Blacklisted 411

The Official Hackers Magazine

Hack The System...

Current News

.NET Edition 6 Released
BL411 Attending DEFCON 14 with SWAG
2007 Membership Card Design Finished

Inside This Edition

Image Manipulation ID
Scanning in the U.K.
ID Theft: Plugging the Keyhole

VOLUME 8 ISSUE 2 SUMMER 2006

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

Web Admin

Ustler

Writers

Ustler, Unicoder,
Dr. Fibes, Jeremy Martin,
The Goldfinger, dual_parallel,
MobbyG, Cactus Jack, ML Shannon,
Grandpa Hackman, Electra-Solve

Inside this issue

Additional information

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

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

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**

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.

8460342QZOPLVSNF-7512

EKCI 92,59,17,28,03

PRINTED IN THE UNITED STATES OF AMERICA

Icons used on the front cover are from Dropline Neu! created by Silvestre Herrera and are released under the GNU General Public License (GPL). A full copy of the license and icons can be located at http://www.silvestre.com.ar/or available on request as required.

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 our peak, at least 150 disk copies <per month> of the disk magazine were sent into the public, 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 the 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

The last two years have been an exciting time for the staff and crew over here. We have become extremely 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 many others. 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 run a vendor booth at these events and we make available our wares - subscriptions, back issues, t-shirts, hats, stickers and other SWAG. We also provide several "convention only" promotions such as the Apple IPOD give-away we held at DefCon 13. Our give-away was a big hit. We're planning on attending DefCon 14 this year and we'll be holding our own private catered reception for subscribers and supporters. Additionally, we'll be handing out membership cards with all new subscriptions this year. Whatever you do, be sure to check out our booth first, you'll be glad you did!

Magazine Development
A major effort has been 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 far surpassed our goal within our timeframe.. To date, Blacklisted! 411 has a circulation over 200,000 copies per issue. Based on orders from distributors and sell through, we're doing excellent in the marketplace. Additionally, we have been seeking and hiring freelance writers, techs, photographers, and editors to increase the quality and scope of the magazine. We've also been promoting the magazine outside of our community to bring in cross-over readers.

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, gadgets and technology.....whatever our creative minds can come up with. Ideas and suggestions on this subject will be accepted and appreciated.

Charities
People generally believe that hackers are awful scum-sucking low life degenerates not fit to inhale the air they breathe. This idea has been pounded into the heads of people repeatedly by the mainstream media. Not necessarily because they're evil-doers, but more likely due to the fact that they simply have no idea what hackers are or what we're all about.

They think we're an uncaring bunch of thieves. They couldn't be any further from the truth. Hackers do care. In fact, they probably care more about the things that really matter than your average Joe does.

Blacklisted! 411 is owned and operated by real people who care about things aside from hacking. No, really. In the spirit of helping people and organizations outside of our community by offering real support, not only have we done a good deed, but we've demonstrated our philosophy at it's core level. We want to help. As such, *Blacklisted! 411* Magazine has officially donated to several local charities in an effort to achieve this goal.

First and foremost is the local chapter of the Ronald McDonald House. Many people have never even heard of this place, but nevertheless, they're a wonderful bunch of people who offer an amazing service to those less fortunate families who have a child in the hospital....they offer a place to stay and a hot meal - for FREE (or a very small donation if you can afford it). We've donated many items to help their cause because we really believe in it. One of our favorite donations was the 200 some odd small children costumes we supplied them with to give to the children around Halloween. If you have children of your own, maybe you can appreciate this place a little better. *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. The festival they operate is much like a small carnival with rides, food, drinks, and entertainment. They also run a huge raffle which is right up our alley as far as lending a helping hand goes. We've been able to supply them with some unique and stunning prizes for the children who attend the festival. Prizes you wouldn't expect to win for a cheap raffle ticket.

Our hope is that we were able to brighten up the day for some children, maybe even a family or two....and help our community at the same time.

Of course, we also donate to EFF and other hacker-friendly groups. That really goes without saying, right?

Closing thoughts
Let's start our closing thoughts by mentioning that we're your friendly neighborhood hacker magazine. We're one of the team players and happy to help people. Please don't feel that you cannot approach us.

So, if you have questions, comments, articles, ideas, suggestions, have a business proposition or wish to offer support in some way, please contact us and let's see what we can come up with. Thanks for your support, hackers!

BL411

Important notes of interest:

SWAG NOW AVAILABLE
That's right! We have SWAG now. We have some cool "Hack the System" T-shirts and baseball caps, plus a wide variety of bumper stickers available at our online store. We'll soon have some additional SWAG and technology available as well. Keep watching. www.blacklisted411.net

DEADLINES
For some reason, people seem to miss our deadline mention in the magazine and online, so be sure to read this. The DEADLINE for articles, letters, artwork and ads for Volume 8, Issue 3 is October 1st, 2006. Got that? OCT 01 2006

ADVERTISING
People often email us asking if classifieds are free. We keep telling everyone YES. Classifieds are free. If you have a classified you want us to run and it's topic related to the magazine, send it in and we'll consider it. Ads are limited to space constraints per issue. First come, first served. Naturally, we reserve the right to reject advertising for any reason.

