPOD). Can you make any recommendations to me on what program to use to make my conversion process a little easier on me? I looked on the internet and there are too many to choose from, so I would rather look to you guys for the path I should follow.

CrabCakes
Routed: Internet

Hey Crabs, this one should be simple enough. Years ago, there was a top notch program for CD-to-MP3 conversion. It was called Audio Catalyst. All of us over here loved that *program. Anyhow, the same guy who made that program (and subsequently sold it to Xing) later came up with a shareware CD-to-MP3 converter program called "Audio Grabber" (available at www.audiograbber.com). It has since become freeware and it's the BEST little converter program on the market. It's free. You can't beat that. The latest version is 1.83 and I just upgraded to it just now, while writing this response to your question. Anyhow, what I personally like about this program is that it has access to the FreeDB built in. What does this mean? Oh, it means a lot! You plop a CD into your CDROM drive, click the "Freedb" button and the CD tracks are automatically recognized and the titles are entered in for you. Talk about a piece of cake. You can convert at a high rate with this little program. It gets a solid 5 stars in my book.*

Dear Blacklisted! 411,

I was wondering if you guys give out free copies/ subscriptions to residents of the prison system? I'm not going to offer you a long sob story. I just want to know if this is something you do. If it is, please hook me up. Thanks

Inmate 007
Routed: Snail Mail

Greetings inmate. Yes, as a matter of fact, we do offer free subscriptions and sample copies to prisoners. All you have to do is send us a letter and make the request. There is, however, a very serious problem with this freebie program. Yes, we send out the free copies every quarter, but some of those copies get returned to us, rejected by the prison as inappropriate material. We try to do right by you guys, but the man is cutting you off. All we can do is continue to try our best to keep you in the loop. Good luck.

Dear Blacklisted! 411,

First off, love your zine. It kicks ass. But you already knew that, I'm sure. Ok, so on to my question. I'm aggravated half to death over here. I've got two files here named: file.bin and file.cue. I'm using Nero and I have the files handy, but I can't figure out how to burn these onto a CD so I can use them. I've asked around but nobody will answer my question. So I turn to you since I know you'll answer me. I just hate to wait for the answer to get to me. Help me!!!

Burn Baby
Routed: Internet

Greetings burn baby. No problem on the help. This is a standard BIN/CUE image. Here's the process. For reference, I'm looking at Nero Burning ROM Ver. 5

1. *Fire up Nero*
2. *Click on "file"*
3. *Click on "Burn Image" <box will open>*
4. *Browse over to the directory that contains your files.*
5. *Select the file.cue file and click OPEN*
6. *Insert blank media into CDROM burner.*
7. *Verify information in "Write CD" box*
8. *Make sure you have write method set to "Disc at once"*
9. *Click WRITE*

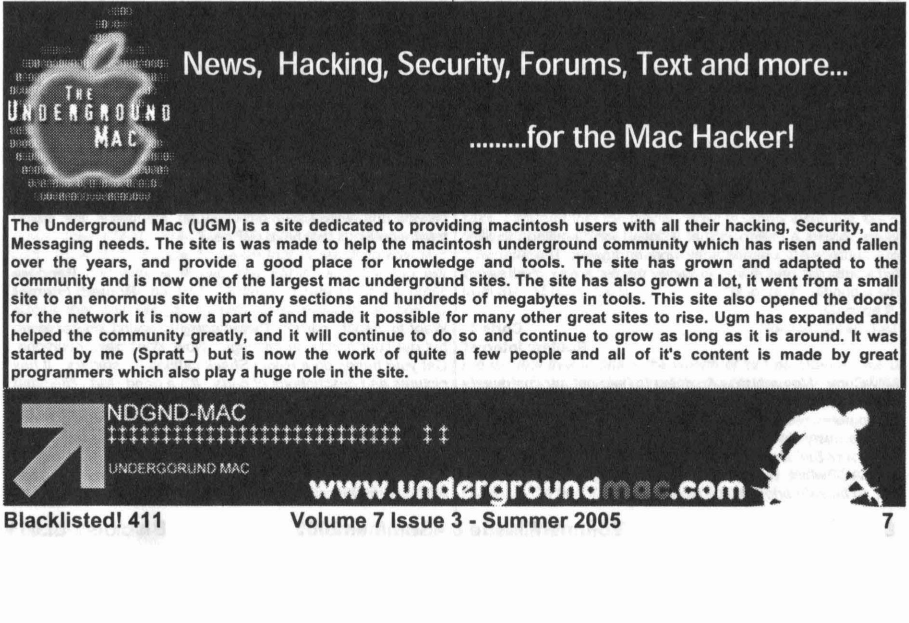
You're done. You will have a working CD with your information burned correctly.

Dear Blacklisted! 411,

Ok, I read about your DVD deal. It sounds really interesting. Can you tell me more? I've been waiting for you guys to put something like this out for awhile now. You're the only hacker magazine out there who seems to have a finger on the pulse of the community, have a good attitude and have the backing to do the crazy and interesting things we all wish we could do. From one hacker to another, I'm dyin' to see what you come up with. Did I read that right? I'll get a free copy of the DVD because I'm a subscriber? That's just too cool! You guys going to have it ready by Defcon? That would be ideal for you, I would imagine.

E. Coli
Routed: Internet

Hey E. Coli. It's all true. I mentioned a little bit more about the DVD in the letter from the editor in this issue. All the current subscribers will get a free copy of the DVD. It's going to sell retail for around $20 and we already have the whole distribution plan in order. We have a preorder/interest website up at the time of this writing. You can get to it from our main website or directly at www.hackthesystemdvd.com. We were hoping to have the DVD prepared for a release at Defcon, but it's just not going to happen. We have a lot more footage than we ever planned on getting, some of this stuff is really good. We decided to go a step further and provide "extras" on the DVD. Anyhow, it's pushed the release timeframe back quite a bit. So, that's a NO on a release of the DVD at Defcon. Oh, and thanks for the compliments. We like to hear how pretty we are.



Dear Blacklisted 411,

I'm a first time reader of your great magazine. I picked up your latest copy at Borders a couple of days ago and was surprised and shocked at what I read. I've been a devout fan and supporter of the hacker "movement" since I was a teenager in the 80's and I've been following with your East Coast "counterpart" for years. They've become somewhat extremist with their political agenda if you ask me. Yes, came from the Commodore 64 and an Amiga 2000 era., so I have some better background on the "old school" hacking ideals. Granted, I didn't get too involved with hands-on like you guys, but I've had my share of fun times. I think you guys are doing the community a great service here and I support you fully. Be on the lookout for my paid subscription.

Now for my question. I know this isn't exactly a hacking question, but I'm sure one of you can help me out here. As you've undoubted noticed, it's been hot as hell here in SoCal for the last few weeks. Well, my central A/C stopped functioning correctly last week and I've been dying in the heat ever since. I called out the AC repair guys and they told it would cost at least $500 (no free estimates here, baby) and they wouldn't even come and see it unless I was prepared to pay them on the spot.

The symptoms are pretty vague, but here's what has been going on. I turn on the AC and it starts running. I can hear it operating from inside the house. I can feel a very light breeze coming from the vents (and what I do feel is cold). The outside unit is running (the fan is spinning). But the house isn't cooling down at all. HELP! Ok, so I'm cheap. I don't want to pay someone $500 if I can fix it myself.

Chris T.
Routed: Internet

Hey Chris. First of all, thank you for the compliments. It's always nice to hear that people like what we're doing. We try to keep it as interesting as possible. Anyhow, your question has to be one of the more off-topic ones I've seen in awhile. However, I have a few suggestions for you anyhow. Given your supplied information, I would have to say that either your airflow is clogged or the blower is failing. Let's assume you have a clog. Have you changed the filter? I know it's obvious, but people seem to forget that air conditioners have filters. I worked in the HVAC industry for a few years, so I've been witness to this problem many times. If you live in a newer home, your filter will either be located in the garage where your evaporator unit is installed or along the ceiling in or wall your hallway. It's fairly easy to locate and I bet you know exactly where it is. Anyhow, pull it completely out and fire up your AC. If you can feel a strong wind coming out, you just saved yourself some big bucks. If not, the blower or possibly the blower controller is failing. In each case, swapping out either part will get you the answer.

[Note: In the interest of helping this guy survive the heat wave, this response was emailed]

Dear Blacklisted! 411,

Guys, thanks a million. What a dope I am! I pulled the filter out and my AC was instantly working again. The filter was thick with dirt and dust. Anyhow, thanks guys. You saved me a bundle. You rock!

Chris T.
Routed: Internet

Hey Chris. No problem. Anything to help out the community or our supporters. Now, don't forget to clean out the filter or buy a new one and REPLACE it back into the unit. The dust can do nasty things — the filter is there for a reason. With this crazy SoCal dust in the air, it won't take long to destroy your AC...which will be even more expensive to get around. Ok, so be safe and HACK THE SYSTEM!

Dear Blacklisted 411,

Your magazine kicks ass. I heard about you years ago, but your magazine wasn't around anymore. Everyone said you guys were an "old school" hacker magazine that bit the dust. So I was surprised to see your magazine at the campus bookstore! I loved your latest issue! The article on "interview with a hacker" sucked, but otherwise was a great success in my opinion. The Electronic Surveillance article by ML Shannon was a good read as was the Limited Resources article. Both of them were interesting. I know it's going to sound lame, but my favorite section was the "Review Corner" that you head up. I enjoyed reading about the things you mess around with and I took the time to look up each and every one of them online. Nice. So, I guess my only question to you would be, are you guys ever going to host a local meeting again? I heard that you guys used to hold a mean party back in the day and I'd like to join in on something like that! Peace out!

Drake
Routed: Internet

Hey Drake. Well, thanks for the words of encouragement. With regard to your question, we've been dying to host a party (or meet) like we did back in the old days. We've actually come up with a plan to hold an end of summer beach meet this year! No kidding. We're planning on giving away all kinds of stuff and feeding as many people as we can. We'll even be filming for our upcoming DVD. So, if you want to come out for a day in the sun with your hacker friends, head on over. You can read about it in this issue. Look for the full page ad.

Dear Blacklisted! 411,

First, does red boxing still work? A simple yes or no will suffice. If yes, what are the specific tones generated by the payphone when a nickel, dime or quarter is inserted? Please include tone duration, etc. If no, why all the hype about red boxing? It seems that there are quite a few arguments about whether red boxing really works or not.

Zurg
Routed: Snail mail

Red boxing still works. YES. You have to use it under the right circumstances before it will work, however. I will not say anymore than that. The tones generated are 1700 hz and 2200 hz mixed together - called DTMF (much like that of the tones generated by depressing keys on the keypad of the phone) The duration of the tone for each coin is as follows:
Nickel - 66 ms on (1 beep).
Dime - 66ms on, 66ms off, 66ms on (2 beeps).
Quarter - 33ms on, 33ms off repeated 5 times.

Dear Blacklisted! 411,

I've been collecting parts and components from a few of the salvage yards you mentioned in your recent issue. GREAT articles, by the way! Anyhow, I was wondering if you can provide me with some direction on identifying the parts, maybe catalogs that have pictures?

Pandora
Routed: Internet

Want to identify parts? This is going to sound kind of lame, but get your hands on catalogs. Now, don't gasp everyone. Get your hands on a Radio Shack catalog for starters. It has pictures and descriptions of parts. It's a good start. Next, get some catalogs from places like:

JDR Microdevices
1850 South 10th Street
San Jose, CA 95112
(800)538-5005

Mouser Electronics
11433 Woodside Avenue
Santee, CA 92071
(800)992-9943

MECI
340 E. First Street
Dayton, OH 45402
(800)344-4465
http://www.meci.com

Marlin P. Jones & Assoc. Inc.
P.O. Box 12685
Lake Park, FL 33403-0685
(800)652-6733

All Electronics
905 S. vermont Avenue
Los Angeles, CA 90006
(213)380-8000
(800)826-5432
http://www.allcorp.com

Digikey
701 Brooks Ave. South
Thief River Falls, MN 56701-0677
(800)344-4539
http://www.digikey.com

Jameco Electronics
1355 Shoreway Road
Belmont, CA 94002
(800)237-6948
http:www.jameco.com

Contact these people and get their catalogs. It will help you out quite a bit. Also, see if you can grab up old copies (from the 80's) of Jameco catalogs - they have some of the best pictures and descriptions of components. Oh, you might want to find an old copy of the ACP Superstore catalog. I still have my copy and use it often.

Dear Blacklisted 411,

I just picked up a copy of your guys mag at our Borders. This magazine kicks major ass. You guys have easy to understand articles and not junked up technical shit. Anyway, I was wondering how I go about building my own pirate radio. if you could send me the instructions on how to build it and what I need to build it, I would be most appreciative, I'll even send an article for each of your issues just to help move your business along. Anyway thanx alot!

Prototype
Routed: Snail mail

We don't have our own schematics to give out, but we can send you in the right direction. Start here:

http://www.ramseyelectronics.com/

Check out their site, request their catalog and consider buying their FM-10, FM-25 or FM-100 setup to play around with. It's a start. Please be aware that transmitting anything over 100 Milliwatts is illegal. The FM-25 and FM-100 will transmit far above this limit, I believe. There are many other places that sell kits (along with documentation on how to construct and operate them, as well).

Dear 411,

This is the first time I have ever seen your magazine. I found Vol. 7, Issue 2 at my local Borders. I have to say that I think it's the best damn magazine I have ever read. I bought it because I am very interested in the world of hacking. I grew up in the 80's along with the rest of the Nintendo generation. I just about defeated and conquered every game in 1 week that my dad could throw in my face to keep me busy. After awhile he got tired of buying me games and so he started carrying video games at his pizza place. I beat all them too and he got angry me asking him to get a new arcade game every other week. And so as the rest of life goes we got our first computer in '91. I hated it. It scared me. The first thing to actually frighten me so I stayed away from it until about late '96. Yeah I know it was a long time to stay away from a computer and I sure as hell regret that now. Well, I did use it periodically for AOL. Then in '97 I got into the warez scene and then gradually became curious about hacking. I know it's kind of late for me to jump on this hacking thing. I should have started right after vid games were too easy. I went to the sites u guys mentioned were good for beginners to go too and then I clicked on the links to DL the linux, but I just got confused. There are a lot of DL files there and I don't know which ones I need. What do I need to make emulators of video games and systems to comp with.

Roman H.
Routed: Snail mail

Most of us over here who grew up in the 80's and remember the arcade industry at it's best (and it's worst) like to refer to ourselves as coming from the "Atari, Commodore or Apple Age" ... Go figure. Anyway, there's no point to be made, really.

Ok, so you started a little late. No big deal. What you do with your time NOW determines where you will fit into the hacker community. All I can recommend to you is to read, read and read some more. If you have questions and you want the answer immediately, do a search on Google. Surprisingly, you can find answers to many of your questions right there.

I'm going to touch on the emulators you mentioned. MAME - Multi Arcade Machine Emulator. If you don't want to go out and buy the old video arcade games, this is the program of choice. You can run it on you IBM compatible (possibly other platforms, but not sure) and it will allow you to run hundreds of the old video arcade games by use of the original ROM (or EPROM) code from the actual game. Look for it on the internet. Use the skills you already have. MAME. Visit them at http://www.mame.net/

Dear Blacklisted! 411,

Just wanted to say that Blacklisted! 411 is a great mag & to keep up the good work. I just discovered it last year and not a moment too late. It's been getting harder & harder for me to walk into a bookstore & find material worth reading. So much commercialized bullshit dogs the shelves. Anyway, I'm down w/ your mag since its right up my alley. I've been into the hacker scene for a little less than 2 yrs & find it fascinating. Prior to that, however, I was a serious hustler involved in all types of ill shit. During that time, I stacked cash while scheming the next plot. I had some wild times along w/ some situations & events that wised me up & changed my life for the better. Now I'm a seeker of knowledge for knowledge sake. I learned that the (know - how) is widely available, but it doesn't come with the wisdom to know when & why to apply it. I do lots of research on a variety of topics & would love to share them w/ you along w/ some of my tales of shadiness from the old days. Later

George F.
Routed: Snail mail

Please feel free to share the wealth of info as often as you'd like. Glad you decided to hop on over to the other side of the "hacker fence" so to speak. Also, you might want to take a look at our siter publication - The Hackers Underground Digest. THUD. It should be on the shelves alond with this and your other favorite hacker rags. If not, send them an article to print and get a free 1yr sub. THUD, P.O. Box 2521, Cypress, CA 90630. Tell them Zack sent ya!

Dear Blacklisted 411,

Nice to see you guys back again. The Mac Spoofing article you guys did way back in 1998 is what got me hooked on your magazine but you weren't around much longer after that. That's ok, crap happens and now you're back. Speaking of which, I about crapped my pants when I saw Volume 6, Issue 1 sitting on the shelf of the magazine rack. Naturally, I had to grab it, knocking someone out of the way to get to it. :-)

I took the time to check out your website—good job! I'm impressed with your comeback. You seem to have it all tied up and everything back together again. I've been dabbling in electronics for the last few years and have made a lot of headway so far. I want to further this experience and hope you can help. Will you be offering any build projects or any pointers on manufacturing circuit boards, soldering, etc? Hope you guys are around for the long haul. Missed you.

A. Zacks
Routed: Snail mail

Thanks for the welcome back. It was a long time coming, but we're back and plan to stick around. We're also planning on having some projects in an upcoming issue, so stay tuned. Congrats on getting into electronics. It's fun stuff.

Blacklisted! 411,

I'm writing to ask you for information about the SEC program in Ontario, California. I know someone with a "ghetto pager" and wanted to know if you could provide ANY insight on the device; it's real-world range, frequency, operation, phone numbers, etc. Any information on why they won't allow you to have extra service on the phone line that the box is connected to? I can understand no answering machine, but why no caller ID, etc? Last, why can't you have someone else who is on the program in your home?

Tech Angle
Routed: Snail mail

Greetings Tech Angle. The SEC program is actually referred to as the "S.E.C.P." in Riverside country and run by the Sheriff's Dept. out of Banning, CA. Their exact address is 1627 S. Hargrave St., Banning, CA 92220. The device you speak of is an "ankle bracelet" and accompanying receiving box (called HomeGuard 200) made by BI Incorporated (www.bi.com) and monitored by Sentinel, a company based out of Irvine, CA.

Many people think the bracelet is a GPS unit, capable of keeping a constant record of your physical location. While it's true that there are versions of this device which do exactly that, the bracelet used in Riverside country is not the same unit. It's a much more simple unit which only transmits a frequency which "announces" it's presence to make sure the subject is within the range of the receiving box.

The box has three lights on it to indicate phone, range and power. When the box is receiving a call or calling out to report (usually when the subject returns after being out of range for some time), the phone light will flash. When the subject begins to exceed the range of the receiving box, the range light will begin to flash. Once the subject has been out of range long enough (time varies), the range light will turn off. The power light is pretty obvious. The receiving box has a battery backup in case there is a power outage which will keep the unit running for up to 48 hours.

Let's talk about range. The manufacturer claims the unit has a range of approximately 300 ft. In the real world, it's more like 100 ft. Frequency: They operate in the 300Mhz band. We need an actual unit to get the specific frequency for you.

Extra phone services. Caller ID: they don't want you to have caller ID so you won't know the monitoring phone numbers that occasionally call back and exchange information with the unit. Answering machines and fax machines - they don't want any device on the line which can answer incoming calls - this could interfere with the receiving box. Same pretty much goes with three way, call waiting, etc. Incidentally, the Sentinel monitoring phone number (the number that calls the boxes) is (949)453-8178.

Apparently, the bracelets are fairly dumb devices and their only job is to constantly transmit a frequency to allow the receiving box to "know" you're within proximity. Because of this, if you have a buddy on the same program, you could theoretically stay at his place overnight and he at yours overnight and the monitoring people would never suspect any wrongdoing. This would defeat the purpose of the supervised electronic confinement program, thus put you in a bad position if caught.

The bracelets, about the size of a small pager, must be in contact with the skin of the subject at all times. If it's pulled away from the skin, it triggers an internal tamper device, which in turn alerts the monitoring company that you've "removed" the device from your person. In addition, the rubber band of the device is reinforced with metal wires. Naturally, cutting through this triggers the tamper switch as well. It has an internal battery which is reported to keep the unit operating for 12 months.

This was an interesting question. If any readers have further information on the topic, please forward it to us.

Blacklisted! 411,

I'm need some help guys. I've been interested in finding more surplus electronics I can purchase for low prices. Most of the electronics stores around my area are either gone or have slimmed down their product line to the point where they are no longer useful to me. Can you guide me? Thanx.

Lord Soth
Routed: Internet

Sure we can help you on this one. First, check out the Serious Salvage Part II article on page 46 of this issue and the first part in the last issue. They're both great sources for parts. Also check out the Surplus Sources article in the last issue on page 40 and 55 of this issue. There are a lot of great sources listed there. Last, you have to visit the following place because they're so close to you:

California Electronic & Industrial Supply
221 N. Johnson
El Cajon, CA 92020
Tel: (619)588-5599
Fax: (619)588-0371
Toll Free (866)CAL-ELEC
URL: www.californiaelectronic.com
Ebay ID: calelectron

They sell on ebay, have a nice big place full of surplus electronics and they will deal. If they have something you want, start negotiations off at 10% of their asking price and work your way up. We've been buying stuff from this place since before we started up Blacklisted! 411. They've been around a long time and they're probably going to stay around even longer.

Blacklisted! 411,

I've always enjoyed your magazine and THUD. I'm glad to see you back after all these years. I figured you were down and out for good after Y2K had come and gone...another one bites the dust. And now you're back!! You were right on the money with your suggestions and comments on the Y2K subject back in 1999 and you ended up saving myself and the company I work for a tremendous amount of money. I just thought it would only be right to let you know how useful and appreciated the information you provide really is. Thanks guys. I'll keep reading and tell all my friends you're back.

Rodney P28
Routed: Internet

We aim to please. We're all glad we could be of so much help to you and your company. If you need any tips on any subject in the future, let us know.

Blacklisted! 411,

First of all, I think you guys have a great magazine and I'd like to see some more issues come out soon!! I've seen your magazine referred to as a "hacking" magazine and a "phreaking" magazine. I've had this discussion with a few people and the consensus tends to be that you are a "phreaking" magazine. Forgive me, but can you define the difference between the two types and which you claim to be? Thank you.

Careful LOA
Routed: Snail Mail

This has always been a point of debate. Let's get down to the basics and then we'll address the issue of what we are all about.

Hacking is creative problem solving by use of available technology. In other words, by use of technology, someone may creatively use and/or modify this technology to get around a problem, limitation or lack of a necessity, usually in the form of needing a tool or some type of access device.

Phreaking on the other hand is an extension, or rather a very specific area <sub culture, even>, of hacking which primarily deals with telecommunications, telephones and long distance service. This type of "hacking" usually requires a hacker to use any number of colored boxes and/or tricks to manipulate access to telephone systems. Anything from red boxing for free phone calls to accessing a PBX system for any number of reasons can be considered "phreaking". This type of hacking has been referred to as "phreaking" for quite some time, however referring to it as hacking isn't completely inappropriate even with the multitude of individuals who claim there is a big difference. Phreaking, just like hacking, is basically used in an effort to gain knowledge on how a system works, finding inherent faults and exploiting these faults in any number of ways.

With all of this said, we maintain that we are at the most generic level of this area and refer to our magazine as a "hacking" magazine. We will cover topics on every aspect of technology, including but not limited to computers, internet, electronics, telecommunications , radio. Because of this, our topics will include what people would define as "phreaking" material. Regardless, this does not make Blacklisted! 411 a "phreaking" magazine. We welcome all technology related topics. Thanks for reading.

BL411,

Doodz! I'm very new to the hacking scene and I wanted a few pointers. I have a few questions for you. I've searched the net and have learned quite a bit using this method.

I am also interested in actual books or magazines I can get a hold of. Can you recommend anything to me? Can you give me any ANAC's for the Dallas TX area? CNA - do you have any numbers to get in touch with one of these services? I have more questions but I will save them for later. Thanks guys.

Garbaggie
Routed: Snail Mail

Here are a few books we'd recommend:

How to Investigate Your Friends, Enemies, & Lovers by Trent Sands & John Q. Newman, ISBN 156866143б

Radio Monitoring: The How-to Guide
by T.J. Arey, N2EI
ASIN 1568661010

Scanners & Secret Frequencies
by Henry L. Eisenson
ASIN 1568660383

Java Security: Hostile Applets, Holes & Antidotes
by Gary McGraw, Edward Fellen, Edward Felten
ISBN 047117842X

The Underground Database
ISBN 156866043X

Privacy Power: Protecting Your Personal Privacy in the Digital Age
by Trent Sands
ISBN 1568661118

Computer Security Handbook (3rd ed.)
by Arthur E. Hutt, Seymour Bosworth, Douglas B. Hoyt
ISBN 0471118540

Acquiring New Id: How to Easily Use the Latest Computer Technology to Drop Out, Start Over, and Get on With Your Life
by Ragnar Benson
ISBN 0873648943

The Modern Identity Changer: How to Create a New Identity for Privacy and Personal Freedom
by Sheldon Charrett
ISBN 087364946X

Web Security Sourcebook
by Marcus Ranum, Avi Rubin and Dan Geer
ISBN 047118148X

This should help you along. We also recommend 2600 magazine, Nut & Volts, Wired and Iron Feather Journal.

Here are the ANAC numbers for the Dallas (214) area:

570 Dallas, TX
790 Dallas, TX (GTE)
970 Dallas, TX (GTE)
970-222-2222 Dallas, TX (SWB)
970-x11-1111 Dallas, TX (SWB)

On the topic of CNA. For those of you who do not know what a CNA is, it means "Customer Name and Address". Phone company personnel out in the field use these to locate the address for a phone line they may be working on. People can use these to find the address of someone they only have the phone number for, but it's usually reserved for phone company personnel alone. However, there are a few companies out there who provide this same service....for a price:

AT&T National Directory Assistance (900)555-1212
Cross-Reference Directories (900)288-3020
Telename (900)884-1212
Unidirectory (900)933-3330

If paying isn't your thing, you can always use a little social engineering and get the information out of the phone company or even dominoes pizza. The Dominoes pizza trick is very old, but it still works. Call them up, order a pizza and give them the number you need the address of. If the person you're looking for has ever ordered from that Dominoes, with the phone number you provided they'll come back with a name and address to verify if they've got the right person.

OPERATION FIREWALL:

The Secret Service Strikes Back

Here is a fascinating story about the information economy, globalization, cyber-crooks, Feds, and how one writer got a little too close for comfort researching this article.

In an investigation of epic proportions, the Secret Service in association with the U.S. Dept. of Justice, U.S. Department of State, the U.K. National Hi-Tech Crimes Unit, the Vancouver, B.C., Police Department's Financial Crimes Section, the Royal Canadian Mounted Police, Europol and local agencies in Bulgaria, Belarus, Poland, Sweden, the Netherlands, *and* the Ukraine *gasp*.. busted and arrested 28 suspects in 8 states and 6 foreign countries. The suspects are facing charges of identity theft, credit card fraud, computer fraud, and conspiracy, among others. The investigation began on the internet and went as far as a passport forging facility in Bulgaria.

The investigation began in July 2003 when the Secret Service, which is now part of the U.S. Department of Homeland Security, began investigating an "unspecified financial crime."

The yearlong investigation, is the third in as many months targeting organized cybercrime.

In August, the FBI seized computers in five states as part of Operation Digital Gridlock, the first federal action against criminal copyright piracy of movies, games, software, and music over peer-to-peer networks. Also in August, the FBI's Operation Web Snare snapped up more than 150 suspects in a variety of cybercrimes, including spamming, identity theft, and hacking.

Once on-line, the Feds soon discovered what many cyber crooks already knew, that a loose-knit global network exists that caters to carders and ID thieves of every stripe, and they do so thru on-line forums like **Carderplanet**, **Darkprofits**, and **Shadowcrew.com** .

On October 28th, the Secret Service issued a press release detailing the busts and revealing **Operation Firewall** to the world. The 28 suspects are believed to have trafficked in at least 1.7 million stolen credit-card numbers, with losses to financial institutions of over $4.3 million. Estimates of potential damages if the gangs hadn't been broken up range into the hundreds of millions, the agency said. Keep in mind these are "estimates". And to be fair, L.E. (law-enforcement) tends to over-estimate and get a little carried away with their "creative estimates" to beef up the numbers so as to look like every bust is an award-winning bust, and worthy of recognition and publicity. For example, I've seen pot dealers get busted with 3 lbs. of dope.

Not a lot of weight in the grand scheme of things, but perfect for my example.

After confuscating it and weighing it out, it appears there is only 1 actual pound of grass, and 2 lbs. of shake, sticks n beans. Crap. Not worth a thing on the "streets", or more likely, not worth anything to local potheads looking for weekend smoke. The dealer still gets charged and to the cops, there is no discrepancy between saleable weed and non-saleable weed. Even though 2 lbs. were worthless, that extra weight is treated as if it was real, usable marijuana and will add to his sentence. In other words, the judge and prosecutor will look at you like you got busted with 3 lbs. for sale, worth lets say $6,000 estimated street value. When in reality, the stash was probably worth $2,000 on the street and the rest was garfo. The Man does not care, even though they know the truth. They will charge you with all the weight, and stick the highest possible estimate on it to make you look worse than you really are. But I digress, I don't know the intimate details of the financial information they recovered or its value, and financial info isn't marijuana. I just wanted to illustrate that estimates are just that, estimates, and need to be taken with a grain of salt. Just because you have a million credit card numbers doesn't mean they are all valid, or even worth anything.

"Information is the world's new currency," said W. Ralph Basham, director of the Secret Service, in a statement. "These suspects targeted the personal and financial information of ordinary citizens as well as the confidential and proprietary information of companies engaged in E-commerce." Truly the world is evolving. If information is the new currency, then crime is truly a industry. There are people who look at criminal activity as a real job. Crime is a billion dollar industry, and anyone that doubts it just isn't paying attention. Case in point; The on-line portals that were busted in this operation have been operating for at least a year, probably 2, maybe more. I seem to remember seeing Carderplanet and Darkprofits around for a long time. And I'm sure many of you remember getting those emails from Darkprofits claiming:

"Welcome to the site www.darkprofits.com, it's us again, now we extended our offerings, here is a list: 1. Heroin, in liquid and crystal form. 2. Rocket fuel and Tomohawk rockets (serious enquiries only). 3. Other rockets (Air-to-Air), orders in batches of 10. 4. New shipment of cocaine has arrived, buy 9 grams and get 10th for free. 5. We also offer gay-slaves for sale, we offer only such service on the NET, you can choose the one you like, then get straight to business. 6. Fake currencies, such as Euros and US dollars, prices would match competition. 7. Also, as always, we offer widest range of child pornography and exclusive lolita galleries, to keep out clients busy. Everyone is welcome, be it in States or any other place worldwide. ATTENTION. Clearance offer. Buy 30 grams of heroin, get 5 free. Prepay your batch of rockets (air-to-air) and recieve a portable rocket-lacuncher for free. www.darkprofits.com This offer won't last! Only until 20th of August all our clients will also recieve a pack of 2 CDs, with best selection of child pornography.

LOL. I remember getting this email. I also remember getting like 3-4 similar ones in the last year. Needless to say, its not true. It was something of a hoax perpetrated supposedly by a former disgruntled member according to <http://www.snopes.com/inboxer/hoaxes/joejobs/darkprofits01.asp>

As a disclaimer on the DarkProfits site explained (with a touch of sarcasm), the August 2003 spam was yet another "joe job". A "joe job" is the sending out of spam using someone else's return address, thus getting a bunch of people pissed off at that someone else.

Darkprofits.net really doesn't sell any of that stuff, but they are far from law-abiding citizens.

They host a "Underworld Entrepreneurs Network" message board, much like www.shadowcrew.com <http://www.shadowcrew.com/> which brings me back to how I discovered Operation Firewall in the first place. It was back in September when I learned of shadowcrew.com

I decided to do some research. I thought I would have a look around the board, which I did.

I even registered as a member. It was obvious to me that the purpose of this board was to trade information on how to commit many types of fraud, connections for counterfeit credit cards and fake ID's, as well as tools for producing cards and bogus ID documents ranging from passports to birth certificates. Even the advertising on the site alluded to "fast cars, big money, and women" which could be obtained by "playing in the shadows." It was a cornucopia of underground information, connections, and tools to get in the game. At any rate, I browsed around a little bit, but then put it on the backburner due to more pressing personal issues. A few weeks later, I went back to look around again. What I saw when I went to the site shocked me so, that I almost fell out of my chair. (Maybe use a screen shot to show the actual page) (here is the text)

This is what I saw…

**ACTIVITIES BY SHADOWCREW MEMBERS ARE BEING INVESTIGATED BY THE
UNITED STATES
SECRET SERVICE**

SEVERAL ARRESTS HAVE RECENTLY BEEN MADE...WITH MANY MORE TO FOLLOW.

Proxies, VPNs, IP Spoofing, Encryption, etc.... You Are No Longer Anonymous!!

**SHADOWCREW MEMBERS ARE FACING THE FOLLOWING CHARGES
(*Charges are Not Limited to Below):**

TITLE 18 USC 371 - CONSPIRACY

TITLE 18 USC 1029 - ACCESS DEVICE FRAUD

TITLE 18 USC 1028 - FRAUD W/IDENTITY DOCUMENTS, IDENTITY THEFT, ETC

TITLE 18 USC 1030 - FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

IF YOU ARE A MEMBER WHO IS CONFUSED AND/OR CONCERNED BY YOUR ACTIONS...PLEASE READ THE FOLLOWING:

RECENT NEWS REPORTS SHOULD INFORM YOU THAT THE SECRET SERVICE IS INVESTIGATING YOUR CRIMINAL ACTIVITY.

CONTACT YOUR LOCAL UNITED STATES SECRET SERVICE FIELD OFFICE....*__BEFORE__ WE CONTACT YOU!*

Needless to say I was shocked and more than a little worried about my status since I was a registered member. According to the reports there were 4000 registered members, but only 28 were arrested so far. According to the new page the Secret Service installed, the investigation is on-going and more arrests will be made. I was merely a casual observer, there only to watch and listen and perhaps come up with an idea for an article. I guess my plan worked! Although not quite the way I imagined it. Now, as a result of being a member of this site, I will no doubt be added to all the databases these individual law enforcement agencies have regarding this operation.

This will now be my second entry into the files of the Secret Service, since I was already arrested by them once in a completely un-related matter. Now I will appear again, my name attached in a very unflattering manner to this global investigation. My name will also be in the Dept. of Homeland Security, and all the rest of the agencies that took part in this operation. That sucks.

I was in the proverbial 'wrong place, at the wrong time.' So far, nobody has contacted me regarding this. And since I never posted, or even spoke to another member on the site, I don't see how they could try to charge me with conspiracy. Its not out of the realm of possibility, in fact, they hint that they will be contacting everyone, but I don't believe I did anything wrong, and therefore, hope I won't be charged with anything. The lesson here is that if you know something shady is going on, and you insert yourself into it, or just observe (in my case) you are inviting trouble. This situation is proof.

It remains to be seen if anything is going to result from this, at least for me, but for the 28 guys already arrested, you can be sure they are going down, and probably more will soon follow as deals are made and more crimes are uncovered by other members. Carderplanet, Darkprofits and Shadowcrew might be out of commission for now, but sooner or later a new site will spring up to take their place and to pick up the slack. On-line criminal organizations are here to stay and one bust isn't gonna make 'em go away. What new forum will spring up next?

As for me, I'm going to start researching things that don't put me in jeopardy of criminal charges. Hhmm, maybe something like 'naked nympho aerobics' or 'horny housewife hackers'...sounds safer, and if it gets gonzo, I think I'll be ok to deal with it.

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

Virus & Worms

Jeremy Martin CISSP, ISSMP, ISSAP, CEI, CEH, CHFI, CCNA, Network+, A+
info@infosecprofessionals.com

Virus damage estimated at $55 billion in 2003. "SINGAPORE - Trend Micro Inc, the world's third-largest anti-virus software maker, said Friday that computer virus attacks cost global businesses an estimated $55 billion in damages in 2003, a sum that would rise this year. Companies lost roughly $20 billion to $30 billion in 2002 from the virus attacks, up from about $13 billion in 2001, according to various industry estimates." This was the story across thousands of news agencies desk January 2004. Out of $55 billion, how much did it cost your company? How much did it cost someone you know?

The purpose of this class is to inform the attendee about how malicious code works, how they spread, and how to protect yourself from infection. The most well know viruses will be covered in the first part of the presentations along with the most recent. The attendee will also learn several methods (while used in combination) that will minimize both risk of infection and potential damages caused by them.

The attendee should have a basic knowledge of computers and be familiar with the Microsoft Windows platform (Win9x, WinNT, Win2k, WinXP, Windows 2003 server).

I. The Why

There is an average of 10-20 viruses released every day. Very few of these viruses actually make "Wild" stage. Viruses are designed to take advantage of security flaws in software or operating systems. These flaws can be as blatant as Microsoft Windows NetBIOS shares to exploits using buffer overflows. Buffer overflows happen when an attacker sends responses to a program longer then what is expected. If the victim software is not designed well, then the attacker can overwrite the memory allocated to the software and execute malicious code.

People make viruses for various reasons. These reasons range from political to financial to notoriety to hacking tools to plain malicious intent.

Political: Mydoom is a good example of a virus that was spread with a political agenda. The two targets of this virus were Microsoft and The SCO Group. The SCO Group claims that they own a large portion of the Linux source code threatened to sue everyone using Linux operating systems (with "stolen" programming source). The virus was very effective knocking down SCO's website. However, Microsoft had enough time to prepare for the second attack and efficiently sidestepped disaster.

Financial: Some virus writers are hired by other parties to either leach financial data from a competitor or make the competitor look bad in the public eye. Industrial espionage is a high risk/high payout field that can land a person in prison for life.

Notoriety: There are some that write viruses for the sole purpose of getting their name out. This is great when the virus writers are script kiddies because this helps the authorities track them down. There are several famous viruses that have the author's email in the source code or open script

Hacking: Hackers sometimes write controlled viruses to assist in the access of a remote computer. They will add a payload to the virus such as a Trojan horse to allow easy access into the victims system.

Malious: These are the people that are the most dangerous. These are the blackhat hackers that code viruses for the sole intention of destroying networks and systems without prejudice. They get high on seeing the utter destruction of their creation, and are very rarely script kiddies.

Many of the viruses that are written and released are viruses altered by script kiddies. These viruses are known as generations of the original virus and are very rarely altered enough to be noticeable from the original. This stems back to the fact that script kiddies do not understand what the original code does and only alters what they recognize (file extension or victim's website). This lack of knowledge makes script kiddies very dangerous.

II. The How

Malicious code has been plaguing computer systems since before computers became a common household appliance. Viruses and worms are examples of malicious code designed to spread and cause a system to perform a function that it was not originally designed to do.

Viruses are programs that need to be activated or run before they are dangerous or spread. The computer system only becomes infected once the program is run and the payload has bee deployed. This is why Hackers and Crackers try to crash or restart a computer system once they copy a virus onto it.

There are four ways a virus can spread:
1.) Email
2.) Network
3.) Downloading or installing software
4.) Inserting infected media

Spreading through Email
Many emails spread when a user receives an infected email. When the user opens this email or previews it, the virus is now active and starts to immediately spread.

Spreading through Network

Many viruses are network aware. This means that they look for unsecured systems on the network and copy themselves to that system. This behavior destroys network performance and causes viruses to spread across your system like wildfire. Hackers and Crackers also use Internet and network connections to infect systems. They not only scan for unprotected systems, but they also target systems that have known software vulnerabilities. This is why keeping systems up to date is so important.

Spreading through manual installation

Installing software from downloads or disks increase the risk of infection. Only install trusted and scanned software that is known to be safe. Stay away from freeware and shareware products. These programs are known to contain Spyware, Adware, and viruses. It is also good policy to deny all Internet software that attempts to install itself unless explicitly needed.

Spreading through boot sectors

Some viruses corrupt the boot sector of disks. This means that if another disks scans the infected disk, the infection spreads. Boot sector viruses are automatically run immediately after the disk is inserted or hard drive connected.

III. Minimizing the effect of viruses and worms

We have all heard stories about the virus that destroyed mission critical company data, which cost companies months to recover and thousands of dollars and man-hours restoring the information. In the end, there are still many hours, costs, and would be profits that remain unaccounted. Some companies never recover fully from a devastating attack. Taking simple precautions can save your business

Anti-virus Software

Another step is to run an antivirus program on the local computer. Many antivirus programs offer live update software and automatically download the newest virus definitions minutes after they are released (Very important that you verify these updates weekly if not daily). Be careful of which antivirus program you chose. Installing a PC antivirus on a network can be more destructive on performance than a virus at work. Norton makes an effective corporate edition specifically designed for Windows NT Server and network environments. When using antivirus software on a network, configure it to ignore network drives and partitions. Only scan the local system and turn off the auto protection feature. The auto-protect constantly scans your network traffic and causes detrimental network issues. Corporate editions usually have this disabled by default. PC editions do not.

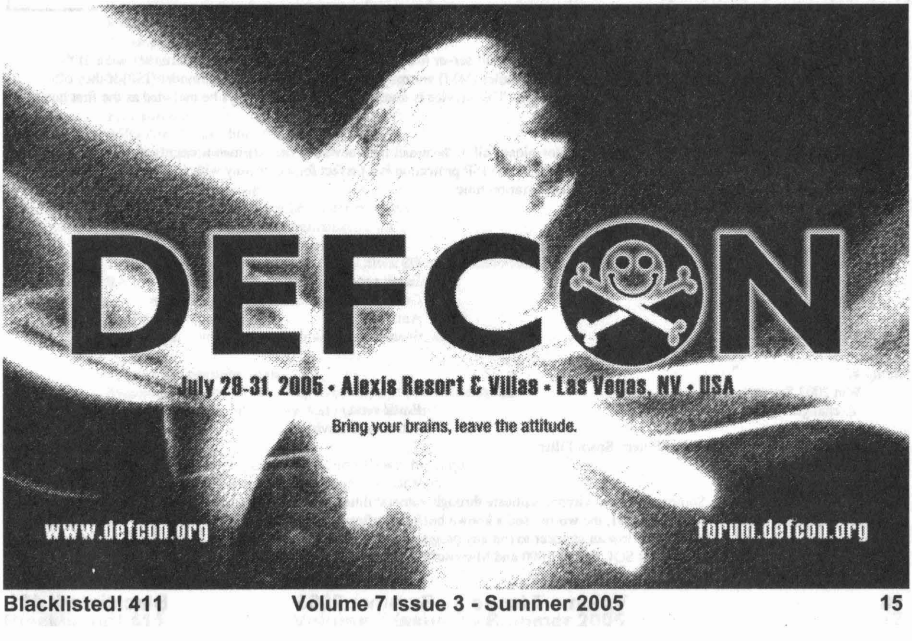
Email Clients

Do not open emails from unknown sources. If you have a website for e-commerce transactions or to act as a virtual business card, make sure that the emails come up with a preset subject. If the emails are being sent through server side design instead of the users email client, specify whom it is coming from so you know what emails to trust. Use common sense when looking at your email. If you see a strange email with an attachment, do not open it until you verify whom it came from. This is how most MM worms spread.

Disable preview panes in email clients. Email clients such as Outlook and Outlook Express have a feature that will allow you to preview the message when the email is highlighted. This is a *Major* security flaw and will instantly unleash a virus if the email is infected.

It is also a good idea to turn off the feature that enables the client to view HTML formatted emails. Most of these viruses and worms pass by using the html function "<iframe src>" and run the attached file within the email header.