ARTICLES
Do we really need to mention this one? We're a magazine and we NEED articles. If you're a writer and want us to consider your work, send something to us. Don't waste any time. We're a PAYING MARKET. What does that mean? It means that we pay for articles which we use...but only if you want the $. We can donate your payment to your favorite charity if you'd like. Our rates are generally $75-$100 a page, depending on size, quality & use of photos.

ONLINE CONTENT
If you haven't noticed it yet, we have a website (www.blacklisted411.net) and we like to fill our pages with interesting, topic related content. If you'd like to write articles/reviews for use on our website, send them in.

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

Welp, this makes another issue late to print and late to the newsstand. It seems like there's a never ending supply of excuses which printers and distributors have available at any given moment in time, most notably when WE need something. Oh, I don't know, like getting paid, maybe? Or how about having our issue printed? I'm still waiting for this one: "My dog died". Close, but not yet.

Yeah, so I won't name any names, but needless to say, I'm a little perturbed right about now. Regardless, no matter what the setback, we're going to keep publishing issues as long as the readers still want them.

So, what's new for this issue? Well, we've streamlined the magazine on just about every level which ultimately means more hacking and less crap. I'm sure that's what you wanted to hear, right? Good. That's what we like.

It appears that we had a little bit of trouble with the shipment of our last issue with the release of our 2006 membership card. We tried our hand at bulk mail, using a service provider and it blew up in our face. Seems that many of our subscribers didn't get their issue along with their membership card. Figures. Anyhow, Alex took the situation head on and replaced the missing issues/cards. If by some chance you're still missing your issue along with the membership card, fire off an email to subscriptions@blacklisted411.net and let us know.

Many have been asking about the Hack the System DVD and if we're still doing it. In short, yes. The long of it is that we're dealing with more serious issues and we've slowed down our work on the DVD itself. Most, if not all, of the footage has been shot and the product is in post production now. There's no set ETA for this product, but we hope to have it ready by Christmas 2006.

Given that approximately 99% of our Q&A letters had to deal with nothing appealing enough for print, I decided to axe the Q&A section for the summer issue. I know, I know. What a bummer. People complain about these kind of crap letter so we won't publish them anymore. If you have some serious questions for print, please send them in. We'd be happy to answer them in print.

What about the online magazine? Again, little to no support from the community, so the project has been put on indefinite hold until we decide what to do about it. We made it six issues in, the whole time asking for support. What'd we get? Tons of praise, little support. The idea is wonderful in theory, but it doesn't seem to work in practice. We're not giving up on it yet, just rethinking the idea before we try a second go at it.

So, we're planning on being at DefCon this year. Hope to see you there. HACK THE SYSTEM.

- Editor

Scanning in the U.K

by Radio_Phreak

Hi I am radio_phreak. I am a scanner here in the UK and am going to explain a little about scanning here in the UK and how with a little bit of creativity it can aid you in your social engineering applications. A little background on myself. I have been into scanning for 2 years now and have generally avoided the scene for a number of reasons:-

1. Why draw attention to yourself and your activities?
2. I find a number of people on the scene steal your ideas.
3. Why should I share my knowledge when people are going to claim it as there own?
3. I am shy

I am not going to tell you exactly how to do all the techniques. My aim is more to put the idea into your head and point you in a better direction. This will allow you to discover all the information and exploit in your own way. If I were to tell you how to say, install yourself into a trunk and you did that, not only would that make you a criminal it would then make you the radio phreak equivalent of a script kiddie.

By all means ask questions, play dumb online, even if you know what you are talking about just to confirm your knowledge but do not just copy people's work. The contents within this article are for educational and information purposes only. If you choose to use the techniques or idea's in this article and are dumb enough to get caught doing anything illegal, it is not my fault. I am just sharing my knowledge because I don't believe that any 1 person should have absolute knowledge and who knows, I might even be wrong and someone else can help me

I am in no way responsible, Consequently, Inconsequently or directly any damages/loss of earnings or anything remotely possible as a consequence of misuse of the information given.

In the UK the Wireless telegraphy act of 1949, states "It is illegal to receive broadcast's for which you are not licensed for." Which basically means in a nutshell: No listening to boats, airplanes, taxis, police, ambulance's, fire brigade (which we can't do anyway because they have all moved to TETRA, read later on in the article). Basically the only things you are allowed to listen to are broadcast radio, amateur radio (how boring) and PMR 446 which isn't really interesting but doesn't stop a lot of people. This is an old and outdated law which originated in 1949. There have even been calls to see scanners banned all together! A few years ago man who shall remain nameless for legal reasons was approached by 2 reporters working for a nationwide TV channel here in the UK Basically he spilled his guts to the channel who then broadcast it. As a result this has led to all sorts of things changing. It has also been suggested that (not by me) spilling his guts. Helped the police push their new communications system, which has 128 bit encryption which is basically uncrackable.

Here in the UK the Police, Fire Brigade and Ambulance service can no longer be heard via a normal scanner they are all on a scheme called airwave (http://www.airwaveservice.co.uk/) it is run buy GSM mobile phone provider 02. This is basically a Tetra based system (Tetra stands for TErestrial Trunked RAdio). It is highly encrypted and so far no programme's or even solutions have come even close to cracking it. The encryption algorithm changes hourly.

I personally believe it may be many years before a crack is found. Tetra is far superior to UHF analogue in that it allows multiple users on to a single frequency (A.K.A Full Duplex Conversations). The people in the control room have the option to announce all units' broadcast or just to speak to an individual officer. In addition to these features with stolen equipment: the control room can lock it out of the network and switch on a GPS unit allowing them to track the unit down. One of the advantages of tetra is that it allows GPS and data packets performance wise it offers GSM like performance without the GSM based costs. The Police were on analogue UHF using Motorola PMR equipment and communicated privately with their control room via GSM Nokia mobile phones. This was found to cost more than the implementation cost's and radio channel hire therefore Airwave was rolled out. There have been rumbling's inside the police however, about a number of things. First it does not have the reliability of GSM and UHF analogue based radio (because it's new and because its all Computer based) also the police do not own the communications infrastructure for Airwave which means 02 UK can cut it off at will. This is being implemented over the next 2 years with all Forces expected to be on airwave by 2007 with some Forces remaining on MPT1327 Trunking schemes until then.

So what reason is there for us to carry on scanning in the UK? Well, for people who are performing security evaluations on a company, you can determine the building's security frequency. This kind of thing can be use to gather all sorts and can and aid you with any social engineering projects you have going and I will explain how.

Consider this, when you are listening to security for a building or area you may wish to enter you can establish the security's patrol time's any internal codes and inside talk patrol locations. You can also gather information on procedures, i.e. what there action is on shift swap. Armed with this information you can do all manner of things. You can create a false intruder alert, drawing security away from the area that you wish to enter. Alternatively if the security guard has to radio your arrival to control someone from your team can then either answer the call or jam it. The problem with this type of solution is that if the control hears your friend or team member answer the call they will instantly know something is wrong causing them to immediately become suspicious. It all seem's a little too techy and mission impossible like, but I tell you its actually great fun! Remember all these things can be bought up on a security evaluation.

There are all manner of different techniques and methods you can use radios for. Here's one I tried that worked. I tried this on my own camera system and must say was surprised when it worked. Remember, if you have a hunch or a gut feeling then act on it.

Consider this; wireless camera's also emit radio signals as well. These can fall anywhere from 900 MHz to 2.4 GHz range. With the aid of a palm top or laptop and the appropriate software you can find wireless video signals like War Driving (it's better known as War Spying). So you can evaluate camera positions and blind spot's, which is the sort of information again that can be raised during a security assessment. With the right sort of equipment you can gain all sorts of information whether it is encrypted or not (which means you be able to impose your own signal over it) this is the kind of thing that can be bought up when white hat's have been tasked to perform a security evaluation of facility's. Equipment wise you are looking for 13cm and 23cm ATV receiver and transmitters. The 13cm radio ham band actually covers 2.3 GHz to 2.5 GHz. You can also get transmitters for this band. Which with the aid of a DVR you can record footage and later play it back on the frequency with more wattage and a half decent aerial (Like a Yagi or di-pole) Just bear in mind yagi is very very directional and di-pole proved all around coverage you could even hack a satellite TV dish with a cantenna or something similar I personally use an umbrella dish or a di-pole all of these antenna's can be homebrewed you may be able to wipe the original signal out and replace it with your own again aiding your entry into the building, if you do not like the thought of purchasing these item's there are a number of website's with schematics for the 13cm ATV receiver and transmitter, personally I prefer to buy them for a number of reasons

- If they Break I can send them back and get a replacement, saves time with a o'scope and stuff
- I know it has been tested before it is released for sale therefore I know its going to work under pressure.
- Sometimes I can't be arsed to sit there and play and tweak things. I lose my temper with things really easily (Which is why most of my equipment is broken)

A few tip's for anyone visiting the UK and planning on scanning. After the appalling and cowardly attacks on the London Underground on the 7/7/2005 we in the U.K are in a heightened state of alert (And quite rightly so) below is a few tips for most of it is common sense but here they are anyway.

- Don't walk up to any official looking person, or in fact anyone with a radio and ask "What channel are you on" because people don't take to kindly to that
- If you are coming into the U.K with a scanner don't arrive with pre-programmed frequency's because scanner's will generate a lot of interest both with Customs , the Police and Special Branch (The Anti-Terrorist Branch) and they will make a note of any frequency's you may have pre-programmed.
- Be ready to be searched the Police have the powers here if you are suspected as a terrorist to hold you without detention for a period of 40 days which can be extended where needed and until they see fit to release you.
- Don't fiddle with anything like scanners in your coat pocket at official events or in tourist locations because I can almost guarantee you, you ARE being watched and you will be approached by the police and lets face it where terrorists are concerned its better to be safe than sorry. Remember also, the UK is a very small country, so that makes surveillance very, very easy.