We will take a quick look at an email with the subject header of "You're now infected" that will open a file called readme.exe.



```
Subject: You're now infected
MIME-Version: 1.0
Content-Type: multipart/related;
        type="multipart/alternative";
        boundary="====_ABC1234567890DEF_===="
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1
To: undisclosed-recipients:;

--====_ABC1234567890DEF_====
Content-Type: multipart/alternative;
        boundary="====_ABC0987654321DEF_====" *** (This calls the iframe)

--====_ABC0987654321DEF_====
Content-Type: text/html;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
<HTML><HEAD></HEAD><BODY bgColor=3D#ffffff>
<iframe src=3Dcid:EA4DMGBP9p height=3D0 width=3D0> *** (This calls readme.exe)
</iframe></BODY></HTML>

--====_ABC0987654321DEF_====--

--====_ABC1234567890DEF_====
Content-Type: audio/x-wav;
        name="readme.exe"       *** (This is the virus/worm)
Content-Transfer-Encoding: base64
Content-ID: <EA4DMGBP9p> *** (Notice the <iframe src=…>)


PCFETONUWVBFIEhUTUwgUFVCTElDICItLy9XM0MvL0RURCBIVE1MIDQuMCBUcmFuc2l0aW9u
YWwvL0VOIj4NIDxodG1sPg08aGVhZD4NPHRpdGxlPldobydzIHRoZSBiZXN0LS0tLS0tPyAt
IHd3dy5lemJvYXJkLmNvbTwvdGl0bGU+DQ0NDTxzY3JpcHQgbGFuZ3VhZ2U9amF2YXNjcmlw
dCBzcmM9aHR0cDovL3d3dzEuZXpib2FyZC5jb20vc3BjaC5qcz9jdXN0b21lcmlkPTExNDc0
NTgwODI+PC9zY3JpcHQ+DTxzY3JpcHQgbGFuZ3VhZ2U9ImphdmFzY3JpcHQiPg08IS0tDWZ1
bmN0aW9uIE1NX29wZW5CcldpbmRvdyh0aGVVUkwsd2luTmFtZSxmZWF0dXJlcykgeyAvL3Yy

*** Broken to protect the innocent.  (Worm is encoded in Base64)

aHJlZj1odHRwOi8vY2l0YWRlbDMuZXpib2FyZC5jb20vZmNhbGhpc3BvcnRzZnJtMT5Gb290
YmFsbDwvYT4NIA08Zm9udCBjb2xvcj0jRkYwMDAwPiAtIDwvZm9udD4NDTxicj48YnI+PGJy
Pjxicj5Qb3dlcmVkIEJ5IDxhIGhyZWY9aHR0cDovL3d3dy5lemJvYXJkLmNvbS8+ZXpib2Fy
ZK48L2E+IFZlci4gNi43LjE8YnI+Q29weXJpZ2h0IKkxOTk5LTIwMDEgZXpib2FyZCwgSW5j
Lg08L2NlbnRlcj4NPC9ib2R5Pg08L2h0bWw+DQ0NDQoNCj==

--====_ABC1234567890DEF_====--
```

Email Servers

The first step to minimizing the effect of viruses is to use an email server that filters incoming emails using antivirus software. If the server is kept up to date, it will catch the majority of Mass Mailer (MM) worms. Ask your Internet Service Provider (ISP) if they offer antivirus protection and spam filtering on their email servers. This service is invaluable and should always be included as the first line of defense.

Many companies house an internal email server that downloads all of the email from several external email accounts and then runs an internal virus filter. Combining an internal email server with the ISP protection is a perfect for a company with an IT staff. This option adds an extra layer of control, but also adds more administration time.
Sample specs for an internal email server are:

Setup #1

Linux:	OS
Sendmail:	Email server
Fetchmail:	Grabs email from external email addresses
F-prot:	Antivirus
SpamAssassin:	Spam Filter

Setup #2

Win 2003 Server:	OS
Exchange:	Email server
Symantec	antivirus: Antivirus
Exchange Intelligent Message Filter:	Spam Filter

Software Updates

Keep you software up to date. Some worms and viruses replicate through vulnerabilities in services and software on the target system. Code red is a classic example. In august 2001, the worm used a known buffer overflow vulnerability in Microsoft's IIS 4.0 and 5.0 contained in the Idq.dll file. This would allow an attacker to run any program they wanted to on the affected system. Another famous worm called Slammer targeted Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000.

When updating your software, make sure to disable features and services that are not needed. Some versions of WinNT had a web server called IIS installed by default. If you do not need the service, make sure it is turned off (Code red is a perfect example). By only enabling services you need, you decrease the risk of attack.

Telecommunications Security
Install a firewall on the network. A firewall is a device or software that blocks unwanted traffic from going to or from the internal network. This gives you control of the traffic coming in and going out of your network. At minimum, block ports 135,137,139,445. This stops most network aware viruses and worms from spreading from the Internet. However, it is good practice to block all traffic unless specifically needed.

Security Policies
Implementing security policies that cover items such as acceptable use, email retention, and remote access can go a long way to protecting your information infrastructure. With the addition of annual training, employees will be informed enough to help keep the data reliable instead of hinder it. Every individual that has access to your network or data needs to follow these rules. It only takes one incident to compromise the system. Only install proven and scanned software on the system. The most damaging viruses come from installing or even inserting a contaminated disk. Boot sector viruses can be some of the hardest malware to defeat. Simply inserting a floppy disk with a boot sector virus can immediately transfer the virus to the hard drive.

When surfing the Internet, do not download untrusted files. Many websites will install Spyware, Adware, Parasites, or Trojans in the name of "Marketing" on unsuspecting victims computers. Many prey on users that do not read popup windows or download freeware or shareware software. Some sites even use code to take advantage of vulnerability in Internet explorer to automatically download and run unauthorized software without giving you a choice.

Do not install or use P2P programs like Kazaa, Morpheus, or Limewire. These programs install server software on your system; essentially back dooring your system. There are also thousands of infected files floating on those networks that will activate when downloaded.

Backups & Disaster Recovery Planning
Keep daily backups offsite. These can be in the form of tape, CD-R, DVD-R, removable hard drives, or even secure file transfers. If data becomes damaged, you would be able to restore from the last known good backup. The most important step while following a backup procedure is to verify that the backup was a success. Too many people just assume that the backup is working only to find out that the drive or media was bad six months earlier when they were infected by a virus or lost a hard drive. If the data that you are trying to archive is less then five gig, DVD-R drives are a great solution. Both the drives and disks have come down in price and are now a viable option. This is also one of the fastest backup methods to process and verify. For larger backups, tape drives and removable hard drives are the best option. If you choose this method, you will need to rotate the backup with five or seven different media (tapes, CD/DVD, removable drives) to get the most out of the process. It is also suggested to take a "master" backup out of the rotation on a scheduled basis and archive offsite in a fireproof safe. This protects the data from fire, flood, and theft.

In the Internet age, understanding that you have to maintain these processes will help you become successful when preventing damage and minimizes the time, costs, and liabilities involved during the disaster recovery phase if you are affected.

Resources

Virus Resources

F-PROT: http://www.f-prot.com/virusinfo/
McAfee : http://vil.nai.com/vil/default.asp
Symantec Norton: http://www.symantec.com/avcenter/
Trend Micro: http://www.trendmicro.com/vinfo/
NIST GOV: http://csrc.nist.gov/virus/

Free software
AVG Anti-Virus - http://free.grisoft.com Free
F-Prot - http://www.f-prot.com Free for home users

Free online Virus scan
BitDefender - http://www.bitdefender.com/scan
HouseCall - http://housecall.trendmicro.com
McAffe - http://us.mcafee.com/root/mfs
Panda ActiveScan - http://www.pandasoftware.es/activescan/activescan-com.asp
RAV Antivirus - http://www.ravantivirus.com/scan

Free online Trojan scan
TrojanScan - http://www.windowsecurity.com/trojanscan/

Free online Security scan
Symanted Security Check - http://security.symantec.com/sscv6
Test my Firewall - http://www.testmyfirewall.com/

More Security Resources
Forum of Incident Response and Security Teams: http://www.first.org/
Microsoft: http://www.microsoft.com/technet/security/current.aspx
SANS Institute: http://www.sans.org/resources/
Webopedia: http://www.pcwebopedia.com/

EVERYWHERE... ALL AROUND YOU...

By Melody Heller

That car has been behind you since you left the store. Are they following you, or simply going in the same direction? They turned... Thank God. They're not after you, but at the next stop light another car turned onto your street. Maybe you're noticing everything lately, or maybe you know someone is watching you...

I think you have the right to know.

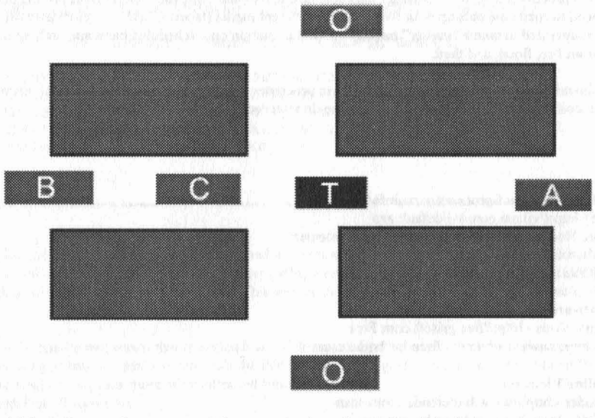
Unfortunately detecting a wheel artist (outdoor surveillance specialist driving a vehicle) is not that easy, unless you're a hard target and have experience in the world of intelligence. Even then you can't always be aware of everything.

Before I tell you anything, you have to learn to think like a surveillance specialist. Know that those who follow you use the tactics of the FBI, and they're not stupid when it comes to stalking you. If they follow you, they surround you. One reason many prefer to stay in the right lane of the highway, just in case they detect anything suspicious. That way, if anyone decide to literally 'surround' you, you might have an option to get off before anything happens. Know this, no matter which method they use to stalk you, they will always try to box you in somehow.

If you think you're under surveillance, you don't look for a guy in a suit and sunglasses, because you will not find one. There are grandmas in wheelchairs watching you. There are happy families with infants in strollers not taking their eyes off you. Learn to not judge people by looks but by their behavior. Learn to pay attention. Be ready for distractions. Don't try to look for vehicles with tinted windows but look for patterns on the road. Cars coming on and off... and on again.

Of course to detect surveillance, one must know surveillance tactics. Here are some basic and commonly used methods by most wheel artists. These methods were first started by the Gestapo (Nazi police) and are still in use to this day.

Floating Box
The 'Floating Box' strategy is the most powerful and commonly used strategy and it's one of the hardest to detect. It boxes you in and follows you. "Floats" around you. This diagram shows you the basic surveillance set up.



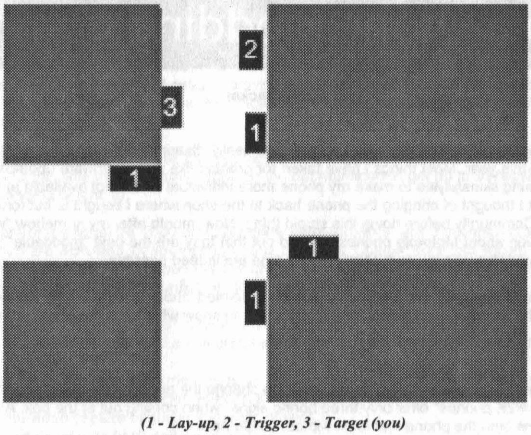
The "A" or Advance vehicle is the warning system of the team. It alerts them of roadblocks, construction, and anything that may be unexpected. Or, if you're bugged, the advance is the person that arrives before you to your final destination.
The "C" or Command vehicle is the "eye" of the surveillance team. They watch you. They have to maintain visual contact with you at all times. This is also the most commonly detected vehicle of the team.
And that's what the "B" or Backup vehicle is for. This is the vehicle behind the command. It takes place of the command in case they think you notice something.
Last but not least, the "O" or Outriders. They are on your sides, usually other streets and they keep you under control. The Outriders make sure they're always boxing you in. Or if you turn, they make sure to surround you right away so contact is not lost.

To do most car surveillance missions successfully, you need at least 5 cars: The advance, command, backup and the 2 outriders. Now, that doesn't mean that you can't find 100 cars following you. If the FBI or someone is **really** out to get you, have fun counting all the agents.

Another popular method of surveillance is called the "Stakeout". This is used when you are parked. The agents surround you and are ready to follow you no matter where you go. This method also on average, includes 5 vehicles... at least. One vehicle, however is the alert button. This is a static vehicle, it never moves. The Trigger, as it's called, alerts the other agents when you make your move, and where.

This method is used on intersections. So, say if you were a 4-way intersection, you would have 4 lay-up vehicles. These are the vehicles that will follow you depending on the direction you go. Until you make your move, they're static as well.

Here is an example: This is a 4-way intersection.



(1 - Lay-up, 2 - Trigger, 3 - Target (you)

On your route, you may and most likely will come across Commit vehicles. These are propositioned and they watch you as you approach, so you will probably not notice them.

Another thing that may help is learning the Brevity Code. This is one of the common languages used during car surveillance operations. If you're all super-spies, you can try and tap into their frequency and see for yourself. They don't speak... normal English, unless the operation isn't very serious. They use codes that a normal person wouldn't understand. Example: "Gamma is flipping, possible spark!" In the everyday English language, that means, "The target has made a U turn. He/she may be detecting surveillance." You will never see agents talk to themselves either. Any idiot with a brain will conceal his voice communication. Especially if they think you're really watching them... They will use Morse Code or another way to communicate so you don't see them.

This article talks about basic surveillance methods. This is not a tutorial, but a simple way to understand the basics of everyday espionage on the road.

Word of Warning: Whoever decides to spy on you isn't always predictable. This article can't guarantee anything. Don't forget to be careful when you're driving and remember to watch the road as well as your enemies.

I hope to write again in the future and discuss this topic on a more advanced state. Meanwhile, you can check out these books, which helped me write this article:

- Secrets of Surveillance, by ACM IV Security Services
- The Art of Surveillance, by Kelly E. Riddle

An insight into the Motorola Phone Modding Community

by leethacker

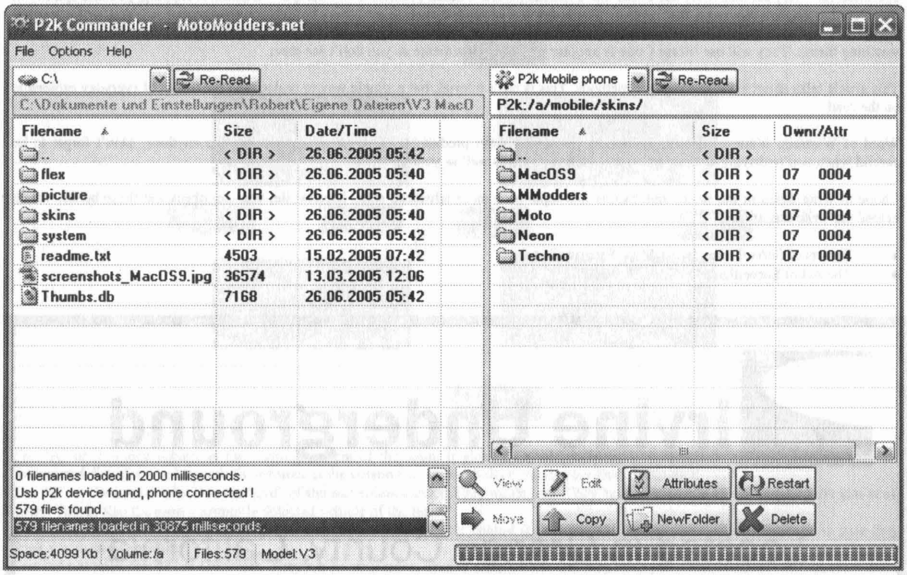
Coming from SonyEricsson and Siemens phones, I was at first really disappointed, when I bought my current phone – a Motorola Razr V3 – earlier this year. Most things I have taken for granted like doing firmware updates with my own computer at home, or the ability of using skins/styles to make my phone more individual where not available at my brand new Motorola phone. I have to admit that I thought of bringing the phone back to the shop where I bought it, but fortunately I discovered the Motorola Phone Modding Community before doing this stupid thing. Now, month after my somehow "wise" ;-) decision, I have a completely different opinion about Motorola phones. I found out that they are the best "moddable" phones one can buy for money, and that firmware updates with my own computer at home are indeed possible.

As I know that there are many people out there, who are disappointed about their Motorola phones, I'll give you a short insight into the secrets of the Motorola Phone Modding Community, to show what is possible with some basic hacks.

Skins

Let's start off with a function most people want: The possibility to change the appearance of the phones GUI. My Razr V3 and most of the other Motorola P2K phones* offer only three boring skins* when coming out of the box. And unfortunately there is no way of getting more skins onto the phone – at least without a little hack. ;-)

Thanks to the guys at www.motomodders.net **[1]** I got the program P2kCommander into my hands, which allowed me (and will allow you) to view and modify the whole file system of the phone. With this little tool uploading skins (which you can get for free from **[1]** as well) is really easy. Basically all you have to do to upload a new skin onto the phone is to put the *.dat and *.ski files of which a skin consists into a folder (with the same name as the *.ski file) in the directory "/a/mobile/skins/" on the phone (*Fig 1*).



C:\Dokumente und Einstellungen\Robert\Eigene Dateien\V3 MacO

Filename	Size	Date/Time
..	< DIR >	26.06.2005 05:42
flex	< DIR >	26.06.2005 05:40
picture	< DIR >	26.06.2005 05:42
skins	< DIR >	26.06.2005 05:40
system	< DIR >	26.06.2005 05:42
readme.txt	4503	15.02.2005 07:42
screenshots_MacOS9.jpg	36574	13.03.2005 12:06
Thumbs.db	7168	26.06.2005 05:42

P2k:/a/mobile/skins/

Filename	Size	Ownr/Attr
..	< DIR >	
MacOS9	< DIR >	07 0004
MModders	< DIR >	07 0004
Moto	< DIR >	07 0004
Neon	< DIR >	07 0004
Techno	< DIR >	07 0004

```
0 filenames loaded in 2000 milliseconds.
Usb p2k device found, phone connected !
579 files found.
579 filenames loaded in 30875 milliseconds.
```

Space:4099 Kb Volume:/a Files:579 Model:V3

Fig 1 - Uploading Skins with P2kCommander

As you can see on the right side of *Fig 1* I have added two skins to the stock Moto skins (Moto, Neon and Techno): A Mac OS 9 skin, and the really good looking black MotoModders skin. You can see in *Fig 2*, how my phone looks with enabled Mac OS 9 skin. Cool, right? ;-)

But changing the menu appearance, the wallpaper and the screensaver is not all you can do with a skin. Some skins even offer custom sounds, custom start up and shutdown animations, custom icons and animations and custom cl.gif's*. For example die-hard Windows fans have the opportunity to use the Windows XP Mobile skin, which offers all the cool stuff mentioned before.

Other cool things you can do ...

Skins are great, but there are also other awesome things you can do to improve your Motorola cell phone. I will mention some of them here in short (please note that not every trick will work with every phone):

Deleting unwanted files: Many Motorola phones like the Razr V3 have no expandable memory. And with the (only) 5 Megabytes user accessible memory the Razr has, every Kilobyte you can get free is worth gold. The problem is: Nearly all manufacturers of mobile phones and nearly all cellular providers put lots of useless stuff like wallpapers, screensavers, ring tones, videos or ugly branded skins onto the phone. And most of this stuff is locked – which means it cannot be deleted. Well, cannot be deleted without a little hack. ;-)

Just use P2kCommander, and you can delete all useless files and change the file attributes of every single file on the phone. Needless to say how useful this little trick is: Some people in the net managed to get up to 9 Megabytes of free space on their Razr V3 by deleting unwanted content. ☺

Custom Funlights: Users of the Motorola V600 probably know what funlights* are. Funlights refer to a sequence of flashing lights on the phone which are activated by an incoming call or event. Custom funlights mean: You can create your own sequences of flashing lights and you can choose the colours of the flashes. All you have to do is to modify the "/a/mobile/audio/funlight.pat" file with a program called "Funlight editor".

Seem editing: The possibility to do seem edits* is definitely the most powerful option a Motorola phone modder has. Cause the so called seems control all vital functions of the phone. Let me give you a few examples what you can do with seem edits:

- You can force the phone to save short messages in the phones memory instead of the SIM card, which results in a highly increased number of short messages you can store on your phone.
- You can activate the video capture option in some old flexes*.
- You can activate and deactivate SMS delivery reports.
- You can set custom cl.gif's and custom start up and shutdown animations.

There are so many things controlled by seems, that it's absolutely impossible to mention all of them in this article. Take my advice and visit xlr8's website about seem editing **[2] [3]**. I guarantee that you will be impressed by what is possible with the change of some bits in the seem files.

Firmware Updates

As most readers probably know, firmware updates often fix software bugs, improve the performance of the device and sometimes contain new features that were not available in prior software revisions. Let me give you an example:

The older software revisions of the Motorola V3 were only capable of playing videos (no capture function!), and the phonebook search was pretty awful. With the newer software revisions these two major flaws were fixed, as Motorola added some awesome new features: Video capturing (***Fig** 3*) and multiple letter search in the phonebook; That's a pretty cool update, right? ;-)

But that's not a quarter as good, as what some Eastern European hackers managed to flash* onto the Motorola E398, which is on the market for as long as a year. Believe it or not, but somehow they got a leaked beta firmware of the rumoured "Apple iTunes phone" E790 in their hands and wrote a guide how this beta firmware can be flashed/flexed on the E398. They even gave the iTunes-modded E398 a new unofficial name: "i398"; I'll better don't talk about the legality of this mod with a leaked beta software – judge yourself. ;-) But it shows what is possible with a simple firmware update.

When you want to know more about flashing your phone and the tools you need for doing a flash, you should visit www.motomodders.net **[1]** and www.howardforums.com **[4]**.

*** Common terms used by the Motorola Phone Modding Community:**

cl.gif: This picture with the dimensions 96x80 pixels is shown on the phones outer display, when the lid of the phone is open (The standard cl.gif is the Motorola "M"; My phone shows "Hack the planet!" which is pretty much cool ;-)).

Flash: A Flash is a file that contains new code for a phone (mainly the phones operating system). By itself, it does not change or affect the graphics or settings of the phone.

Flex: A Flex is a file that contains graphics, settings and Java midlets (Java games / applications).

Funlights: Refers to a sequence of flashing lights and screens on the phone that is activated by an incoming call or event. Amongst many other tools Funlight Editor is the best choice for editing funlights.