You Have Been Warned!

A little advice. I have done this in the U.K and it might also be a good idea's for any Social Engineers to get yourself a radio amateur licence. You might think well why should I? sod the government and all that blah. Well think of it like this, if you get caught in possession of radio's and TNC's (Terminal Node Controller) and all sorts you have got a genuine reason. You are a radio ham experimenting with different ways of using your radio to the max and simply explain you are a licensed amateur and you are more than within your rights to be in possession and using the equipment. This has got me out of trouble in more than one incident I tell you and sure beats a jail sentence and a fine doesn't it? You don't have to do it, but it is an excellent way to cover your ass, it is also advisable to transmit on the Ham bands as well every now and then who knows perhaps you might even enjoy it! For more information on getting licensed go to http://www.arrl.org/.By becoming a Ham as well not only will it not raise suspicion when purchasing equipment, it also opens up equipment that is not normally available to just normal people. Remember also "illegal use" of your equipment can lead to confiscation of equipment and maybe even prosecution.

A set up at home, my EGHQ (Evil Genius Headquarters as my fiancé calls it) is in my home, I have all different manner of equipment I will list all them all here and there uses and covert aerial's. Scanning wise I have a Realistic Pro-2042 and a UBC278CLT both linked to a commercial desktop discone style antenna which provides coverage from 50 MHz-2000 MHz (not that I operate any lower than 140 MHz anyway).The 278 is there to listen to local traffic. I intend to modify it so that it has a discriminator output (for more information on discriminator output's go to http://www.discriminator.nl/index-en.html). I can then link it up to AIS software called "Ship plotter" and create real time marine radar. My Pro-2042 is basically used to monitor everything else. I do have plans to buy an Opto Trakker allowing me to decode DTMF, CTCSS (so I know the correct tones for when I plan to create a false radio message during a security assessment) it also decodes some Motorola trunking systems. In the very near future (as time and money allow) I intend to link the Pro-2042 to a computer so I can use a VOX recorder so I can listen into stuff while I have been away. I also have been writing a database in HTML and intend to run this on a small computer with a touch screen (available off of eBay for next to nothing). Using this alongside my scanners to allow me rapid access to my information, sure beats searching through thousands of print outs doesn't it?

Transmitting wise I have 2 Jingtong handheld radio's capable of transmitting 137-174 MHz and 400 to 470 MHz linked to a small dipole hidden behind a drain pipe (which aids in keeping my EGHQ secret). I also have a marine band radio but I don't use it to transmit because those frequencies are monitored by the coastguard and they have D.F (direction finding) equipment and it's more of a hobby thing anyway. Don't forget to carry with you a good amount of mobile equipment as well because lets face it who really wants to lug a car battery around with them? Remember you are a social engineer, not a criminal and there is nothing wrong with LEGITIMATE system exploration. It's when you use your knowledge for gain that you become no better than a script kiddie.

To Summarize

- Always look for bargains on eBay, at ham technical sales and retail outlets. Remember commercial products are always best because they are tested and have a warranty should they decide to stop working
- Be careful when learning i.e. if you have installed yourself into a trunk don't walk down to the place and start talking to them
- Remember 1 of Murphy's law's if it looks to good to be true it usually is so don't get cocky.
- Experiment, Experiment, Experiment by all means look for information on the net and learn it. Who knows perhaps you will discover something new.
- Be prepared to share knowledge.
- When asking questions in online groups, act dumb you will find people will provide more information if they think you are a newbie and remember, they are superior and you respect there knowledge, nothing like an inflated ego to make someone tell you all of there secrets (social engineering again).
- Keep on buying 411 cos this mag kicks ass!

For those of you who are interested I am in the process of establishing a website on geocities I only started learning code three weeks ago so you may have to bear with me. I will have one up and running with pictures, sound recording and all the other lovely things that you may or may not be interested in. Remember keep on learning, keep on discovering and keep on not getting caught also remember if it is too good to be true, it usually always is. So don't get cocky with your knowledge and don't use it for naughty things

URBAN LEGENDS, FICTITIOUS NEWS & WIKIPEDIA

By Erik Giles

There's been much talk in recent years about the power of information. Good, bad, and even humor can result from false or inaccurate use of this power. I have always been fascinated by the power of false information, which is one reason I am attracted to the business I work in (bank fraud prevention) and a reason that drives my interest in hacking, hackers, social engineering, and writing for Blacklisted!411.

Recent events got me thinking about this topic. The biggest was tragedy of the miners in West Virginia, followed by the salt rubbed in the wounds of the victims families due to false rumors and reports of their survival.

What a nightmare that must have been for those folks in West Virginia; days of anxously waiting at the church for news about your trapped loved one, then the elation of the miracle of their survival, followed by a second, possibly worse horror of finding out they truly were dead. I feel for the victims families. For posterity, I picked up a copy of the USA Today last week with a headline proclaiming the miners survival. I imagine that one day this newspaper will be remembered with the same notieriety as the 'Dewey Wins' headlines from Deweys loss to Roosevelt. To their credit, USA Today ran an apology the next day, not every news source did this.

Another recent incident of this kind was the phony article in Wikipedia, that falsely implicated a respected journalist as having a part in the assassination of one of the Kennedys. That this man had been a good friend of the Kennedy family, indeed, he was a pallbearer at Robert Kennedys funeral, made this one particularly cruel.

Another one was a recent fake 'Amber Alert' about a non-existent missing child that was forwarded to me by my sister. Snopes.com is very useful in these situations, it helped me to confirm that this Amber Alert was indeed false.

Bad News: Stop the Presses

Probably the most famous example of an erroneous news item were the various 'Dewey Wins' or 'Dewey Defeats Truman' headlines from the 1948 election. I do have a bit of sympathy here for large-scale print media that operates under deadline pressure. The time needed for production runs and a daily deadline sometimes means that a newspaper has to print the best available information they have at the time and they don't want to get scooped by the competition. The Dewey case probably caused very little real harm, apart from some consternation on the part of some Dewey fans, but that was nothing like the pain felt by those poor souls in West Virginia.

And who can forget Steve Glass's "Hack Heaven", an entirely fictitious and easily disproved story about a hacker who'd scammed the non-existent "Big Time Software Firm" called "Jukt Micronics" out of thousands of dollars. As a writer of fiction who has been working to get published, I have to admit a bit of begruding respect for Glass. I think Glass could be an excellent contributor to this magazine, for he is an expert in the field of fiction as well as social engineering. His career at The New Republic stands as one of the classic examples of social engineering of our times. Glass's ruse was so complete, he covered his tracks with fictitious web sites, copius fake reporters notes, cell phone voicemails and email messages.

And on top of all that, Glass was played by Hayden Christiansen in a move about his exploits called 'Shattered Glass'. That's pretty impressive, if you think about it. I mean, I'd be bragging quite a bit if someone made a movie about my life, casting me with the same actor who played the greatest all-time movie villian known as Darth Vader.

A close cousin to this is the intended fiction story that somehow gets misinterpreted. This is pretty rare given the rise of electronic media and the fact that most people realize that fiction appears. War of the Worlds, a fictitious account of a Martian invasion that was dramatized as a series of newscasts, is the prime example. Apparently some folks were so spooked by the story that they opened up with their rifles on local water towers, mistaking them for Martian vehicles. A more malignant version of this kind of thing are news stories intended to influence stock prices, up or down. Many people don't know that it is possible to make money on a stock. The SEC has gone so far as to create phony websites which tout a non-existent stock, as a means to create more public awareness and prevent investors from being scammed.

Urban legends & Hoaxes

When I was a kid, I fell for all manner of urban myths, from rumors about spider eggs in bubble gum, or exploding cacti, to alligators in the sewers. I think that my first encounter with urban legends was in junior high school. My friend in the 9th grade told me about some old lady in his neighborhood who'd attempted to dry out her cat by putting it in the microwave, of course killing it. To my credit, at first I didn't believe the story but he swore that it had happened in his own neighborhood and he knew which lady had done it. So I believed it. Sometime later this same friend told me about how the old lady had come home from work to find her pet Doberman was ill, apparently having ingested something, and when the vet pumped its stomach they found the fingers of a thwarted burglar. I didn't believe that either, but again he claimed the lady lived 'just down the street' so I fell for it again.

Some time later I repeated one of the stories to someone else, who informed me that it was an urban legend. At that point I realized that I had, in my own mind, ascribed the Doberman finger story and the microwaved cat story to the same old lady in my friends neighborhood, they had had merged together within my mind, back to the same old lady in my friends nighborhood. But, I was shocked most of all to realize that I had never consciously made the connection between the two incidents. And I also wondered, why had I been so gullable? I decided I had been hooked because my friend claimed to have personal knowledge of the incidents, that he knew who the old lady was and where she lived.

A more malignant story I remember from my college days was when a friend of mines father worked as a referree during a nationally televised college football game. During the game, this referee was injured. This not only greatly upset my friend who was watching it, but it got worse when someone else we know called her home and informed her that her referree father had sufferred a severe injury and would have a hard time being able to walk again. Thuis wasn't true; the injury he suffered was no picnic, but his ability to walk was never at risk. To this day I can't believe our mutual 'friend' did that.

How do Urban Legends get started?

Some urban legends are created on purpose, to harrass or embarrass someone else. According to Snopes, a high school student in Pennsylavnia was apparently angry at another for stealing his girlfriend, and created a phony email bemoaning his 'severe ostriopliosis of the liver' which caused him an 'enflamed liver' with his rivals name attached, has circulated for years and caused numerous phone calls by concerned 'good samaritans' who want to help.

Other urban legens, like the doberman finger story, the microwaved cat, and others seem to have to intended victims but they circulate anyway. How would these have gotten started? I have no idea.