P2K: Refers to a type of command that is used to communicate between computer and phone. Nearly all modern Motorola GSM phones since the V600 (V620, V635, Razr V3, E398, ...) are called "P2K phones".

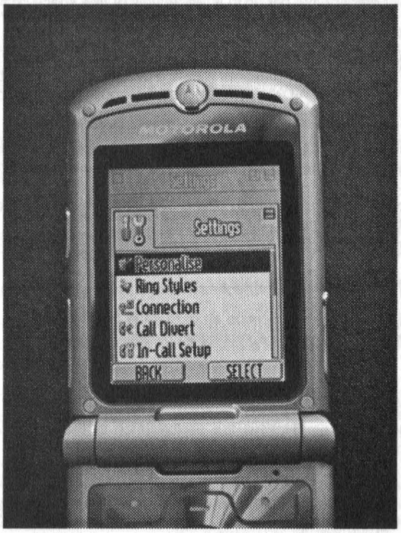
Seem: Seems are "storage containers" for phone settings. Each setting is stored as a single bit, which can have a value of 1 or 0. P2Kman and a normal HEX Editor like XVI32 are a good choice for doing seem edits.

Skin: Refers to a collection of files (including at least one *.dat and one *.ski file) that changes the GUI (graphical user interface) of the phone. This includes, but is not limited to: Menus, Wallpaper, Home Screen Layout, Icons and Animations. Please note: Phones with a software version that begins with "TRIPLETS" are not compatible with skins (for example the Motorola V600). Skins can be uploaded to the phone with P2KCommander.

Last but not least I have to mention: Be careful, because you can easily f00bar your phone with the information provided in this article. And yea, you will definitely void your warranty by doing any modifications to your phone (that includes installing skins, editing the seems, flashing the phone, ...). But hey, which phone modder really cares about that?! Now it's time to "pimp your phone" ... ;-)

Links

[1] http://www.motomodders.net (the best place to visit when you want to pimp your phone)
[2] http://www.xlr8.us/hofo/ (xlr8's seem editing guide)
[3] http://xlr8.us/hofo/map.txt (xlr8's seem map)
[4] http://www.howardforums.com (many phone modders hang round here)



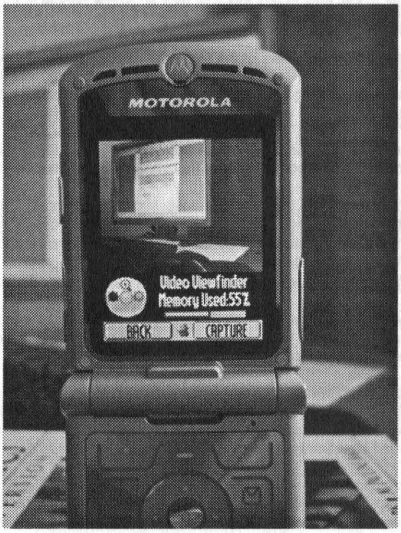


Fig 2 (left) – Is this really a Mac? No, but a phone with a kick ass OS 9 skin! ;-)
Fig 3 (right) – A Motorola Razr V3 with enabled Video Capture function

BLACKLISTED! 411 MAGAZINE PRESENTS

HACK THE SYSTEM!

(the DVD)

Our latest project is in the works, and will be coming soon to a DVD store near you!

We're putting together a brand new DVD about hackers, the hacker community, technology and all related issues. The DVD is arranged as a documentary with a mix of "reality TV" thrown in to capture the interest of a wide audience - old school & newbie hackers, teens, college students and professionals alike. Packed with interviews from the Blacklisted! 411 staff, contributors, real life hackers (both white hat and black hat), celebrities, industry leaders, law enforcement and local government, this won't be your average hacker video. It's the ideal of the Blacklisted! 411 team to bring to the table an informed look at hacking, the reality, the pitfalls and associated amusement. We're serious, but we'd like to keep it fun, too.

You asked for it, so here it is!

Meet many of the Blacklisted!411 staff

Meet our own Editor in chief, Zachary Blackstone! You'll also finally be able to meet the infamous, octopus wearing, Extreme Kidnapping's very own Goldfinger! You'll also meet Ghetto Mafia of our "street crew" and many other staff and crew members!

Live tutorials and how-to's

See how a red box is really made and what it does. Watch wardriving in action. Caller ID spoofing, social engineering, and how to find goodies at a salvage yard. Just a few of the "must see" things which will be available on this DVD.

Fascinating interviews of law enforcement officials, hackers in the news, and software moguls

You'll enjoy what other members of the hacker community have to say. Some from behind bars, some previously behind bars, some rich dudes that got their start from hacking, and some hackers we met on the street. Not to mention you'll love to hear what law enforcement officials really thinks about hackers.

Hilarious comedic skits

Who wants to watch a DVD with boring all talk, talk, talking? You'll see skits that rival any of the popular reality jackass skits out there! Hear some hysterical phone pranks, and many more skits and pranks that will leave you either speechless or rolling on the floor laughing!

Clips of the most outrageous "for hackers only" beach party

See the ad in this issue for more info on the Blacklisted! 411 end of summer beach party. Be sure to be there, you might see yourself on the DVD!

If you'd like to learn more about the DVD, or if you would like to contribute to it, please check out the website at:

WWW.HACKTHESYSTEMDVD.COM

RFID: Chip on my shoulder

By: The Goldfinger

In this day and age technology is advancing at breakneck speed and its really amazing what is being created and what is now possible thanks to new technologies. While I'm all for progress, and new exciting technologies that make my life easier, I'm also wary of how many of these technologies are being used, especially with regard to privacy issues. If you read 1984, and I know alot of you have, you know that so much of that book is coming true, but at that time, its author could have never foreseen the technology available today. We have stuff today, and in development, that was science fiction 20 years ago. With all this new technology comes new opportunity. But as with almost anything, there is always the potential for abuse. Many of the new gizmos and gadgets that are coming out are used for tracking purposes, and surveillance. Big Brother is in full effect. Speed traps, highway surveillance cams, vehicle mounted black boxes, barcodes, and my new favorite, RFID tags! RFID is Radio Frequency IDentification, which is a method of remotely storing and retrieving data using devices called RFID tags/transponders. An RFID tag can be tiny, and fitted into almost any small object, such as a adhesive sticker and can be attached to or incorporated in a product or just about anything.

Types of RFID:

RFID tags can be either *active* or *passive.*

Passive RFID tags don't have their own power supply. The minute electric current induced in the antenna by the incoming radio frequency scan provides enough power for the tag to send a response. Due to power and cost concerns, the response of a passive RFID tag is brief, typically just an ID number. Lack of an on-board power supply means that the device can be quite small: commercially available products exist that can be embedded under the skin. As of 2005, the smallest such devices commercially available measured 0.4 mm ×× 0.4 mm, and thinner than a sheet of paper. They are practically invisible. Passive tags have practical read ranges that vary from about 10 mm up to about 6 meters.

Active RFID tags, on the other hand, must have a power source, and can have longer ranges and larger memories than passive tags, as well as the ability to store additional information sent by the transceiver. Today, the smallest active tags are about the size of a coin. Many active tags have practical ranges of tens of meters, and a battery life of up to several years.

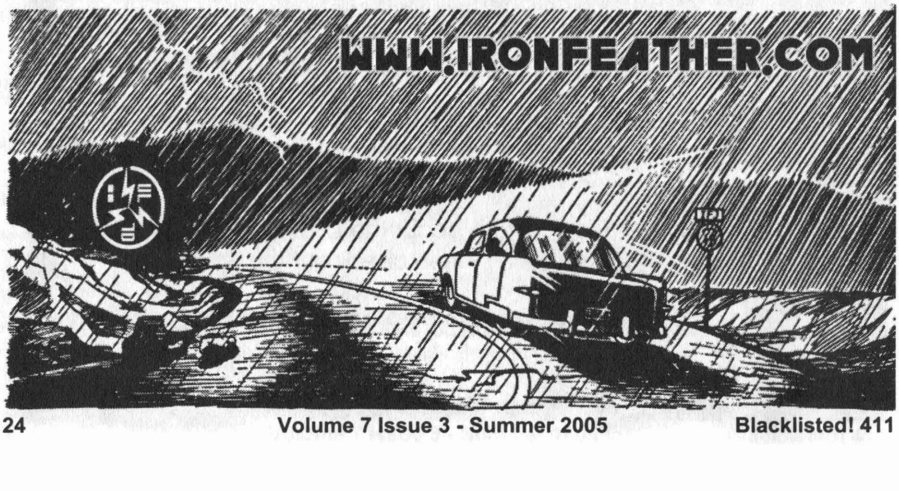
Passive tags are cheaper to manufacture and don't depend on a battery, and the vast majority of RFID tags in existence are of the passive variety. As of 2004 tags cost from US$0.40. The aim is to produce tags for less than US$0.05 to make widespread RFID tagging commercially viable. However, chip manufacturers' supply of integrated circuits is not sufficient and demand is too low for prices to come down soon. Analysts from independent research companies like Gartner and Forrester Research agree that a price level of less than $0.10 is only achievable in 6-8 years, a potential hurdle to widespread passive RFID adoption. However, using some new manufacturing techniques can lower the price of RFID at a faster pace.

While the cost advantages of passive tags over active tags are significant, other factors including accuracy and reliability make the use of active tags more common today.

There are four different kinds of tags commonly in use. They are categorized by their radio frequency: low frequency tags (between 125 to 134 kHZ), high frequency tags (13.56 MHz), UHF tags (868 to 956 MHz), and microwave tags (2.45 GHz). UHF tags can't be used globally as there aren't any global regulations for their usage.

The RFID system

An RFID system can consist of several components: tags, tag readers, tag programming stations, circulation readers, sorting equipment, and tag inventory wands. Security can be handled in two ways. Security gates can query the ILS (Integrated Logic System) to determine its security status or the tag might contain a security bit which would be turned on and off by circulation or self-check reader stations. The



purpose of an RFID system is to allow data to be transmitted by a portable device, called a tag, which is then read by an RFID reader and processed according to the needs of a particular application. The data transmitted by the tag may provide identification or location information, or specifics about the product tagged, such as price, color, date of purchase, etc. The use of RFID in tracking and access applications first appeared during the 1980's. RFID quickly gained attention because of its ability to track moving objects. As the technology is refined, more intrusive and invasive uses for RFID tags are in the works.

A good example of usage is in the library. Security gates can detect whether or not a book has been properly checked out of the library. When users return items, the security bit is re-set and the item record in the ILS is automatically updated. In some RFID solutions a return receipt can be generated. At this point, materials can be roughly sorted into bins by the return equipment. Inventory wands provide a finer detail of sorting. This tool can be used to put books into shelf-ready order.

Current usage

RFID usage is popping up everywhere. *Low freq.* tags are commonly used for animal tracking and identification, which isn't really that new. Other uses include beer keg tracking, and vehicle anti-theft systems. Pet tracking chips are becoming more common too. Two RFID frequencies are used: 125 kHz (the original standard) and 134.5 kHz (the international standard).

High-frequency RFID tags are used in library books, and at bookstores. They are used in pallet tracking, building access control, airline baggage tracking, and clothing item tracking. High freq. tags are also used in ID badges replacing the earlier magnetic stripe cards. These badges only need to be held within a certain distance of the reader to authenticate the holder.

UHF RFID tags are commonly used commercially in pallet and container tracking, and truck and trailer tracking in shipping yards. Microwave RFID tags are used in long range access control for vehicles.

Tollbooths all over the country are adopting the E-pass system (EZPass, FastPass, SunPass, I-PASS) which uses RFID tags for electronic toll collection. The tags are read as the vehicle passes, and the toll is automatically debited from the users pre-paid account. The system helps to speed up traffic through toll plazas. I'm all for improving wait times. *thumbs up* Although it looks like some govt. officials think the technology might be good to apply to border crossing too. The idea sounds similar to the "trusted traveler" or whatever it was called program that would let certain people who proved themselves as "safe" to cut security lines at airports. Drivers would still need to stop, but the RFID system would record who they are and when they crossed, as well as let the border patrol know not to spend too much time checking them out. It's not hard to see how this system could be easily abused. "Get across the border free" cards stolen (or bought) from "safer" travelers would suddenly become a hot commodity among those who wish to get across the border illegally, or who have something to hide.

Electronic cash is one of the big ideas that "they" want us, meaning *everyone,* eventually to adopt. True enough, it would make things very convenient in many circumstances, but at the same time, you'll effectively give up your financial privacy. Every single transaction would be recorded and a record would exist. In cosmopolitan and savvy places like Hong Kong and the Netherlands, they are already using cards embedded with RFID chips as e-cash to pay for mass transit fares and retail items. The Octopus Card is an example. www.octopuscards.com

In the 2004 model year, a "smart key" option was made available in some Toyota and Lexus models utilizing a key fob with an active RFID circuit which allows the car to acknowledge the keys presence within 3 feet of the sensor. The driver doesn't even have to take the key out of his/her pocket or purse to open the doors or start the car. Now that's convenience. *thumbs up*

Not all the uses of RFID make you think convenience or even utility. Some of the uses purport to ensure safety, or accountability, but will just chap your ass. A recent headline read; "Parents Upset Over Mandatory Chipping Of Kids". A elementary school in Sutter, CA introduced a scheme last month to use RFID to identify its pupils. The RFID chips are worn around the neck in the form of ID badges and can be used to monitor where the children are on school grounds, and carry the child's name, photo, grade and unique school ID number. Parents were obviously upset. One parent was quoted as saying, "Are we trying to bring them up with respect and trust, or tell them that you can't trust anyone, you are always going to be monitored and someone is always going to be watching you?", according to a report in the *Associated Press*. While the school thinks its a great idea to improve safety measures and keep track of students, I think its another example of Big Brother making the leash even shorter. *thumbs down*

As with any new technology that has implications for privacy or personal liberty, prisons are fertile testing grounds. In other words, its always easier to convince people that this "new" technology is useful and beneficial, by testing it on inmates first. Corrections facilities in Michigan, Ohio, California and Illinois already employ wristwatch sized transmitters that can detect if prisoners have been trying to remove them and send an alert to prison computers. While I don't really see a problem with using them in this way, while they are incarcerated, I think it could become problematic if they tried to convince people that they had to continue wearing them after release....

Conspiracy Alert!

Sure they have supervised release, and tether programs for house arrest, but I'm looking at the big picture. Someday some politician will say, "All criminals, past and present, need to be supervised at all times", "We can't risk having them re-offend". Solution? Once your in the system, your implanted with an RFID chip and there it will stay. Think it can't happen? Think again, the powers that be ("they") want everybody to be monitored 24/7. They can't wait to slap a chip in your ass. Right now, "they" want to appeal to many by showing the great benefits and convenience of using RFID and "chipping" everything. Meanwhile, "they" work behind the scenes to pass laws that will allow for mandatory 'chipping' of certain populations like criminals/prisoners. Since a large % of Americans have been in the system, and are currently in the system, this is a great way to 'chip' a huge segment of the population. Another large % will voluntarily accept 'chips' for this or that, even themselves since it will be just sooo convenient! Once everyone is 'chipped', say good bye to privacy, *and hello to total surveillance!* *2 big thumbs down* I admit that Fox Mulder is the only one that believes me on this, but regardless, the technology exists, and it is appearing in more things on a regular basis. Beyond that, there are *numerous* plans in the works for widespread RFID usage. As with anything, open debate and a careful analysis should prove useful to all parties as long as there are checks and balances.

Preventive Forensics

Implantable RFID "chips", are being used to thwart crime as well. Were fast approaching a reality as seen in Minority Report. A reality where crimes are attempted to be stopped before they happen. The US and some other countries in Europe have increasingly started relying on this science. Its about focusing from post-facto solutions to pre-incident detection and prevention. Forensic psychological tools like brain mapping, polygraphs and narco-analysis are being introduced to combat security risks. Some companies like Applied Digital Solutions has proposed a chip with its "unique-under-the-skin" format as a solution to identity theft, secure building access, storage of medical records and even anti-kidnapping applications. I'm something of an expert when it comes to kidnapping. In countries like Columbia and Mexico, where kidnapping is a daily occurrence, a chip like this could prove beneficial. However, there are factors to consider. First, your risk must be assessed. Why would someone want to kidnap you? Unless your a politician, executive, narcotrafficker or just plain wealthy, your at-risk status is probably very low. If you fall into one of those categories, and there are a few others, then your risk might be elevated. In Mexico, for example, the Mexico City police dept. has implanted approximately 170 of their police officers with the Verichip, so they can be tracked in case of kidnapping. Kidnapping is a everyday thing in Mexico, not only for cops but also narco bandidos, and even tourists. What is known as the "express kidnapping" was pioneered in Mexico. Kidnappers snatch you up, and take you right to the ATM, where you pay your own ransom *-NOW!* The Verichip is also being promoted heavily as an anti-kidnapping device for mexican children. Solusat, the Mexican distributor of the VeriChip is marketing the device as an emergency ID under its new VeriKid program. The service even got the backing of Mexico's National Foundation of Investigations of Robbed and Missing Children, which has agreed to promote the service.

According to a press release announcing the collaboration, the foundation estimated that 133,000 Mexican children have been abducted over the past five years. A Solusat executive said the terms of the agreement are still being hashed out.

"There are distinct projects on the table, but one form of finding (children) is by putting scanners in strategic locations where a search is being conducted for a VeriKid that has been reported missing," said Carlos Altamirano, Solusat's associate general director. The company wants to place walk-through scanners in malls, bus stations and other areas where a missing child might appear. The chip also could be used to identify children who are found unconscious, drugged, dead or too young to identify themselves. Critics say kidnappers could circumvent the device easily.

"My big concern is that kidnappers will simply use 'high-tech' tools like knives to get rid of them," said Lauren Weinstein, creator of the Privacy Forum, an online digest related to privacy and technology issues.

The Electronic Privacy Information Center www.epic.org warned that inserting a type of LoJack into children and workers to track their movements could violate their civil liberties.

The VeriChip is injected under the skin of the upper arm or hip in an outpatient procedure. Other potential uses of the chip, according to company officials, include scanning unconscious patients to obtain their medical records or restricting access to high-security buildings by scanning workers to verify their clearance.

In Mexico, the cost of the VeriChip and the doctor's fee for implantation is about $200, in addition to a $50 annual fee to maintain the database. The handheld scanner costs an additional $1,200, Altamirano said.

These are just a few of the many places that RFID is making an appearance. And many more will soon come. Watch for my next installment on RFID. Coming soon to an item or person near you!

A HACKER KNOCKED ME UP AND NOW I'M STUCK WITH HIM

By Zer0 Hack

There I was, sitting in the bathroom of my hacker boyfriends apartment. Peeing on a stick! Then there they were, two lines. The package says to wait three minutes, but that second line showed up almost the instant I peed on the thing, immediately after the first line. Ok, so two lines means I'm not pregnant right? Whew! But I'd better check the directions to make sure. Hmmmmm, there it is, two lines = pregnant. PREGNANT! WTF! No way, good thing there are two test that came in the box. I pee again and get the same results. And there begins the rest of my life.

I was in my very early twenties, and not at all prepared to be a mommy. I had heard that sex equals pregnancy, but not for me, I was using birth control. The birth control box states that only 1% of women taking it will still get pregnant. Naturally I assumed that meant only 1% of the entire population taking birth control pills will get pregnant, and those odds must be astronomical. Not so. That 1% means either 1 out of 100 or 1 out of 1000 women taking birth control pills will get pregnant, depending on which brand you use. In reality, those are not that great of odds. As a 30 year old mother of almost four kids now, who used various forms of birth control, I must tell all you youngsters out there that sex does infact equal pregnancy. Stunning, I know, but it's true. If you don't think you are ready for a baby, then don't have sex! Ok, my preaching is done, now for the rest of my story.

I was lucky, my boyfriend was a good man who did in fact love me. Even though we were scared to death about our future as parents, we jumped in with both feet. We had a fabulous wedding, which only took a month to plan. Amazing! If you ever had anything to do with planning a wedding, a month of planning for a fabulous wedding truly is amazing. I give credit to my mom and my aunt for that, they should go in business as wedding planners, and advertise that they can guarantee you a wedding in a month from start to finish, LOL! At the wedding many of my family and friends asked me what my husband did for a living. I told them that he was a hacker, he wrote articles for hacker magazines, etc. I didn't know too much about what it meant to be a hacker. Before I met my husband I thought a hacker was what everybody else thought a hacker was, a thief who broke into other computer systems and stole things. Since I met my husband, I learned a lot about what a hacker really is. So, I would further explain when asked about my husbands profession, that he was a good hacker and not the kind that the media personifies. He loves technology and makes it better for the rest of us. I think that summed it up simply and to the point where most people could understand. And surprisingly most people responded really well to hearing he is a hacker. I think that's because the wheels in their heads started spinning and they immediately thought, "Alright! A hacker in the family means free computer help!" Which my husband HATES to do. In fact, my husband refrains from telling anyone he is a hacker for fear that they will ask him for computer help. Not for the fear of the stigma that comes with the word hacker, but because he doesn't want to get sucked into their computer problems. I find that most hackers, even though they are amazing with computers, hate working on other peoples computers. Anyways, the wedding was great, the food was great, and the wedding night was great too, wink wink.

A few months later our beautiful baby girl was born. Who would have thought that a hacker would make a great daddy. He changed her diaper, he held her, he rocked her, her breastfed her, haha, just kidding, but he did burp her afterwards. He was very hands on, and has been with each of our kids. I must admit that because of the business he's in, he gets to work out of our home, which in turn gives me a lot of help with the kids and the house. Not a lot of women can say that about their husbands. That is one of the greatest upsides to being knocked up by a hacker and being stuck with him. But trust me there are plenty of down sides too. This is where I give advice to anyone who is contemplating marrying a hacker or is married to a hacker. We've only been married seven years, but I think I've learned quite a bit in all that time.