I am going to purposely make an attempt to start up a new urban legend today, and all I will say is that it involves laser pointers and some other well known urban legend themes. If an urban legend associated with laser pointers and eye damage does get forwarded to you, please drop me a line at erikgiles_07@yahoo.com.

I'm really interested to see if it gets forwarded, how long it lasts (if at all), and whether or not it changes over time. If it ever makes snopes dot com I will certainly let you all know.

Links:

www.snopes.com
urbanlegends.about.com/
http://www.editorandpublisher.com/eandp/news/article_display.jsp?vnu_content_id=1001805699
http://www.pbs.org/wnet/historyofus/web13/segment5_p.html
http://college.hmco.com/history/readerscomp/rcah/html/ah_028041_1948.htm' http://en.wikipedia.org/wiki/Thomas_Dewey
http://news.com.com/2100-1023-215292.html
http://www.sec.gov/news/headlines/scamsites.htm
http://www.mcwhortle.com/ipogreenlight.htm
http://www.forbes.com/1998/05/11/otw3_print.html
http://www.cbsnews.com/stories/2003/05/07/60minutes/main552819.shtml
http://www.usatoday.com/tech/news/2005-12-11-wikipedia-apology_x.htm
www.wikipedia-watch.org
http://www.snopes.com/inboxer/medical/cancer.asp

Urban legend

Alert: Don't look through your door security peephole!

This guy Ian Restil who lived next door to Amy (my girlfriend) went last week on a business trip out of town. The plane got in late, and he checked into his hotel anxious to get some sleep before the big presentation he had to give the next morning.

At about 5:11 in to morning Ian was awakened by a knock at the door. When he looked through the peephole, he sawa flash like a cameras flashbulb, and the next thing he knew, his vision in his right eye was black. In some pain and dizziness, he went to the hotel lobby, still in his pajamas, and summoned a cab and went immediately to the emergency room.

Apparently, after being examined, the police arrived and he found out more of what had happened. It is a new and increasingly common trend. He'd been flashed directly in the eye by a laser pointer, through the peephole of his hotel room door.

The man missed the big meeting and as a result, he lost his job, including his health care benefits. His company did not care what had happened to him, they only cared that he missed his presentation. He now has severe ostriopilosis of the retina, meaning his eye is enflamed and his vision is blurred. He needs a variaiton of Lasik surgery to repair it, but due to the loss of his job and his health insurance, he cannot afford the approximate $5,000 cost.

Apparently, this has been a common occurrence in some cities, as new gang initiation rites require some new initiates to blind someone with this method. Luckily, no one has sufferred permanent vision loss but this is a real possibility.

Ian Restil wants everyone to forward this to as many people as possible, to warn them about this very real threat to their health. o.k. you guys . . . this isn't a chain letter, but a choice for all of us to help Ian save his vision, if he doesn't getthe surgery within 6 months, his blurred vision and enflamed retina will be permanent. , the american ostriopilosis society will donate 3 cents per name to his treatment and recovery plan. one guy sent this to 500 people !!!! so, i know that we can send it to at least 5 or 6. come on you guys....

1) It's a an awesome way to rack up POSITIVE karma points :)

2) just think, she could be you one day . . . and in addition there's no need to send any form of money, just your time.

So how about it? Thanks in advance!

Identity Theft: Plugging the keyhole

By: Dusk Knight

Overview

Identity theft is one of the most severe of the common crimes. It is literally assuming the identity of your victim, such as using their credit card or name to obtain something. This article will help teach you how to recognize and avoid situations that could potentially lead to your identity being stolen which can have a large negative impact on your life, from your credit history to your family. I cannot possibly go over all the ways your identity can be stolen or all the solutions for each attack, but I hopefully covered most of the more common ones and gave some simple ways to avoid them.

A simple ID theft example: The pizza parlor

One of the simplest attacks I've heard that have been successfully done is by going into a pizza parlor and acting like they are reading the menu while they are either recording all the conversations in the room on small recorder or if they have a good memory, listening to names and remembering them. This is especially done during busy times so they can chose the target and get the kind of pizza they want. They will make a note of the name of the customer and the time the pizza is to be ready. If the customer pays for the pizza and leaves the parlor until its ready the thief can leave and call the parlor 15 or 20 minutes after the pizza was supposed to be ready and tell them that he is running late. When they say that the pizza has already been picked up the thief then will make a fuss about how somebody else must have got the pizza and demand either a new pizza or a refund.

Though I know people who have accomplished this successfully I also know people who have failed. It is not a failsafe strategy and especially wont work if the parlor isn't in one of its busy times of the day, or they happen to target a frequent customer, or somebody in the parlor knows the customer they targeted.

Some examples of how thieves might get your identity and how to avoid them

The Attack: Phishing.
One of the ways that I am personally targeted frequently is through phishing. This is when the attacker either sends an email or puts up a website that mimics a company out and hopes that people don't notice the small difference and enters their personal information. I recently got an email that looked like it would have come from PayPal saying that my account had been accessed by a third party and said I needed to re-enter all of my information. The email contained a link that the link title was to PayPal's website but the actual URL was to a name that looked similar to it but was off by one letter. Because I thought the email seemed phishy I looked at the URL and knew that it was not really PayPal

Evasion:
Always verify where these emails and sites are really leading. If in doubt, forward the email to the company and ask if it is authentic. In my case an easy check if I still wasn't sure after I looked at the URL would have been to log into my PayPal account and looked for anything on there that would have said my account was on hold. I know for a fact something on my account would have flagged me.

The Attack: Dumpster Diving
Another common way people can get your identity is to go through your garbage. If you throw away a credit card, or an offer for a credit card that you get in the mail and they find it. Another thing I have found my personal information is on my check stubs from my employer. This for a time had my social security number on it until I pointed it out to the management, who pays a service to write the checks and send it out for them, and shortly after that they starred out all but the last four digits of it. So in reality there is a lot of things that people commonly throw away that contain your personal information. The thieves know it and you should watch out for it.

Evasion:
Buy a shredder. Every paper that you throw away should be shredded. I especially recommend using a

cross-cut shredder so it cuts the paper into little tiny squares that would be next to impossible to put back together. Strip cut shredders are difficult to put back together, but it's still possible if the thief puts the time into it. I have even seen people going as far as putting all of the papers that might contain personal information in their fire pit or fireplace. Though this might be a little overkill.

The Attack: Packet sniffing
Though this attack method is getting easier to avoid, it is still probably pretty easy. Especially over corporate or public networks. My classmates and I used to do this in high school to attempt to get full access to the Internet. My school had a filter that wouldn't allow us to go on inappropriate websites. By sniffing the packets that our teachers would send out when they went to access the Internet, I was easily able to obtain their password and start using it to access the Internet.

Evasion:
Avoiding this one was simple. The sniffers stopped working when the school admin caught on and upgraded to using switches in place of the hubs. Though, I believe there were still ways to do it I never really cared to find one. After all, I had a new way to get the passwords shortly after. Another way you can avoid this is to use security. A lot of sites that collect personal information use SSL (Secure Socket Layer) to encrypt your data. Try to use these sites as much as possible, I actually wont even buy from sites that don't.

The Attack: Key Logging
A Key Logger is a program or device that captures key strokes. I actually had a physical device that I attached to my keyboard that would log around 130,000 keystrokes and all I had to do is type in the password I had set and it would display all the keystrokes that occurred.

Evasion:
Don't put things you don't want people to know into a computer used by other people. You never know who might be watching you. It's very difficult to tell if your keystrokes are being watched, and I see people doing this all the time. Library computers are a hot spot for checking mail, be weary of these, you could lose your password very easily if you use one.

The Attack: Carbon Copy
Besides magnetic strip readers that stores have, they often have carbon copy machines that can take an imprint of your credit card. These work good for when the network is down or the power is out, but it would also be very easy for a restaurant waiter or waitress to use to get your credit card information. With doing this they then have your name and your credit card number and can easily use this to get money from you.

Evasion:
You can refuse to allow the waiter/waitress to walk off with your card, or you can go to a cash machine and get cash. I actually have found most restaurants at least in my area have ATM machines right in the restaurant. When I pay using my card I explain to them that I don't let it leave my sight for my safety and most of them don't mind me following them to the cash register till the transaction completes, a few of them make fun of me for it but find it irritating, but thats their problem not mine.

The Attack: Looking over your shoulder
Though I am not entirely sure how often this one is done, the idea is in my head that it is possible. I go to coffee shops all the time that people are sitting there using their laptops with their headphones on being completely oblivious to their surroundings. It would be incredibly to look over their shoulder and see what they are typing, especially if you have good vision.

Evasion:
Once again, this is one that you just need to be careful what you type when you are in a public place. This is why passwords are often starred out. But you know, credit card numbers are usually not. They should be, but they are not.

Now that you know a few of the more common attack types and some simple ways you can evade them I want to point out that the list is not complete, and there is almost always other evasion tactics you can use.

Common Mistakes

I see a lot of common mistakes. Even from people that are close to me. I once was at a bank with my girlfriend and they asked her to verify her identity by giving them her social security number, and she obediently recited it in an audible level. I really blame the bank for this honestly, because they should have handed her a piece of paper and a pen and asked her to write it down for them, and then when they were done should have either put it into a shredder so she could see it being shred or handed it back to her so she could take care of it later. Though she is also to be blamed for saying it out loud without thinking about it. Another time I was with her, and she was returning something she charged on her store credit account, and they handed her a piece of paper. I had told the clerk that she had done a good job by not making her ask for a piece of paper and just getting it for her.

I also have to point out that a somewhat related mistake to the previous one is giving out your information freely. I know somebody who got in a fender bender, and the lady didn't want to get the cops involved, and that person gave the lady that hit her her contact information. It wasn't very long before the lady had a lawsuit against her and she had to fight it in court over who owed who money.