I think a hacker is a totally different breed of man, unlike the stereotypical man we all know. In my experience a hacker is more of a homebody, they like consistency and therefore are usually more loyal. They don't usually go out partying and drinking with the guys. Because of their interests, they might be self-employed, like my man, and work out of the home. This can be great if you get along with him all of the time, and it is definitely great when they can help you with the house and kids. A hacker has the brain capacity, and the drive, usually, to eventually use their skills to become rich. They might even wind up winning the noble peace prize for an invention. But in the meantime, being self-employed and not rich can be very difficult. There might be times when you have to eat mac and cheese and peanut butter and jelly sandwiches for every meal. Then maybe a week later you have a big fat check, which you'll use to catch up on the bills and buy some groceries, then you'll wind up back to square one until the next big check comes and the cycle continues. This can last a while, but eventually he'll pull you out of that rut. You have to realize that he is constantly working the wheels in his hacker head and coming up with new ideas. They will pay off, just be patient. Hopefully, you're a special breed of woman that can put up with the ups and downs of the financially unstable life. Have faith in him, he needs your faith. Without it, he may not accomplish all the wonderful things he is capable of accomplishing.

Hackers LOVE their toys, and love improving on any they receive as gifts. They'll either return the gift for a bigger better one in a brand that they specifically will only buy, or they will manipulate the toy to do other things. But they do love their toys. The more technologically advanced the toy, the better. They love tools, which they use to manipulate their toys or other everyday items that they can improve upon. My husband says that he could receive tools for every occasion as a gift, they can even be tools he already has, and he will be beyond thrilled. Luckily, I have learned what brands he will want. And here's a tip, if you can, buy the most expensive one, that way it avoids another trip with him to the tool shop to do an exchange. Luckily, our hacker men will usually know what to do with the tools, unlike most men who like to pretend that they do. The only problem with them is when they start a home project, it might take months, no wait, years before a simple project is completed. In the meantime, they've started a few other home projects which have yet to be finished as well. Been there, done that, still doing it. Ok, so maybe that last part is a stereotypical male thing to do, and not just a hacker trait.

Hackers enjoy SciFi and hacker shows and movies, but personally, I think they just enjoy enthusiastically pointing out all the inaccurate things they find in these shows. If you haven't noticed yet, they love to show how technologically savvy they are. I don't believe that they can help it. It's just the way their brains work. Most of us wouldn't even notice those fine details in such movies, so we can stay quiet and enjoy the show. But they have a hard time enjoying a movie that isn't believable to them. Just as we wouldn't enjoy a love story movie, where the main characters had no chemistry, it's just not believable. Anyways, beware of watching one of these shows with your hacker man, and be prepared to roll your eyes a lot and don't feel bad if you have to tell him to shut-up and watch the movie.

Hackers think they have the solution to any problem they hear about on the news. That's always fun to listen to. Again, be prepared to roll your eyes and tell him to shut-up until the news is over. The only problem with this is that you will see him grunting and groaning when he sees something he wants to comment on and when a commercial comes on, he lets the floodgates open. Either that or he will open his big mouth during the news anyways, in which case it might be better to avoid watching the news with him altogether. Oh, and be careful of those news excerpts during the commercials of your favorite show, those small little news commercials can get him started as well. If you have the ability to, you may want to pause your show until he's done ranting. Or better yet, record your favorite show, and zoom past the commercials.

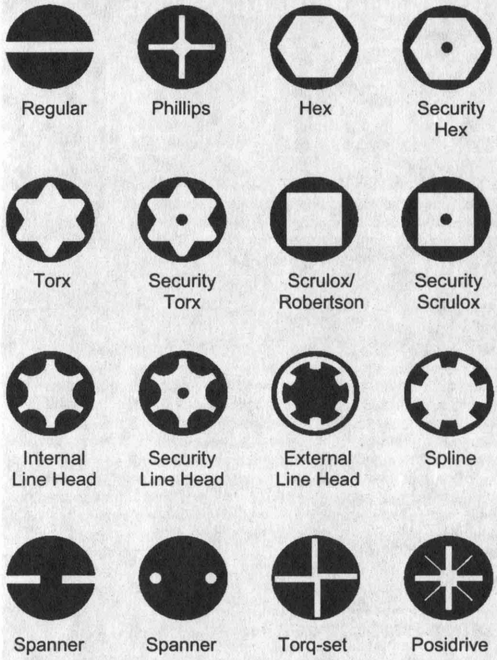
A hacker loves to stay up late on his computer. I HATE this! It is probably my biggest pet peeve because I can't sleep if my husband is not in bed with me. Luckily, my husband doesn't do this much anymore. I think he hates how grumpy I am the next day more than I hate that he stays up too late. So, if you see him buying Jolt Cola or some other high caffeine drink, be sure to hide them or dump them out, and never under any circumstances buy them for him! You'll just be encouraging his late night behavior. If he tries to sneak away to the computer late at night, it doesn't hurt to entice him to stay with you. If the classic nighty doesn't work on him, try working on his other head, the one with his brain. Ask him what he thinks about God, if time travel could be a reality, or if he thinks there really is extraterrestrial life out there. Trust me, this will work like a charm. In fact, sometimes it works a little too well, as he lays in bed with you talking about such deep thoughts until dawn. Well hey, at least he stayed with you!

Hackers are notorious packrats! I can't emphasize this enough. They're usually born like this and drive their mothers crazy when they come home from a trash can with all kinds of "neat" stuff. This "neat" stuff was usually something that they could fix for a profit, or fix it and use it, or something that they felt they could cash in on years later. My husband has a four car garage stuffed to the gills with this "neat" stuff. Believe it or not, a portion of it is from things he collected as he was growing up. Usually they collect electronic items or sorts. But my husband goes all out and will collect just about anything he can get his hands on, and admits that he has a hard time not grabbing a great deal, whether he needs it or not. I've noticed this trait in my children as well, so I'm convinced that it truly is a genetic thing. The urge to collect is very strong in my little family. You wouldn't believe what my kids have brought home, and what I've found in their drawers, but that's another article. As a wife and mother, handling this packrat syndrome is very difficult, especially when their "neat" stuff starts expanding from the garage into the rest of the house.

Now the most important thing you'll need to know about being the significant other of a hacker is that they need plenty of ego stroking. When they start talking to you in some language only hackers understand, you just need to nod and grin. If you can, actually pay attention part of the time to a few key words and see if you can make a question out of them. Oh, how he'll love that! Now remember, stroking the ego is not necessary while watching a movie or the news. There is a time and a place for his hacker-ese, such as long car rides (ugh), or your late night deep conversations about life and God. He'll want to speak his mind all the time because like I said before the wheels in his hacker head are always turning. It's your job, if you want to keep your sanity, to teach him when it's appropriate or not.

I've been "stuck" with my hacker for over seven years now. I've learned quite a few things about the personality traits of a hacker from my husband and his hacker friends. I'm sure not all hackers will follow these traits, but I think in general, they typically follow them. There are some hard to handle aspects of hackers, but let me tell you that their good traits far outweigh their bad traits. Once you get to know their personalities, you'll soon learn how to handle them. And quite honestly, if I had to deal with what a lot of other wives out there have to deal with regarding their men, I'd probably not be married right now. I could not handle it if my husband worked 40+ hours a week, if he had to travel for a living, if he went out with the guys after work for a drink, if he partied every weekend, if he was a womanizer, if he was an unmotivated loser, or if I simply didn't get all the attention I needed whenever I wanted. I honestly think a hacker makes the best partner in the world. A hacker that loves his toys, hey, that means that you have fun toys too! I love our lifted SUV! I've actually grown to love his scifi shows, in fact, Stargate SG-1 is my favorite show now, we love watching it together. Besides his answer to all the worlds problems, I can't watch the news anyway, it's way too depressing for me. I actually love our late night chats about life and God and whatever else we can think of. I love to hear his deep insights, you can tell he's really thought out what he believes. Ok, now the packrat syndrome, I still have a hard time with that, but I do know one day it will pay off. He has things in his garage that would make old time collectors drool. Twenty years from now, those items will make us rich if nothing else will. It really is very exciting to think that your husband may someday come up with something that makes the world a better place. I have no doubt that my husband will do just that! I'm anxious to see what another seven plus years brings us. The best thing that ever happened to me was getting knocked up by a hacker and being stuck with him.

Driver Bits



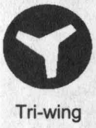
So, you have some piece of equipment you want to open up, but you have no idea what the hell that little fastener is? There are all sorts of oddball screws (screw balls?) out there and here's a sample of some of them.

Use the Regular and Phillips diagrams to get an idea of how the diagrams work for the rest of the screw/bit types you're unfamiliar with. The white part of each diagram is where the bit fits into the screw. The Black portion of the diagram is the base of the screw that the bit is surrounded by when the bit is inserted. It'll make sense after awhile.

Often, you will find Spanner screws used to hold wall plates in place at schools... primarily in bathrooms.

You will find Security Torx screws used in all the ST-1600 thru ST-2500 cable boxes.

External line head screws are really unusual. Or are they? Check out Super Nintendo, Nintendo 64, Gameboy, Pocket Gameboy, SNES Carts, N64 Carts, Gameboy Carts, Sega Genesis, etc, etc Mostly, if not entirely, Japanese made home video game systems.



Do you want some of these? Do you need some of these? It'd be a good idea to stock up just to have them handy in case you do happen to need them some day. Find them at the following locations:

Jensen Tools, Inc.
(800)426-1194
http://www.jensentools.com

Parts Express
(800)338-0531

WANTED

Photographs!

If you have a photo of a payphone, local telephone company vehicle or building, local cable company vehicle or building, interior of a telecomm. or other utility building, inside a manhole, inside a utility box or some other interesting item, please send them to us along with a short "memo" explaining what it is that we're looking at!

If you send a photo that we end up using in our magazine, we'll mention your name along with the photo.

REVIEW CORNER

BY ZACHARY BLACKSTONE

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.

Micro Voice Disguiser
Classification: Tool
Cost: $69.95
URL: http://www.spyworld.com/Surveil1.htm

Ok, so I like voice disguisers/changers. I think they're cool. Some of them are better than others for various reasons, but I'm nit picky that way. I had the opportunity to play with this little guy a few weeks ago and, even though I don't care too much for the sound quality, it has one very redeeming quality. It's small. Very small. In fact, it's so small, you can slip it right over the mouthpiece of a payphone which is really cool. There are many reasons people might want one of these, but the main reason is always the same: they want to sound like someone other than themselves. Ok, this voice changer meets that goal, but the quality of the voice processing isn't the best in the world. Anyone with half a brain on the receiving end of the call should notice that it's a manufactured/processed voice and that can be a problem in some circumstances. That's why I prefer the high end units that are so damn good, you can't tell that it's voice processing you're listening to. The problem is that most of the high end units are too bulky to carry around with you or use on a payphone. All in all, I think this is useful, a little pricey for what you get, but still useful. If you can't afford the big toys, this one is a nice entry level voice changer.

Key Katcher
Classifications: Tool
Cost: $96.00
URL: http://www.hackerstickers.com/products/keykatcher-keylogger.shtml

Have you ever wanted to catch your significant other red handed doing something naughty online? Well, this key katcher is just the ticket. There are three models available: the 32K, 64L and 128K. We got our hands on the 128K model and we've been putting it through the hoops over here. So, what does it do? If you're a hacker, I'm sure you know exactly what this little device does and how useful it can be. However, for those of you not in the know on this subject, the Key Katcher is a small device that plugs in-line with your keyboard on the back of your PC. It will "capture" all the keystrokes entered into the keyboard and save it for further examination. Why is this useful? Well, you can fire up any old text editor and type in the password...next thing you know, the entire contents of the capture device is dumped into the text editor.....passwords, emailed to people, articles they've written for school or work, etc. Very nice. Personally, I'll tell you why I love these things. You see, I'm an editor and I write a lot of articles. Windows, the unfortunate choice of our standard PC operating systems over here, has this terrible habit of crashing from time to time - either the OS itself or whatever text editing program I may be running at the time. However, because of my forward thinking, I have this capture device handy which usually keeps a solid record of whatever I typed just in the off chance something catastrophic happens. It gives me incredible peace of mind. To all the writers out there, you should get one of these. I recommend the largest capacity unit. Why? Because it's not really that much more cost-wise than the unit with the lest capacity. Anyhow, this great little device holds 128K of text, has an outstanding interactive menu system, has the capability to have the password changed at will and can be turned on and off as you require. The device does not need batteries, can be pulled hot or cold (with power on or off) without damaging the unit or the contents it has stored, does NOT require any software to be installed and connects to your PS/2 port. My assessment of this device? Given the large capacity, the small size, ease of use and associated value, I give it two thumbs up.

HackTV Episode 2
Classification: Video [Underground]
Cost: Free
URL: http://www.binrev.com/hacktv/

Over a year in the making, the long awaited episode 2 of HackTV was just released a couple of days ago. Naturally, I was first in line to get my copy. Brought to us by none other than the crew at Digital Dawg Pound and the makers of Binary Revolution, HackTV is probably the best underground hacker show available right now. And, trust me, I watch all of them, including the ones you guys have probably never even heard of. So, in my opinion, what we have here with HackTV is the best that the hacker community is putting out. I was very exited to see that a new episode had been released, so I wasted no time and viewed it the second I had my copy. Let me tell you about episode 2. First off, Stankdawg explains that several hurricanes were to blame for the delay in getting a new episode of HackTV. OK. Next, a little exploration of an apartment building utility room and then of a Bell South telecom box. That was actually pretty interesting to see, though the explanation ran on a little. Last, a quick tutorial from Acidus about mag stripes and Stripesnoop. That was very interesting since I love hardware hacking. Anyhow,. I give the video a thumbs up. Go get your copy and support their efforts.

Bug Detector
Classification: Tool
Cost: $239.95
URL: http://www.spyworld.com/Surveil1.htm

So, you're worried you might be bugged? You can do something about it, you know. And it's well within the means of the general public. I've been goofing around with bug detectors since the 80's and always found them to be an interesting gadget to study. I've seen them all, from suitcase sized professional units to the little handheld units like this one. I've even looked at the covert bug detectors which seems silly, but I suppose they have their place. Ok, so first off, the word "expensive" came to mind when I first saw this gadget. Ok, so I grabbed one up and played around with it for a few days. Here's my assessment of it. It's extremely simple to use and it appears to work quite well. The no-frills approach to their design makes it incredibly easy to locate a bug and dispose of it. I had one of our guys set up a small FM transmitter bug in our office and then I came in with the "bug detector". It took me less than a minute to locate the bug. Not bad. We then tried the same experiment but with several (4) transmitters. I was able to locate all four within 5 minutes. Ok, so it works, pretty well I might add. Now, let's talk some specifics. Apparently, this little device will receive and sniff frequencies ranging from 50Mhz to 3GHz. That's a pretty wide range. It works with video transmitters, fm transmitters and, surprisingly, cell phones. Yeah, you can zero in on a cell phone with it (because of this, it threw off my initial multi transmitter test, in fact). So, if you have an extra $240 plus shipping to blow on a neat toy like this, I think it's worth the investment. I give it a solid two thumbs up.

282 Hour Digital Recorder
Classification: Tool
Cost: $345.00
URL: http://www.spygear4u.com/product.asp?productid=865

Another digital recorder? Yep. This one was worth every penny, too! Why, you might be asking yourself. Well, the recording time. It has 1GB of storage and can record up to 285 HOURS of audio! That's just insane. I have a lot of digital recorders and this is the largest capacity unit I've seen to date. You can connect this to your PC using the USB port. It comes with lots of extras like a telephone recording connector, a microphone for your lapel, stereo earphones, USB cable, etc... even a couple AAA batteries. Anyhow, it's very small, lightweight and packed with features. It has three recording modes, built in speaker, clock, timer, variable playback modes, speed control. Something really unusual about this digital recorder is the fact that is has a built in FM stereo receiver. Yeah, really. Anyhow, you can record right off your favorite FM station and save it for later use. Love that feature! Further, it has an MP3 player built in. It's just cool. I'm tossing this one into my toolbox. Two thumbs way up!

SlimTRAK covert GPS tracker
Classification: Tool
Cost: $749.00, plus $50.00 activation fee, plus $8.00 per month fee
URL:

Ok, you want to see cool, get one of these. It's SO easy, anyone can use it. The transmitter is very small and easily hidden. Slap one of these in your car and leave it there. Sign onto the slimtrack website and you can access a wealth of information on the whereabouts of your tracked vehicle. You can find out time, speed, street address and last stop. Out of the box, the unit updates every 2 minutes or so, which is close enough to real time for me. You can even program the unit for quicker update times. How's that for cool? I put this to the test. Accuracy is pretty good with regard to speed calculation, and actual physical location. I know the price is high, but the device is just too cool and worth every penny if you ask me. If you have someone you want to keep track of (like your kids), this is more than adequate. This almost reminds me of the old Teletrak system, but with the added function of being able to check online and see a MAP of the location. It's a very simple to use device that anyone could appreciate. How's it work? It uses GPS to determine it's location and transmits information on the GSM communication band. The information is transferred to the website and then made available to the user/subscriber. Not for everyone, but definitely worth a looksie. I give these guys two thumbs up for their great gadget/service.

WRT54G/ S

Expanding you Linksys device

By: Ustler

Personally I love anything you can put linux on, and if it only cost 40$, that's even better. In the past year, Linksys has been kind enough to release its source code for the general public for a variety of routers and devices. The device we will be examining today is the WRT54G and WRT54GS. It was originally meant to be an 802.11b/g router, but can easily be expanded to do much more. Along with better performance, and functionality, we also boost the transmitting power up to 251mW, which by far is about 800% better than the default 28mW. But with this boost comes serious heat problems, so just to be safe, I would suggest you continue reading before trying anything!

WRT54G Vs WRT54GS
The main difference between the two routers is Linksys's proprietary "Speedbooster" technology (Found in the WRT54GS). Although I don't endorse the purchasing all new wireless devices to get the boost in speed, the hardware differences are well worth the price. When purchasing a WRT54G, you must consider that there are several revisions to the hardware. Just to be safe, I recommend buying the WRT54GS, because you can rest assured that you have the added benefit of a 200MHz processor rather than the 125MHz found in the WRT54G Revisions 1.0 and 1.1. Also, the newer GS and G models include 32 MB of Ram, rather than the 16 MB in earlier versions. The main difference between the G and GS is the fact that GS models have 8 MB of flash while the G models have only 4 MB. This added room allows you much more freedom when added additional features to your router. Also note that prices on both routers have dropped significantly with the release of the new SRX (Pre 802.11n) model. I would encourage everyone to wait for the official 802.11n release instead of buying into proprietary technology (Often discontinued when new standard comes out). If you have more questions on differences, a full layout has been provided by our dedicated friends at linksyinfo.com (http://www.linksysinfo.org/modules.php?name=Content&pa=showpage&pid=6).

After Purchase: ***Firmware Considerations***
Well, you finally decided to splurge and purchase a WRT54G/S. After you purchase the product, it will come with Linksys stock firmware, which by far is very limited to what the WRT54G/S is fully capable of. There are a couple firmware variations out there to consider, which we will cover in this section.

To make things a lot simplier, we are going to classify the firmware versions into 3 groups: Beginner, Advanced, and Expert.

Beginner firmware is meant for those GUI depended people who have no idea what a command line is and just want the thing to have a better range than it did out of the box. They don't care about anything but connectivity, so additional features are out of the question.

Advanced firmware is simply the GUI firmware with more options and slightly more configuration necessary. The users in this group like to push the bounds of their Linksys router and create want to create the ultimate geek toy. They feel safe playing around as long as they have the re-assurance of a GUI to fall back upon if problems arise.

Expert firmware is meant for those hard core Linux fans that know about everything to do with linux. They don't care about a GUI because they have every possible Linux command memorized, and are very confident that they can navigate their way around with ease. They are also able to recover any problems that might arouse when playing with their new found toy.

Breakdown:

Beginner	*Advanced*	*Expert*
HyperWRT (http://www.hyperwrt.org/)	**DD-WRT** (http://www.dd-wrt.com/)	**Operwrt** (http://openwrt.org/)
EWRT (http://www.portless.net/menu/ewrt/)	**Talisman/Alchemy** (http:/sveasoft.com)	

Other Firmware not included:
Wifi-box – Hasn't been updated since October of 2004.
Freifunk – German firmware.

Those are essential the major distributions (Note all firmware have power boost ability)

HyperWRT – Easy to use, offers the ability to boost power, firewall scripts, QOS along with other features. Very simple, easy to use and does not offer a lot of additional services.

EWRT – Offers nocatsplash (Public Portal), SSH access and a writable jffs2 partition in flash. Also simple to use, very similar to original Linksys firmware

DD-WRT – Supports everything that Talisman has, but also adds in a lot of other services. A list of all possible services is listed in the DD-WRT section. If you're looking for something that provides great services, I would highly suggest using this firmware variation. This is one of the best firmware options, in my opinion.

Talisman/Alchemy – Sveasoft has pioneered the way in router firmware development. A lot of the firmware listed in this article are based upon the original Sveasoft code. Because of this, it deserves some mention as a highly configurable, expandable and cost effective solution. This firmware have the ability to do Vlans, MAC-filtering, writable jffs2 partition, WPA2 (AES/TKIP), Radius, WEP, SSH, PPTP VPN, STP, HTTPS, QOS etc. The only problem is their newer version, Talisman, requires you to register for a reasonable fee of 20$ and is MAC controlled (Only can have 10 registered MAC addresses and it wont let you install on anything else but those ten).

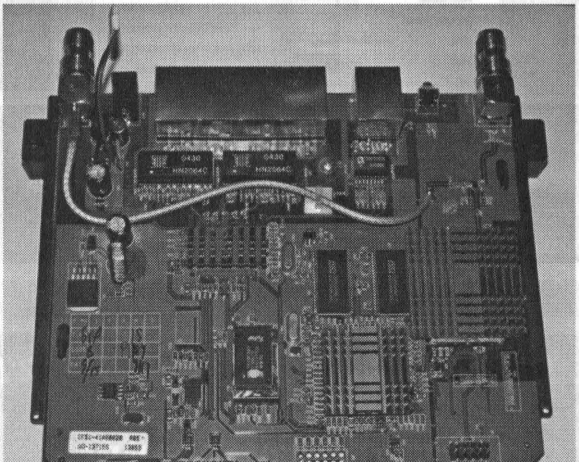
OpenWRT – Linux Experts only! No GUI, and pure Linux. Everything is done from the command line which leaves little room for error. Also you have the option of adding a lot of hardware add-ons such as GPS, LCD display, USB port, headphones, VGA port, Bluetooth, webcam, ability to overclock and much more.
(Complete list can be found at http://wiki.openwrt.org/OpenWrtDocs/Customizing)

In this article we will focus more on DD-WRT, EWRT, Talisman. Space and time restraints won't allow us to show the pure power of OpenWRT and since only some of the reading audience are Linux gurus (Im sure a lot of you are), we will concentrate on advanced and beginner versions.

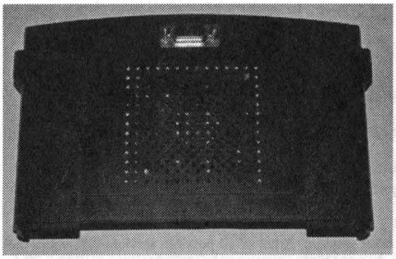
Once you have your WRT54G, you should ensure you have downloaded firmware to match your hardware revision number

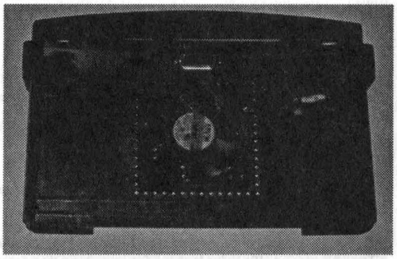
Hardware Cooling
Before we start installing looking at firmware, we will cover what I have done on my Linksys device to help promote cooling. These guys can get really hot when you start boosting their power above 70-80mW. To help cool my devices, I am using a combination or heat sinks and a fan.

WRT54G V3



As you probably noticed, we have several heat sinks attached. The larger flat copper heat sink is attached to the radio that connects to the external antenna connectors (Heat sink on far right). The second heat sink, which is just a tad bit smaller than the radio heat sink (The one in the center) is on the actual processor and MAC chip from Broadcom. The third heat sink, one on the far left is placed on the Ethernet controller. All three chips get quite toasty. On the far upper left hand corner, you will notice a stray cable. This is used for my internal fan (Shown top of next page)





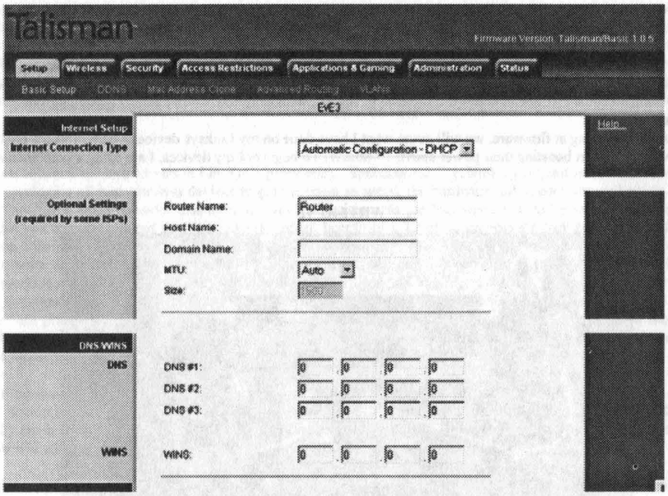
As you noticed, I have an optional serial port that can hook into the pin header located on the bottom right hand corner of the internal picture. The other connector located next to the green light is a Jtag connector which I haven't had the time to install the pin header for yet. Also note that there are extra holes drilled in the top to allow better circulation. Without these holes, the router would make a loud sucking or whistling noise that drove me nuts. Intake holes are also located on the sides of the box to promote circulation (Not pictured).

This is somewhat noisy, but the box is located in the central part of my house and provides superior coverage through my thick barrier walls.

Firmware:

Talisman

Since I am using Sveasoft's Talisman on most of my boxes, we will take a look at it first. Not only does Sveasoft do a great job of adding functionality, but they also include a great looking GUI.



Internet Setup

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some ISPs)

Router Name: Router

Host Name:

Domain Name:

MTU: Auto

Size: 1500

DNS WINS

DNS

DNS #1: 0 . 0 . 0 . 0

DNS #2: 0 . 0 . 0 . 0

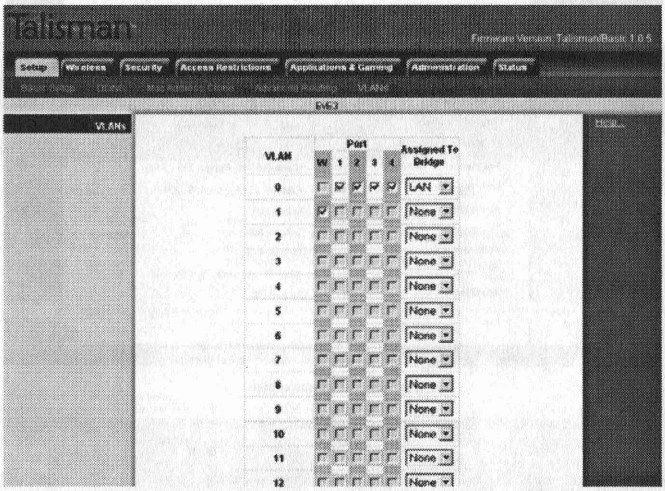
DNS #3: 0 . 0 . 0 . 0

WINS

WINS: 0 . 0 . 0 . 0

Main page

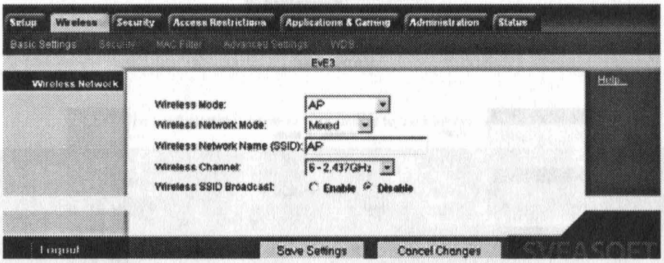
By far the best ability are the Vlans, which are easily configured using the beautify GUI interface. I use this to provide segmentation between the wired and wireless clients to ensure proper security.



VLAN	Port					Assigned To Bridge
	W	1	2	3	4	
0	☐	☑	☑	☑	☑	LAN
1	☑	☐	☐	☐	☐	None
2	☐	☐	☐	☐	☐	None
3	☐	☐	☐	☐	☐	None
4	☐	☐	☐	☐	☐	None
5	☐	☐	☐	☐	☐	None
6	☐	☐	☐	☐	☐	None
7	☐	☐	☐	☐	☐	None
8	☐	☐	☐	☐	☐	None
9	☐	☐	☐	☐	☐	None
10	☐	☐	☐	☐	☐	None
11	☐	☐	☐	☐	☐	None
12	☐	☐	☐	☐	☐	None

Vlan Configuration page

The wireless page offers many options, most notably are the ability to operate in: AP, client-routed, client-bridged and Adhoc mode.



Wireless Mode: AP

Wireless Network Mode: Mixed

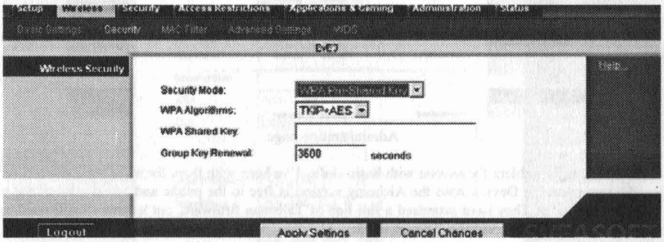
Wireless Network Name (SSID): AP

Wireless Channel: 6 - 2.437GHz

Wireless SSID Broadcast: ○ Enable ● Disable

Wireless Configuration page

As mentioned before, the AP has the ability to WPA2 (AES+TKIP). We also have the standard WEP, RADIUS WPA, and RADIUS to work with.



Security Mode: WPA Pre-Shared Key

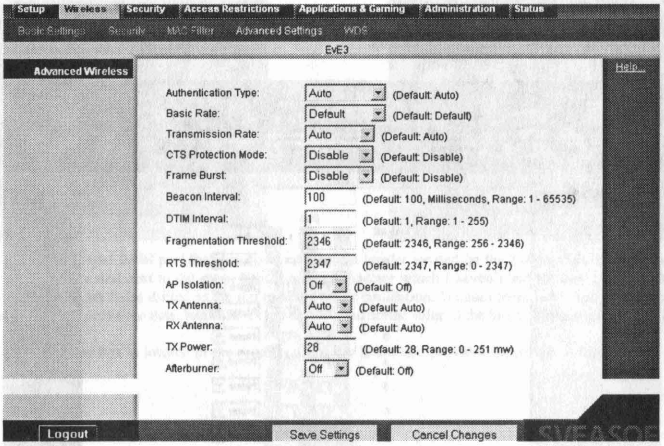
WPA Algorithms: TKIP+AES

WPA Shared Key:

Group Key Renewal: 3600 seconds

Wireless Security Page

The available options for configuring your wireless AP are rather numerous and give you complete control. The second to last option is the power boosting ability. Default set by Linksys was 28, but its safe to say you can go anywhere from 70-80 without burning your box up. I would suggest starting low and incrementing the power to ensure you don't burn or damage anything. 80 mW seems to give a reasonable amount of coverage. (I would show you coverage differences, but haven't got the time or proper weather to do it.)



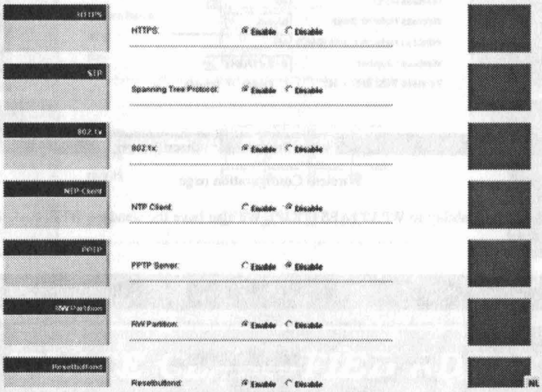
Authentication Type: Auto (Default: Auto)
Basic Rate: Default (Default: Default)
Transmission Rate: Auto (Default: Auto)
CTS Protection Mode: Disable (Default: Disable)
Frame Burst: Disable (Default: Disable)
Beacon Interval: 100 (Default: 100, Milliseconds, Range: 1 - 65535)
DTIM Interval: 1 (Default: 1, Range: 1 - 255)
Fragmentation Threshold: 2346 (Default: 2346, Range: 256 - 2346)
RTS Threshold: 2347 (Default: 2347, Range: 0 - 2347)
AP Isolation: Off (Default: Off)
TX Antenna: Auto (Default: Auto)
RX Antenna: Auto (Default: Auto)
TX Power: 28 (Default: 28, Range: 0 - 251 mw)
Afterburner: Off (Default: Off)

Wireless configuration page

The Security, Access Restrictions and Application and Gaming pages are about the same as the stock Linksys firmware, so we won't take a look at those. They are somewhat self explanatory.

The administration pages contain the ability to activate/deactive any additional services. These services include: AP Watchdog, Cron, DNS masq, HTTPS, STP, 802.1x, NTP, PPTP server, R/W Partition, resetbutton, routing, SNMP, SSH, syslogd, Telenet and UPnP. Some of these options are shown below. Also, note that if you are unable to figure out how to use a certain feature, the help link on the right hand side has detailed information.

Help button!



HTTPS: ● Enable ○ Disable
Spanning Tree Protocol: ● Enable ○ Disable
802.1x: ● Enable ○ Disable
NTP Client: ○ Enable ● Disable
PPTP Server: ○ Enable ● Disable
RW Partition: ● Enable ○ Disable
Resetbutton: ● Enable ○ Disable

Administration page

Sveasoft's firmware shouldn't be a problem for anyone with basic skills. I've been with them for some time and am very happy with my 20$ subscription fee (Must support the Devs!). Also the Alchemy version is free to the public and offers a lot of the same functionality that the Talisman firmware provides. They have promised a full line of Talisman firmware, but we are all still waiting for their release. Currently we only have the Talisman Basic version (Shown above).

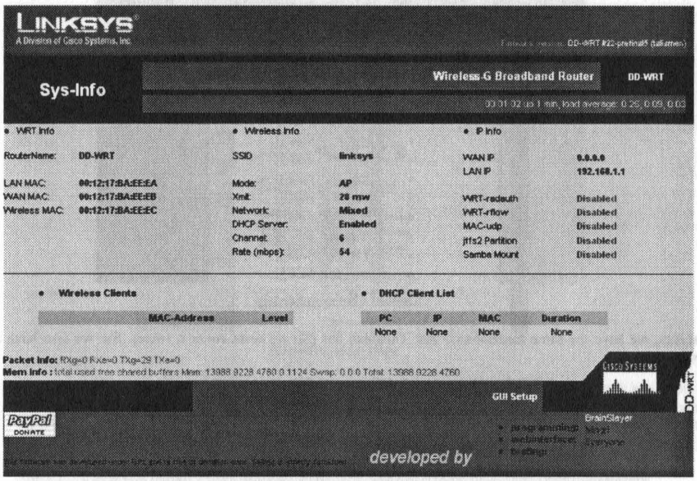
Also, with Talisman, you can install kismet drone (Wardriving), but requires you install and configure it via the shell (Also can be done on other firmware variations). For more information try the links below:

http://toys.lerdorf.com/archives/20_Kismet_on_the_Linksys_WRT54G.html

http://www.renderlab.net/projects/wardrive/wrt54g/sveasoft1.html

DD-WRT

DD-WRT in my opinion, offers better functionality than talisman. The built in functionality further exceed that of Talisman.. A quick look at DD-WRT, show a clean, well organized firmware with a good developer to back it, and only lacks the development team that Sveasoft has.



DD-WRT #22-prefinal5 (talisman)

00:01:32 up 1 min, load average: 0.25, 0.09, 0.03

- WRT Info

RouterName:	DD-WRT
LAN MAC:	00:12:17:BA:EE:EA
WAN MAC:	00:12:17:BA:EE:EB
Wireless MAC:	00:12:17:BA:EE:EC

- Wireless Info

SSID	linksys
Mode:	AP
Xmit:	28 mw
Network:	Mixed
DHCP Server:	Enabled
Channel:	6
Rate (mbps):	54

- IP Info

WAN IP	0.0.0.0
LAN IP	192.168.1.1
WRT-radauth	Disabled
WRT-rflow	Disabled
MAC-udp	Disabled
jffs2 Partition	Disabled
Samba Mount	Disabled

- Wireless Clients

MAC-Address	Level

- DHCP Client List

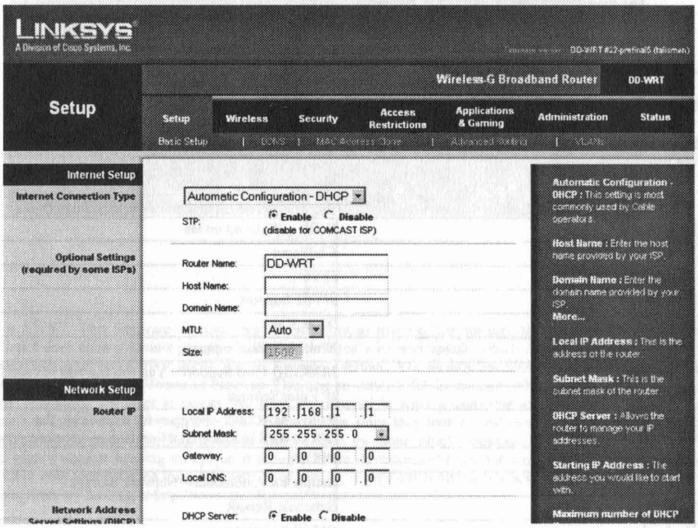
PC	IP	MAC	Duration
None	None	None	None

Packet Info: RXg=0 RXe=0 TXg=29 TXe=0
Mem Info : total used free shared buffers Mem: 13988 9228 4760 0 1124 Swap: 0 0 0 Total: 13988 9228 4760

BrainSlayer

Summary Page

The configuration screen is very similar to the Linksys version.



DD-WRT #22-prefinal5 (talisman)

Internet Connection Type: Automatic Configuration - DHCP

STP: ● Enable ○ Disable (disable for COMCAST ISP)

Optional Settings (required by some ISPs)

Router Name: DD-WRT
Host Name:
Domain Name:
MTU: Auto
Size: 1500

Router IP

Local IP Address: 192 . 168 . 1 . 1
Subnet Mask: 255.255.255.0
Gateway: 0 . 0 . 0 . 0
Local DNS: 0 . 0 . 0 . 0

Network Address Server Settings (DHCP)

DHCP Server: ● Enable ○ Disable

Automatic Configuration - DHCP : This setting is most commonly used by Cable operators.

Host Name : Enter the host name provided by your ISP.

Domain Name : Enter the domain name provided by your ISP.
More...

Local IP Address : This is the address of the router.

Subnet Mask : This is the subnet mask of the router.

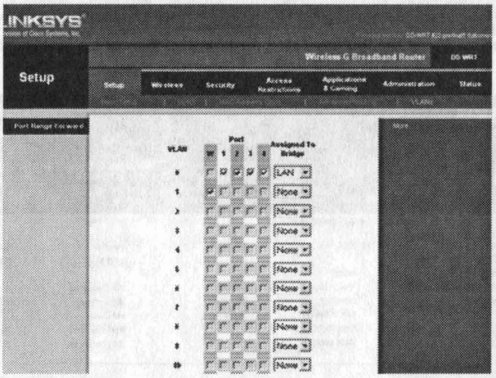
DHCP Server : Allows the router to manage your IP addresses.

Starting IP Address : The address you would like to start with.

Maximum number of DHCP

Main Page

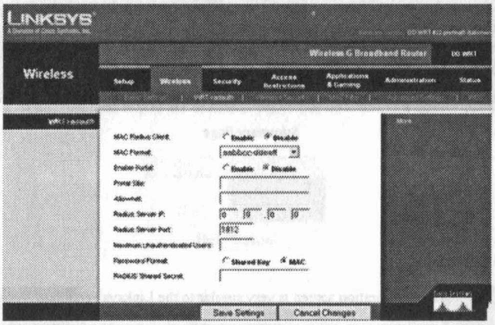
DD-WRT Also offers Vlans, just like Talisman.



VLAN	W	1	2	3	4	Assigned To Bridge
0	□	☑	☑	☑	☑	LAN
1	☑	□	□	□	□	None
2	□	□	□	□	□	None
3	□	□	□	□	□	None
4	□	□	□	□	□	None
5	□	□	□	□	□	None
6	□	□	□	□	□	None
7	□	□	□	□	□	None
8	□	□	□	□	□	None
9	□	□	□	□	□	None
10	□	□	□	□	□	None

Another vlan membership

On wireless ability, we have the same functionality that Talisman has (So we wont cover it twice). But we also have a built in radius server called wrt-radauth



MAC Radius Client: ○ Enable ● Disable

MAC Format: aabbcc-ddeeff

Enable Portal: ○ Enable ● Disable

Portal Site:

Allowed:

Radius Server IP: 0 . 0 . 0 . 0

Radius Server Port: 1812

Maximum Unauthenticated Users:

Password Format: ○ Shared Key ● MAC

RADIUS Shared Secret:

Photo of the WRT-radauth client

A full explanation of the options can be found on the DD-WRT support forum:

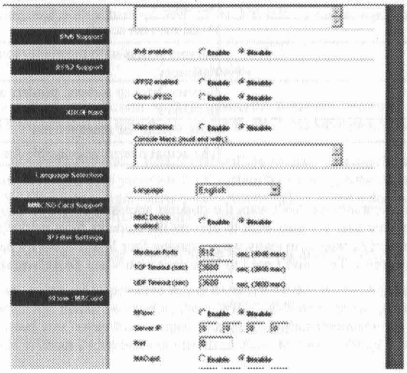
http://forum.bsr-clan.de/viewtopic.php?p=10738

The rest of the options are standard to Talisman. The last part we will cover is the Administration page that offers a slew of optional services that are listed below.

Addition Options

Boot Wait	WOL – Wake up on lan
Cron	Chillispot
Dhcpd	IPV6
DNS Masq	JFFS2 Support
Loopback	Xbox Kaid
802.1x	Multi-language support
NTP Client	MMC/SD Card Support – Yes you can add storage!!
PPTP	IP Filter Settings
Resetbutton	RFlow/MACupd – Program for monitoring the WRT54G/S in a nice GUI interface on your computer
Routing	PPOE
SNMP	Samba FS Automount – Network Storage
SSHD	Schedule Reboot
Syslogd	SMTP Redirect
Telnet	WDS/Connection Watchdog
UPnP	

Most noticeably is the MMC/SD card Support along with the Samba FS AutoMount and the IPV6 Support. SD Card install hardware mod can be found at http://kiel.kool.dk:27/



IPv6 Support

IPv6 enabled ○ Enable ● Disable

JFFS2 Support

JFFS2 enabled ○ Enable ● Disable

Clean JFFS2 ○ Enable ● Disable

XBOX Kaid

Kaid enabled ○ Enable ● Disable

Console Macs: (mac1 and mac2)

Language Selection

Language English

MMC/SD Card Support

MMC Device enabled ○ Enable ● Disable

IP Filter Settings

Maximum Ports 512 sec. (4096 max)

TCP Timeout (sec) 3600 sec. (3600 max)

UDP Timeout (sec) 3600 sec. (3600 max)

Rflow / MACupd

Rflow ○ Enable ● Disable

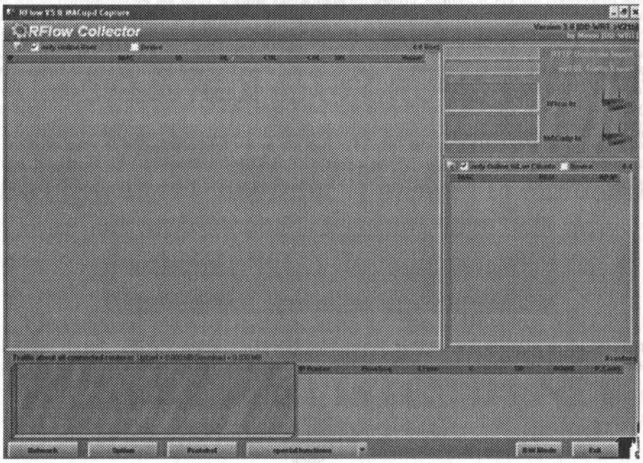
Server IP 0 . 0 . 0 . 0

Port 0

MACupd ○ Enable ● Disable

Administration page

Rflow Connector is DD-WRT management suite for Windows. Personally, I like the idea behind it, but haven't had much time to play with it yet. To my understand Rflow allows you to monitor, in real time, any number of collective routers. It also allows you to see each individual client, the protocols they have used, and bandwidth consumption (Just in case you want to kick those file sharing bandwidth hogs off!)



Rflow Collector

EWRT

Last but not least is EWRT. This firmware version does not offer not as many of the features that DD-WRT and Talisman/Alchemy firmware provide, but it does have a distinct purpose. EWRT is outfitted with nocatsplash, which is a captive portal. Captive portals are those things you often encounter when try to access a hotel's wireless service. You usually encounter a page asking you for a credit card number, hotel room number, or a TOS (Terms of Service). This can be very useful for anyone willing to share their internet connection with their next door neighbors, but want to ensure that they are required to enter a username and password without much technical knowledge. For space sake, we won't fully go into EWRT screenshots since they look almost exactly like the DD-WRT firmware and offer about the same basic functionality. This firmware can be used by those simply looking for the power boost (NoCatSplash is optional!). I would highly suggest keeping an eye on it though; future development plans include a content management suite, radius support and many other cool features. One thing that may be of interest is their small tutorial on how to equip your WRT54G for outdoor use. If you have spare time, try looking at http://www.portless.net/menu/enclosures/

Vlans

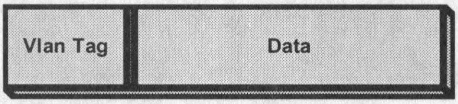
Ok, unless you have some advance networking experience, you probably won't know what Vlans are. As you heard me state before, Vlans are probably the best addition to the Linksys firmware. But you may ask, what is a Vlan? A Vlan is a Virtual Local Area Network. To explain it very simply, Vlans are the equivalent of running two separate wired networks through your building. But instead of wasting cable, we use the powerful Vlan functionality to create these virtual LANs. Each LAN can be made to be totally separate from each other, or you can create firewall rules to allow traffic between the two LANs. This is great when your running an unsecured public access point and don't want them accessing your private computer. My favorite example is in a school setting and is broken down below.

Group	*Access*
Students	Basic internet access
Teachers	Internet access with the ability to access intranet resources.
Resources	Servers, backup servers, printers and other networkable resources
Administrators	Responsible for management
Networking Devices	The actual routers responsible for network connectivity.

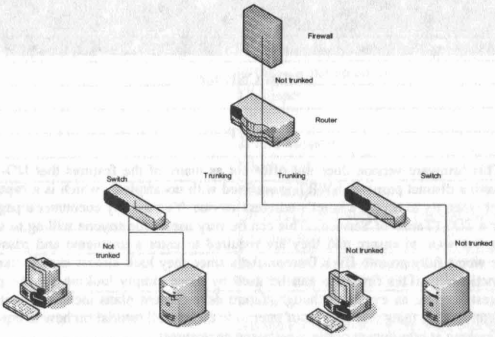
The breakdown is self explanatory. But essentially we don't want the students accessing resources (Such as grade book programs, printers and storage space) that are meant for teacher use. We also want to prevent the students from messing around with switches, and routers. So we create 4 Vlans in this case. You might be wondering why we are having four Vlans when we have 5 groups. The main reason is the administrators need access to 3 Vlan categories. They don't need to have their own Vlan! So we segment it like this,

Vlan 1 – Network devices
Vlan 2 – Students
Vlan 3 – Teachers
Vlan 4 – Resources

To allow teachers the ability to access network resources, we set the ports that the teacher's computer is using to have membership in both Vlans 3 and 4. This allows them to network amongst themselves and still be able to access their network resources. Network devices are the routers and switches, and they reside on their own Vlan. The students and teacher have no need to even know these devices exist. Doing so, could allow a student or teacher to change you Vlan configurations or network settings, thus causing chaos. Students don't need to access anything on the LAN and only need to be able to access the internet. Administrators need full access to Network Devices, Teachers and Network Resources, but not to student computers. You don't want to open the administrators to the dangers of teenage hackers. So the Administrator group would have their port membership set to Vlans 1, 3 and 4. You may be wondering, what if I have more than one device, what do I set the uplink membership to? Well the answer is simple, you want that port to do trunking. Trunking is when the device receiving the information is capable of managing Vlan tags. To fully understand Vlans, you have to understand that when data is transmitted it is sent in packets. When a port is set to trunk Vlans over a port, it does not remove the Vlan number when forwards it to the device at the other end. The device at the other end examines the Vlan tag, and knows who and who not to forward it to. Most of your computers on your network won't need to have trunking enabled. This is because unless you have you computer set up to accept Vlan tags (Some network adapters support it), it won't know what to do with it. (You can set your admin computer to trunk to its port, allowing you to change your Vlan membership on the fly!) Vlan tags are meant for sending data to other physical segments of your network without loosing control of who it's going to. (Note a port with multiple memberships must be tagged, a port with one Vlan membership does not require tagging)



To illustrate what your network should look like, we have provided the following diagram. The links that are tagged are clearly labeled. The link to the firewall itself is not tagged. The firewall does not need to know what Vlans are which. Its main purpose is to protect your intranet.



Wireless Solutions

The most secure solution is not to allow dynamic assignment of Vlan membership to wireless clients. Instead, you should set up a firewall for one of those Vlans and require that the client, such as a teacher or administrator, to VPN into it. This prevents others from trying to gain access by tricking the switch or AP into giving them different Vlan memberships. Another solution, which is not as secure, is to run multiple SSID's (Not supported on WRT54G/S that I know of). Network devices, such as the Cisco Aironet 1200, offer the ability to have multiple SSID's, each assigned to their own Vlan. In this case, you could use WPA combined with something like MAC filtering (Make it a little harder for the hackers) to prevent access to secure Vlans. Another consideration to note, is if you have your AP within public reach, they can easily be reset, thus destroying your SSID to Vlan configuration. A hacker, with decent knowledge could easily get his hands on some Vlan hacking software, and with a trunked link, allow himself access to any Vlan he wants (MAC Filtering, and Port Authentication will prevent this)

Conclusion

This article was meant to give you a brief introduction to three powerful firmware versions, and show you the pure power of the WRT54G. Now that you understand what you can do with them, let use know if you have problems or any questions. Or if you really want to try some cool stuff, you should demand a Part II that will cover hardware mods along with Kismet, Shell Access, IPKG functionality, and maybe turning your WRT54G into you own PBX system by running Asterisk off a SD card or USB hard Drive!!! Or how about turning your own Direct TV Dish into a highly directional antenna? How about a dedicated Linksys device in your car with an SSID of "Hey stupid, stop wardriving"? The possibilities are endless. Enjoy

Hope everyone at Defcon is having a good time. Maybe you'll find me wondering around. Hey, its spot the author time! JK

Please note: Blacklisted411 and the writer are not responsible to any damages caused while playing with your WRT54G. Doing any of the firmware modifications voids you warranty. Please be careful, these WRT54G/S devices can get really hot and start a fire, so be sure to monitor heat and place in well ventilated area, away from carpet, clothes and other flammable objects. If for some odd reason, I made a mistake, please understand I wrote this in about 24 hrs and am very tired. Hard to correct things when your tired.

NOTICE:

**** BLACKLISTED! 411 FORUMS ONLINE ****

Blacklisted! 411 magazine is pleased to announce that our long awaited message forum is now officially open for business.

Please visit our forum located at the following URL:

WWW.BLACKLISTED411.NET

CLICK THE FORUMS LINK ON THE NAV BAR

Blacklisted! 411 magazine is committed to offering both the advanced as well as the newbie hacker a common place to exchange ideas and to discuss hacking, phreaking, technology and community news.

Our hope and intention is to help bring the wide-spread hacker community closer together for a common goal to learn and to experience. Enjoy!

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

2005 END OF SUMMER BEACH MEET!

HOSTED BY BLACKLISTED! 411 MAGAZINE
and HACK THE SYSTEM DVD

THE PARTY TO END ALL PARTIES OF THE SUMMER!

WHEN: SATURDAY AUGUST 27TH

TIME: 3PM UNTIL CLOSING

WHERE: HUNTINGTON BEACH, CALIFORNIA

DIRECTIONS: TAKE BEACH BLVD. SOUTH UNTIL YOU HIT THE BEACH. ENTER THE BEACH FROM BEACH BLVD. AND DRIVE TO THE LEFT. LOOK FOR THE QUARANTEEN FLAG (YELLOW FLAG WITH BLACK BALL IN THE MIDDLE).

YOU WILL NOT WANT TO MISS THIS!

MEET TONS OF FELLOW HACKERS

****FREE FOOD****
****FREE BACK ISSUES OF BLACKLISTED!411 MAGAZINE****
****RAFFLES****
****GOOD TIMES****
****SUN YOUR BUM****
****GET SAND IN YOUR CRACK****
****FINALLY TAN YOUR WHITE TWIGS****
****SEE THE BONFIRE TO END ALL BONFIRES****
****YOU MIGHT BE ON THE NEW HACK THE SYSTEM DVD****

Blacklisted! 411 magazine and Hack the System DVD presents a thank you to our favorite fans! We want you to know that you are appreciated and valued. And to show our appreciation, we're throwing you a party! Not just any party, but a beach party! The last Saturday of August will be a day to remember. Mark your calendars now! Camera's will be rolling, so be sure to be there and you can possibly be on the new up and coming Hack the System DVD! You might also see your picture in the fall issue of Blacklisted! 411 magazine or on our website! Bring your swimsuit, your towels, and your friends.

Details, date, time and place are all subject to change. Check the official website often for updates on this event.

The Hacker Chronicles

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

PART IV

**** 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 College Years

Continuing where I left off in the last issue, I'm now thinking back to when I first started College. I wanted to go to college for the same reason every one else does. To get an education. NOT!! I wanted to have fun and play just like the rest of you. The college parties were insane. I couldn't even begin to admit to the things that went on at the parties. Needless to say, I definitely had fun.

Anyhow, college started out pretty slow for me. I had to get adjusted into my new schedule of working 70+ hours a week along with taking full time classes at a junior college and a technical school. I had a huge workload to deal with. I was more interested in making money at my $26/hr job than cracking open the books, so I worked out a deal with my professors and instructors - as long as I kicked ass on the tests and finals, I didn't have to attend class. This was only after I had been acing my tests for a couple of months, however. They all agreed and for the next five years and three bachelors degrees later, it worked like a charm.

As far as my hacking career in college, it was pretty boring at the JC more or less, but I did have access to the utility room on many occasions which was nice. The technical school on the other hand was a blast. My classmates were mostly normal people who had no clue what they had gotten themselves into, which proved to be entertaining more than anything. However, since I was already so advanced, I got some immediate notice and was allowed to do everything the other students didn't get to do, such as play around with the high end equipment, take my time and goof around with my own projects, etc.

This was about the time I found some new electronic salvage yards which had a much better selection of parts to look through and better prices. I started buying up parts every free moment I had a chance to hit these places up. Eventually, I set myself up with a high end circuit board fabrication area so I could make some nice projects. Initially, I just had the intention of doing this for my own projects at school but quickly realized there was some potential for making money. Before I knew it, I was making some incredible projects and turned them into kits, complete with parts for nearly half of what the other "project" companies were selling their versions for. Mine were feature rich compared to the competition. So I went around school and sold them to other students who were into the electronics hobby. It was a nice way to offset my salvage yard expenditures.

Some of my better projects included a full functioning electronic keyboard (music) with sound sampling capability, a 16 box digital recorder (retail RAM prices were outrageous at the time, mind you), a menu driven call diverter box, a digital call sign box for the ham radio dudes, a fully featured autopatch and other various devices that generally hooked up to the phone line or somehow worked in conjunction with radio transceivers.

This lead to another idea I concocted one day. I was looking through my piles and piles of parts with a good friend and he said, "why don't you sell part kits to the school". What a great idea I thought to myself. After going back and forth with the people in charge of purchasing parts for the electronics classes, I was able to strike up a deal and provide "kits" which provided every electronic component the student would require and then some. It was a lot of parts for their money. The school was happy, the students were happy and I was happy. It was a win-win-win situation.

I dove deep into programming around that time. I learned C++, Turbo Pascal, assembly for half a dozen different processors and helped with the ground breaking of a few script languages now in use today. Now, when I look at code, it's just like reading text for your average Joe. I highly recommend learning at least one programming language to anyone who asks. If you can learn one, learning the rest of them is a piece of cake. They're all similar in one way or another.

Remember the BBS I had been running during high school? Well it was still around and flourishing during my college years. I added more lines, upgraded the equipment and held a special monthly meeting which somewhat remind me of going to Defcon, but on a much smaller scale. The meeting as we called it was merely a reason to party. :) Naturally, I figured a way to milk the idea. I allowed all the females on the BBS free unlimited access… the guys, however, were only allowed up to 1 hour of free time per day. I set up a donation schedule to purchase extra time and the guys couldn't pay me fast enough. The money earned from this completely paid for the BBS operation, all of the upgrades, phone lines and hosted meetings.

Other "chat" boards started to pop up around this time. I had been operating the only known chat board in our area for years, but the idea started to catch on and suddenly there were at least a dozen to choose from. However, regardless of this fact, my system just plugged away.

The one job I had during my college years was at an amusement park. Man, I had fun at that place. The position I had allowed me the opportunity of seeing all the rides from a completely different perspective. Not only did I get to see the rides while they were shut down, I also got to see the control rooms, the guts if you will, of these rides. Additionally, when the rides were shut down from time to time for renovation, I took the time to walk through the entire length of each ride to take a close look at what made them tick. I found out a lot of interesting things about the rides, how they were constructed, how they operated, their flaws and possible dangers. I basically conducted what would now be referred to as "urban exploration" exercises. I didn't know it at the time, but the information I had gathered would eventually prove to be useful in a way I had never imagined.

As I mentioned before, I was working 70+ hours a week at this place. I was making bank and loving every minute of it. I really did enjoy my job and made the most of it. I took it upon myself to explore their computer network when nobody was looking. Yes, I had legal access to the system, but I explored it in great detail whenever I had the chance. Things that nobody bothered to do, nor cared about. Interestingly enough, every employee, their full personal profile and work status as well as their associated pay rate was located on this network and modifiable. I took great note of this fact and considered it to be a very serious problem.

We had an area in the back of the park which we called the "bone yard". It was a dirt area which had roughly 80 containers, you know the large metal containers usually on the back of big rigs and various departments used it to store whatever they felt like. Anyhow, I used to visit the bone yard routinely to see what people stored. I found everything from ancient computer systems to stacks and stacks of files. It was pretty cool.

By the time I had left college with my degrees, I had a bank account full of $$ from the years of hard work and no time to spend any of it and a desire to take a break. A real break. For the next two years, I pretty much floated around and did nothing worthy of mention. Yeah, the BBS was running and sustaining itself. Yeah, I went to a ton of parties. But as far as hacking went, I was out of the loop. Didn't care to be a part of it, nor spend my time doing much else than exploring just how lazy I could really be. Naturally, I was still interested in technology as always, but I didn't have the drive to go out and create anything new. On that note, I'm going to close out this installment. See you in the next issue.

I know what you did last session

By: Jeremy Martin, aka n3cr0psy
info@infosecprofessionals.com

While Janet was sitting in a cyber cafe sending emails to friends and surfing the web, there was a person sitting three tables away reading each email she sent before they ever get to the email server. During this period of time, the thief is able to gain access to her bank account, steal passwords to several business websites, and "archive" her credit card numbers. This scenario is not far from reality and is the main reason that using cryptography is so important in today's technological world.

Most people think that cryptography is an island in the magical land of make believe. However, cryptography is very real and not as complex as most would believe. If you use the Internet, you are likely to use applied cryptography in your day-to-day functions. This can be accessing you bank account to retrieve your monthly balance to purchasing the newest season of your favorite TV show from an online shopping mall. Companies use cryptography to make sure sensitive data stays confidential between the intended parties and the data stays intact. Cryptography is the art of converting messages into a secret code or cipher to protect it from prying eyes. This process alters a plaintext message using an algorithm to create a ciphertext/encrypted message.

History of Ciphers

Cryptography has been in use for thousands of years. In fact, it was in use before 2000 B.C. Egypt in the form of hieroglyphs. The Greeks even used encryption referred to as the Scytale cipher. The Scytale was a long strip of leather with writing on it and was worn as a belt by couriers. This leather strip would be wrapped around a specific sized staff to decrypt the ciphertext. Another popular cryptographic algorithm used by Julius Caesar. This for of encryption shifts the alphabet three spaces to the right and is also referred to as ROT-3.

Applied Cryptography

Ok, but how do I use it and why does it affect me? The basic uses of cryptography are to provide confidentially (secrecy of the data), integrity (protection from intentional or unintentional alteration), and authentication (prove you are who you say you are). Some forms even allow for Nonrepudiation services that prove that the message was written, sent, or received. We will briefly discuss the most commonly used cryptographic schemes that you may use every day while leaving the trivial details out. You will hear the terms X.509 and digital certificates (used in digital signatures) throughout this paper. The most well know companies that sell these certificates are:

- *CA Cert - http://www.cacert.org/ (Offering free digital certificates)*
- *Thawte - http://www.thawte.com/ (Offers free personal email digital certificates)*
- *Verisign - http://www.verisign.com/*

File access

Stenography: Stenography is the art of concealing files or messages in other media such as a .JPG image or .MPG video. You can add this data in the unused bits of the file that can be seen by using a common hex editor. Stenography is the easiest way to hide a message, but is by far the least secure. Security by obscurity is only intended to keep the honest, honest.

PGP: Pretty Good Privacy was created by Philip Zimmerman in 1991 and was the first widely accepted public key system. PGP is suite of encryption tools used for encrypting various types of data and traffic. PGP can be used for S/MIME and digitally signing a message. They use a web of trust that allows the community to trust a certificate rather than a hierarchy Certification Authority (CA) to verify the user's identification.

Personal/Freeware: This can be downloaded from MIT for free.

- Diffie-Hellman key exchange
- CAST 128 bit encryption
- SHA-1 hashing function

Commercial: PGP® Software Developer Kit (SDK) 3.0.3 has received Federal Information Processing Standards (FIPS) 140-2 Level 1 validation by the National Institute of Standards and Technology (NIST).

- RSA key exchange
- IDEA encryption
- MD5 hashing function

Internet traffic

HTTPS: Hypertext Transfer Protocol over Secured Socket Layer. Do not mistake HTTPS with SSL. This is a common misnomer that is spread by those that do not understand SSL. HTTPS uses SSL to create an encrypted tunnel between a client and a server. This tunnel lasts the entire connection and is the most common website security feature on the Internet. This form of encryption is established by the use of a server side X.509 certificate that digitally signs the message.

S/MIME: Secure Multipurpose Internet Mail Exchange. S/MIME uses two X.509 certificates (also called digital signature) and both signs and encrypts the email. The author digitally signs the email with their private key. Once this happens, the message is encrypted with the recipient's public key. When the message reaches the recipient the message is decrypted with the recipient's private key, and then verified using the author's public key. Email clients like Netscape Communicator and Microsoft Outlook can use S/MIME with little setup required.

S-HTTP: Secured HTTP. The benefit of S-HTTP over HTTPS is the fact that each message is encrypted rather then using a tunnel that is vulnerable to both a man-in-the-middle and a session hijack attack. Another advantage of S-HTTP is that it allows for two-way client/server authentication

Tunneling encryption

IPSec: IP Security Protocol is the most commonly used network encryption for the corporate world. When most people in the computer industry think about Virtual Private Networks (VPN)s, they immediately think of IPSec. Companies that use IPSec need an encrypted tunnel that allows all network traffic to flow through. Unlike SSL, IPSec is not limited to a port. Once the IPSec tunnel has been established, the system should have the same network access that it would have at the physical location. This offers far more power, but also requires far more overhead. Another issue is security. The more open the network, the more vulnerable it is. This is another reason why VPNs are usually on the outside of a firewall. Vulnerabilities to IPSec include session hijacking, and replay attacks.

SSH: Secure Shell provides a terminal like tunnel that protects the data crossing the network and should replace clear text protocols like Telnet and FTP. One of the most popular windows SSH clients is Putty.

SSL: Secured Socket Layer can be used to create a single port/socket Virtual Private Network (VPN) using a server side X.509 certificate. The most common use of SSL is webpage traffic over HTTP or HTTPS. SSL is vulnerable to man-in-the-middle attacks. Anyone can create a CA to distribute certificates, but keep in mind that a digital certificate is only as trustworthy as the CA that controls the certificate.

WEP: Wired Equivalent Privacy. This algorithm uses either a 40-bit key or a 128-bit (24 of the bits is used for the initialization vector) key. Most devices also allow for a wireless access point to filter MAC addresses to increase access controls onto the device. WEP is vulnerable and has been exploited by criminal hackers (crackers) while wardriving since WEP has hit the market. Some of the more popular tools used for wardriving are:

- Airsnort - a WEP encryption key recovery tool
- Kismet - an 802.11 layer2 wireless network detector
- Netstumber - an 802.11 layer 2 wireless network detector

WPA: Wi-Fi Protected Access is a new standard that may overtake the old WEP technology in the near future. WPA uses a Pre-Shared Key (PSK) for SOHO networks, and Extensible Authentication Protocol for other wired/wireless networks for authentication. Some cryptoanalysts claim PSK is a weakness due to the fact that a cracker can access the key and brute force the key until it is known. The encryption scheme that is used is Temporal Key Integrity Protocol (TKIP). TKIP ensures more confidentiality and integrity of the data by using a temporal key instead of the traditional static key. Most people welcome this technology over the less secure WEP.

Each encryption model is vulnerable to one attack or another. Below is a list of attack techniques that are used by cryptoanalysts to break the keys used to protect the messages

Ciphertext-Only: This is the easiest to instigate, but hardest to succeed. The attacker retrieves the ciphertext data through listening to the network traffic. Once the key is has been salvaged, the cracker can attempt to brute force the message until it resembles something legible.

Known-Plaintext: This covers the scenario of the cracker having both the plaintext and corresponding ciphertext of one or more messages. In WWII, the Japanese relied on cryptography, but had a weakness of sending formal messages. These messages were able to be broken because the ciphertext started and ended with the same message. Part of the plaintext was known and cryptoanalysts were able to decipher the message using the known-plaintext method.

Chosen-Plaintext: Similar to the know-plaintext attack, but the attacker can choose the plaintext to be encrypted. An attacker can assume someone else identity and send a message to target that needs to be encrypted. Since the plaintext is chosen and the target sends the encrypted message, the chosen-plaintext attack is successful.

Chosen-Ciphertext: The cryptoanalyst is chooses the ciphertext and has access to the decrypted plaintext.

Birthday Paradox: This attack is successful when a hash value of a plaintext matches the hash value of a completely different plaintext. This anomaly is proven mathematically among 23 people, there are 23*22/2 = 253 pairs, each of which being a potential candidate for a match.

Brute-Force: This form of attack is implemented by passing through every possible solution or combination until the answer is found. This is the most resource and time intensive method of attack

Dictionary: The attacker compares the target hash values with hash values of commonly used passwords. Dictionary files can be downloaded from hundreds of Internet sites.

Man-in-the-Middle: The attacker intercepts messages between two parties without either target knowing that the link between them has been compromised. This allows the attacker to modify the message at will.

Replay: Replay attacks are simply the replay of captured data in an attempt to trick the target into allowing the unauthorized access.

Back at the cyber café, if Janet connected to a secured web server using SSL to do her online banking and used S/MIME to send private email, the cyber thief would never had a chance of seeing her unmentionables.

War driving Meets Social Engineering

By Doobie Won

War driving is one of the fastest indications of the level of insecurity in a specific area. Most of us have assembled the kits, driven the miles and logged the points. This paper will not cover the actual wardrive. What it will cover is the eminent dangers with the information gathered from it. The basic goals of social engineering are the same as cracking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network.

Recently a group scanned a section of road frequented by millions of visitors a year. Over 1000 access points were identified. At first glance the list may look like any metropolitan area. It's no secret that insecurity is not restricted to any race color or gender. What was found in this list was a full name of a certain person as the SSID. (For the sake of their personal interest they will remain nameless).

Let's say that it was your name. The following can be completed in as little as 30 minutes. The aftermath could be with you for a lifetime. With the use of GPS, you have cut at least 5 minutes off the total time due to the fact that you have the building identified.

Step 1
Entering the name into the search engine may seem like the first thing they do, but your jumping the gun. Attackers obtain the easiest information first and then obtain the details. The first step the attacker will use is to run the name on the yellow page's site. In a few seconds the name is verified and they obtained the address and phone number. The use of unlisted information will only affect roughly 5% of all searches worldwide.

At this point the professional social engineer would begin a probe using the phone number. It is important to realize that 99% of all people assume that you are who you say you are.

Step 2
The second step is a very specific search on the Internet. Only a few sites have to be used to get the best results. Examples of sites that reveal personal data include: Ancestory.com,Kindredkonnections.com, People.yahoo.com, usa-people-search.com, 1800ussearch.com, ussearch.com, familysearch.org. The use of search engines such as Google and Mamma.com access a larger scope of possible information on the target and has been found to be more useful. Pay sites enter a new level of danger into the equation. Information can be gathered from sources such as credit histories and background searches just to name a couple.

The output will be a detailed gathering of personal data: family member's names, locations, various dates as well as current and past jobs with locations and phone numbers. In some states, part of the VIN and the LIC# of the vehicle parked in the driveway will net you an owner's name. It is also good to remember that public account of marriage, awards, and even death will be readily available for the attacker.

The use of extensions in the search process may reveal key pieces of sensitive data that might otherwise go unnoticed. Entering the name with possible credit card ranges into Google may result in obtaining their financial data. Entering Office extensions may result in more than you bargained for. With the information gathered thus far from the victim, you may even be able to start guessing financial website logins.

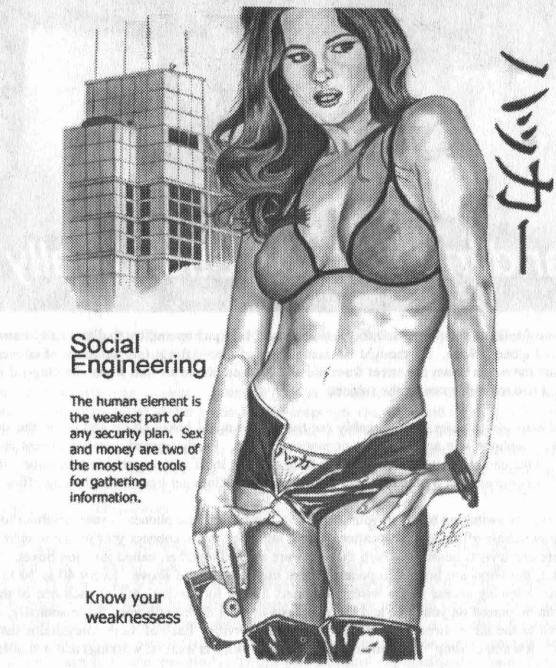
Now that the details have been compiled the possible outcomes are limited to the psychological state of the person gathering the information as well as there intent. No programs or probes are needed to infiltrate the host computer. The world in which we live is built on rules and boundaries. Security is not one of them. Do yourself a favor: use encryption, use complex passwords, and for the love of security, don't use personal information on your router.

Editors note: The above referenced use of the google search engine to find information on people has been coined "Google Mining" as of late. Just thought it would be a good idea to mention it. Hack the System!

Social Engineering

Resistance is futile

By Double-O-Jake



Social Engineering

The human element is the weakest part of any security plan. Sex and money are two of the most used tools for gathering information.

Know your weaknessess

So, you're sitting at work doing your job just like you do on any other day of the week. A well dressed gentleman whom you've never seen before walks up to you can demands that you give up a piece of information on a certain someone or company. Never stating his name nor how he may be associated with the company you work for, the man looks and sounds serious and he appears to know what he wants so you quickly decide he must be your superior...and you give up the information. You go about your day and probably don't think about it again.

Well, you probably just got hacked, owned or whatever you want to call it. A proficient social engineer can walk into a situation, get exactly what he wants and walk out, usually without making much fuss or leaving any evidence behind, including a strong memory of what he looked like. The pro's are so good, most companies have no idea they're been engineered until it's too late. In fact, the sad truth is, they will probably never even know about it. The social engineers target? The unsuspecting employee that has no idea who he's really working for. This tactic is especially well suited for large corporations or retail stores who generally employ people who don't think for themselves. If they did think for themselves, they would probably be self employed like so many other are today.

Take the case of Wal-Mart employees. I shop at the place, I admit it. Why? Because they have the best prices on most of the things I like to buy. Why else? Oh yeah, they have a cool phone system to mess with. And yes, you can get an outside line and place long distance calls. Nice, but far from the point I was trying to make. The point is that they hire just about anyone, mostly people without a degree or higher education, regular everyday people. The problem with this? If you haven't figured it out yet, a gifted social engineer could walk into a place like this and wreak havoc. Anything from getting free product, to causing someone to lose their job, perhaps even many people losing their jobs. For instance, I was doing some of my weekly shopping for DVD's and I heard over the intercom, "YOU ALL SUCK" then a "click". Someone had accessed their intercom from an outside line and made their statement. Upon further investigation, I found out exactly what had happened. A caller, who remained unidentified called in and spoke to customer service. The lady working customer service was convinced that the called she was speaking to was a company executive and required emergency use of their intercom system. Naturally, the CS lady had no idea how to do this, but the caller was kind enough to tell her how to make it happen. She followed his instruction and the call was transferred to the in-house intercom. The message was then placed. That easy.

Now, this was, in my opinion, a fairly harmless prank, however it could have been much worse. What if the called decided to use the intercom system to create a panic? I won't give details on my thoughts of what could create a panic, but what if the caller had done this? Someone could have been hurt or possibly killed in a situation like that. Have you ever seen a stampede of human beings running for their lives? I have. It's not a pretty site. One tip: stay out of their way unless you want to be trampled over.

Anyhow, this short article is to point out that there are nefarious social engineers out there who can cause damaged. If you work for a large company, always know who you work for and who to ask for help if something questionable comes along.

TELECOM HOT DROPS

Is your landline conversation really safe?

One day I was talking to my best friend on the phone and then I heard some lady pickup and try to dial a call. I assumed it was someone at my friends house since I lived alone. Nope. He thought the same thing of me. After a few moments of conversation with this third party, I learned that she had just moved in down the street from me and she had phone service when she plugged in her phone… so she had been using it! Interesting. I had to learn more on the subject.

If you live in a community without utility poles, you probably see these little metal boxes all up and down the streets of your housing tract. What are they? They're telephone line access points or junction boxes. Easily opened, you can access the wires that bring the phone service into your home. One can also access the dial tone from the box itself with a portable telephone - this is known as beige boxing. So, what's a hot drop? Let me explain a little bit about how these phone lines get from the switching office to you.

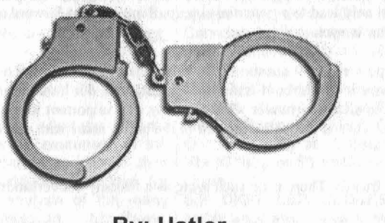
First, imagine the telephone company switching office in your area. This is where all the phones in your neighborhood ultimately connect to the phone system. From the switching office to your location, wire is stretched out to connect your phone to their switching equipment. Along that stretch of wire, there are several points at which the wires are spliced together, called junction boxes. When the wire finally makes it into your housing tract, the wires are bought to pedestals like the one pictured above. Every 40 to 50 feet or so, there will be another one of these, each time, allowing access to the wires to connect homes for service. It's at each one of these points, where the wires are splice, that a "tap" can be placed on your line and the wires run off to a different home. So, essentially, any number of homes could theoretically be connected to the same wires that provide your phone service. Each of these connections that isn't who the line is meant for is called a "hot drop". It's a line "drop" into someone else's home which is live (ie: working) and it should not be.

I want trolling around my neighborhood one day and allowed myself access to the utility closets in each of the apartment buildings up and down the street. What I found was very interesting. For instance, where I lived, we had exactly 20 apartments. However, the utility box which contained the phone lines had exactly 50 lines available (of which only 20 were in use). I tested each of the lines and found that around 38 of them were working lines with dial tone. Since only 20 were in use at my apartment building, I could clearly see that there were an extra 18 lines or "hot drops" available to mess with. I refrained from doing any further testing. But I found the same thing happening in all of the apartment complexes up and down my street. Eventually, I devised a plan where I used the phone companies own wirepairs to get a direct line from my home to my friends home all the way down at the end of the same street (about 5 blocks away) and it worked for several years before the phone company pulled the plug.

On a few of the trips around my neighborhood, I found other interesting items within the utility rooms/closets. At one location, I found a an elaborate call diverter in place. I took a good look at it and determined that it was a professional piece of equipment and left it alone. In another, I found a completely self contained automatic recording device connected to a line. The recorder had an inventory control tag on it which clearly identified the unit as belonging to a private detective firm. Not really smart of them if you ask me. I also found some small hand tools, some spools of wire, a few small pamphlets and even a linemans handset. Aside from that, I enjoyed the colorful notes that the telecom guys had written to each other within the confines of the utility space. It was obvious that the telecom technicians were having a lot more fun on the job that the Edison workers or the cable workers. I assume this because there were few, if any, notes between those workers.

The point of this article is to make people aware of this and to illustrate that the hard wire phone lines that we use and take for granted as "safe" are anything but safe. Anyone who knows what they're doing could come along and tap into your line, record conversations, use the line to make long distance calls, etc. Good grief. Luckily, I don't think most of us have to worry about it. When you're on a call and someone joins into your conversation, you better start wondering.

THINGS TO REMEMBER WHEN DEALING WITH THE POLICE



By: Ustler

Well this seems like a subject that is hardly ever discussed, and is usually left to the lawyers. But just In case you are questioned or arrested here is some information you should consider.

First off, never volunteer information or consent to a search of your possessions. Just to stress how important this is, here is a quick example. Let's assume you are accused of hacking into a large corporate database and stealing hundreds of credit card numbers and personal information. You are picked up and questioned. Your first impulse is to try and help the police since you know you had no involvement in the crime. So you agree to have your computer and possessions searched. Here is the problem. Even if you didn't commit the crime, Information that is illegal or misleading can be used against you. Such as visiting blacklisted411.org, downloading illegal music, software and even your personal communications can be subject to search and seizure all because you agreed to have your computer searched because you where INNOCENT.

Make sure if they ask to search your possessions, or home, clearly state "I do not consent to this search". Without a search warrant, anything discovered when this ILLEGAL search was performed is not allowed to be admitted in court unless it was in plain sight when the approached you. If they already have a search warrant, ask to see it. If they force themselves in, do not resist them. Doing so could allow them to arrest you for trying to destroy evidence or prevent a lawful search. Make sure to let them know that you still do NOT consent to the search. When they are searching, follow them around, and ensure they are only taking the items listed on the search warrant. It will usually say something like "Electronic media, computer storage devices, and magnetic backup devices". If something is in plain sight and they find it (Drugs etc) they still can confiscate it and charge you with possession.

If you have your possessions in a locker, make sure to keep them in a backpack. If the locker belongs to a school, workplace or is otherwise not owned by you, the owner can allow the police to search it without a search warrant, but the law does not allow them to open up your personal possessions. Also a lock on your backpack can further help protect you rights. Without a lock, the police could state that the backpack was open and the evidence was in sight after opening the locker.

Second off, if you are interrogated or questioned, you have the right to remain silent. Remember, the police have the ability to LIE to you. This can include, but not limited to, producing convincing evidence of your guilt and lying about witness testimony. Remember, don't respond to these tactics. When being interrogated ask repeatedly if you under arrest, if they say no, tell them that you will be leaving. If they won't allow you to leave, demand that they provide you a lawyer. If you are under arrest, make sure to ask them what they arrested you for and state that you will not be talking to the police until you have a lawyer.

While you are being questioned, remember the police will often try to draw emotions such as anger or remorse. If you are having problems containing your emotions, remain quite and think on something that has no relevance to the interrogation, such as your favorite video game or favorite movie. If you are able, clear your mind and ignore everything the police are saying. Do not make eye contact with the police; this can only lead to a potential slip up. Stare straight forward and if they try and distract you, or shout in your face, demand to speak to your lawyer.

If you are under the age of 18, the police cannot question you without your parents' presence. This is usually the case, but I highly suggest checking your local law since it varies from state to state. First off, don't admit anything to your parents. If your parents waive your right to a lawyer, remain silent no matter what they say. It's important to note that these police interrogation rooms have wonderful listening devices, so even if the police are not in the room, make sure you either are speaking to a lawyer or don't speak at all.

Remember, the police are not your friends. There is no such thing as a friendly conversation. They are there to do one thing, obtain information against YOU.

We often hear about police brutality, but what happens if you are brutalized. Evidence of brutality can be a major pawn in a court room. If the police hurt you in any way, they can easily be sued for a lot of money. Even if you don't want the money, the threat of a lawsuit by you lawyer will usually cause them to back off and leave you alone. While being questioned, if you are grabbed, or forcefully pushed in anyway without necessity from the police, immediately cover that area and demand to see a doctor. If they refuse, state you are hurt and require medical assistance. If they insist that you are fine, demand to see a doctor and remind them that they are not trained medical professional. If they still refuse, demand a lawyer and lay on the floor and refuse to talk. When you do get to a doctor, make sure to tell them what happened. Do not undermine the force used on you, in fact make sure to stress how you where brutalized. If you do have to go to court or want to file lawsuit against the police, the nurse will make a wonderful witness. If you have no signs of damages, let them know that you don't bruise easily and that you still suffered pain. If they press on your wound and you feel the slightest pain, let them know.

If you are being arrested, the police must identify themselves. If you try to flee and the police did not identify themselves by showing a badge or giving a vocal command stating who they are, you cannot be charged with resisting arrest. For all you knew, they where a gang of ruthless thugs after your wallet. Just I case they do identify themselves and you continue to flee, you can easily be charged with resisting arrest which definitely will not help you in court. The best you can do is walk away unless they call your name. Under this circumstance, you can argue that you did not know that they where trying to arrest you or did not hear the officer because of the background noise, so you cannot be charged with resisting arrest.

Thanks to television, we all know that after being arrested you must have you Miranda Rights read to you. Just for some background on the subject, the term Miranda Rights came from the case of MIRANDA V. ARIZONA 384 U.S. 436 (1966). The following is a quick overview of the case. In 1963, the theft of $8.00 from a Phoenix Arizona bank worker was committed. Not long after the crime, the police arrested Ernesto Miranda with the suspicion that he was somehow involved. After two hours of being questioned, Ernesto Miranda not only confessed to the theft, but also confessed to the Rape of an 18 year old woman that was committed 11 days prior to the theft he was charged with. During this time, he was never offered a lawyer or informed of his rights. Based on his confession, he was convicted and sentenced to 20 years in prison. His lawyers appealed to the U.S. Supreme court arguing that his rights had been violated. The U.S. Supreme court agreed, and vacated his previous conviction and allowed him to go to trial without his confession being offered as evidence. Please note the police do not have to read you your rights or offer to provide you a lawyer if you are not under arrest and simply being questioned. Also remember, that you must understand your Miranda rights. So if you are slightly confused about the smallest detail, you can insist on having them explain it, or request legal console to further help you understand. If for some reason, you have a poor understanding of English, or don't fully understand your rights, evidence or confessions can be thrown out.

The last and final thing we will cover is how not to allow them to obtain fingerprints or DNA while being questioned. First off, the police are not your friends. If they offer you a drink, do not take it. The drink, which is owned by the police, can easily be dusted for prints and used against you. Keep you hands in your pockets at all times or on your own body and away from police property. As for DNA, do not allow them to take it. If they try and force you to have a blood test done, stress to the nurse or doctor that your religious beliefs do not allow doctors to take blood, hair or mucus samples. I would highly suggest you quickly convert to something like "Christian Scientology" or other religious organization that does not believe in traditional medicine. This may help but don't rely on it. Remember, they can't get a court order for your DNA unless they have probable cause.

In conclusion, by taking these steps you can further ensure that your rights are not violated by the police. Please take proper precautions, no one really likes going to jail or to court for that matter.

Note to law enforcement: I fully understand you are just doing your job. I mean no offence by this article. It's only meant to help protect the rights of individuals, not to allow criminals to escape prosecution.

Note to readers: Under no circumstances does blacklisted411 or the writer of this article encourage you to lie to the police, even though they lie to you. We encourage you to seek professional legal advice before dealing with any branch of law enforcement. This article is being written from my personal beliefs and observations of police tactics (Not from T.V.) and independent research done on my part. This article is for information purposes only and is protected by my First Amendment rights (Free speech, freedom of the press).

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. <BR> 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

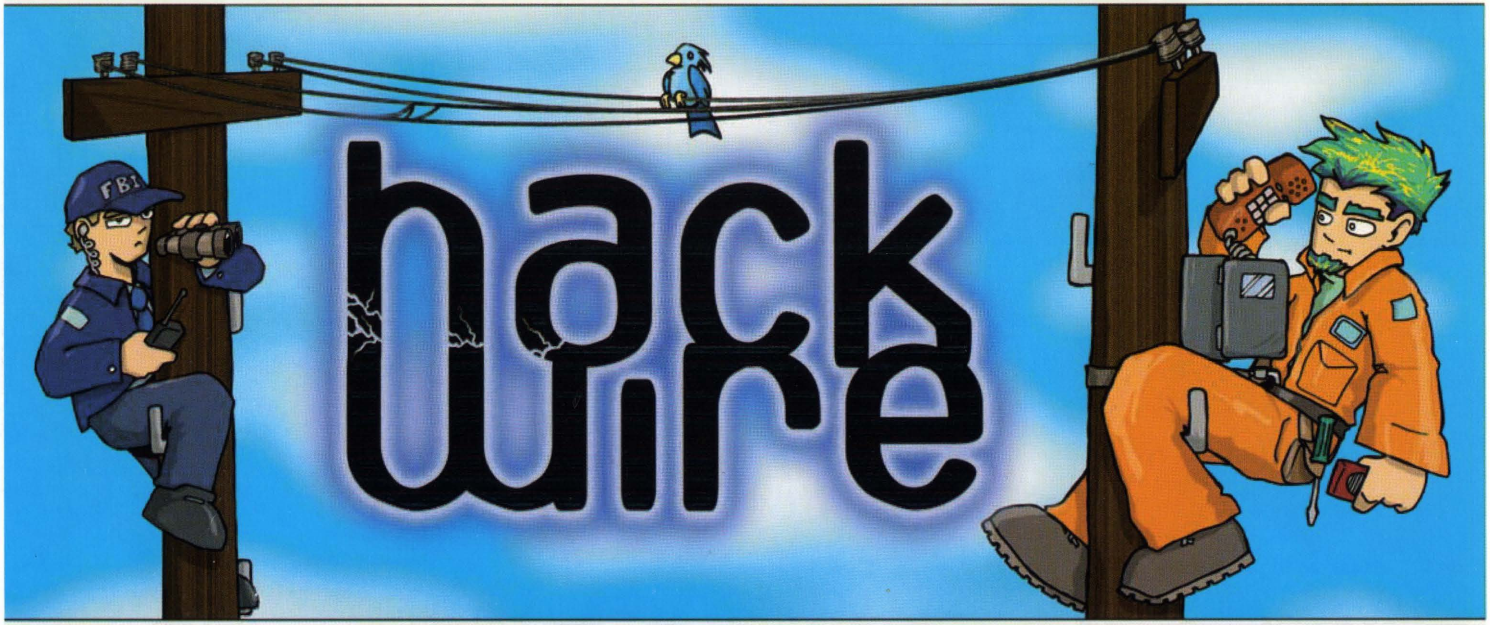
(666 Area Code) - Tijuana, B.C.

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.


hack
wire
FBI

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