Another mistake I sometimes see is somebody reciting a phone number and a name out loud when they are talking on the phone. Though, this isn't as bad as your social security number, this can still lead to a few problems, especially if you either give out your house number or you are the owner of your house and have your name in the phone book.

What to do if your Identity has been stolen

Social Security:
If you suspect somebody has been using your Social Security Number, you can request a copy of your Social Security statement by going to the following address and filling out the form:
https://s044a90.ssa.gov/apps6z/isss/main.html

If you find that your Social Security Number has been stolen, and as long as you have not filed for bankruptcy a new one can be given to you by using the contact information provided on http://www.ssa.gov.

Credit Cards:
Because of the Fair Credit Billing Act, you are only held liable for up to $50 for any purchase on the card that is not you. You must contact the creditor and tell them the error within 60 days of receiving the bill. You can find out how to contact the creditor by going to the creditor's website (Visa, Mastercard, etc.)

References used

Though most of this article was written off of personal experiences and memory I did use a couple of resources.

Wikipedia To help define exactly what is and isn't Identity Theft
http://en.wikipedia.org/wiki/Identity_theft
To help define exactly what is and isn't Identity Theft

Who Else Is Me
http://www.whoelseisme.com
To be accurate about what to do if your identity has been stolen

About the author

Nicholas Steele, a.k.a Dusk_Knight, has been actively into computers, security, and programming for five years, even though he has known how to use a computer since he was a lot younger. He works a side job of consulting even though he is mainly a college student and factory worker. Even the factory he works at pulls him from what he is doing to fix the computer systems from time to time.

FEASIBILITY OF AN EXHAUSTIVE SEARCH ATTACK ON THE RC5 ENCRYPTION ALGORITHM

By Rick Davis

Intro

RSA laboratories has lead the way in cryptography since its inception in the mid 1980's and their RC5 algorithm developed in 1994 helped to improve their already shining image although after a number of years the question remains of just how effective this aging system still is. Originally designed by Ronald Rivest, a professor at MIT at the time, the system was amazing and even today it stands up to all attempts to break it by using assorted mathematical tools although any code can be broken through a brute force attack, at least in theory. It is with this in mind that the following sections attempt to show the current state of the RC5 system.

A Brief Background

When discussing cryptography systems its important to understand some key terms and concepts. Basically, at the core of any encryption is some kind of mathematical system which encodes and decodes the information. The RC5 system is no different and its genius is that it is based on three components each of which utilizes only three very basic mathematical operations. The three parameters that determine the level of protection offered by the algorithm (block size, key size and number of rounds) are all variable which allows the user to set an appropriate level depending on their needs.

Understanding how the operations behind the system works is only half the issue where the other half is understanding what effect computers have in relation to the algorithm. Many types of research in the field of mathematics, of which cryptography is a part, rely heavily on a computers Random Access Memory (RAM) in order to solve problems however this type of encryption can be attacked via the brute force method with very little RAM. Of course the trade off is that a massive amount of processing power is needed.

This has both good and bad points for the code-maker and code-breakers alike. First, with a RAM intensive attack you can generally only use one computer whereas a distributed network of systems can be used where only computing power is needed. Also, systems that can apply large amounts of RAM are very costly and rare while 4Ghz computers can be bought for a couple hundred dollars.

It is also important to view the field of computers as a moving variable since progress in the field cannot be accurately predicted. For example, in the 1960's home computers were science fiction and mainframes were just moving along, in the 1980's home computers had under 10 Mhz of speed with under 64k of RAM, the 1990's saw home systems with 500Mhz CPU's and 64MB RAM and then today we are almost about to see 5Ghz CPU's (with multi-core and multi-processor systems getting popular) and RAM topping out at a whopping 2-4GB. Aside from the limits of design economic considerations also effect a major hardware purchase. Global conflicts, materials shortages and other unforeseen events all contribute to wildly fluctuating prices.

Current Search Attacks

One of the most productive attempts for the exhaustive search has been conducted by the distributed. net group. They rely upon the power of distributed computing to slowly chip away at the key space. Anyone who chooses to can simply go to their website and download a client program which runs quietly in the background of any computer and through the efforts of some 20,000 computers their system successfully cracked the 56-bit as well as the 64-bit system. Keeping in mind that these successes took 250 days and 1750 days respectively across tens of thousands of computers however it does show that this search attack is possible. The question is at what point does the key space expand faster then the level of technology and how realistic will it be at that point to commit to a brute attack. Answering these questions is vital for anyone interested in deploying the algorithm as well as those who may step beyond the confines of this particular equation.

The Current Attack

Currently the distributed.net project is working on the 72-bit challenge and it is with this challenge that we can begin to determine the feasibility of the brute attack. The first thing to keep in mind is that the project only runs until the key is found therefore its possible to find the key within the first ten percent of the keyspace, its because of this that the time of completion is misleading therefore a full view of total time required is absolutely necessary in order to gauge the strength of this algorithm.

A quick look at figure 1 and you can see the total number of keys possible for a 72-bit key is 4,722,366,482,869,645,213,696. But to really appreciate this number you have to build an estimate of just how long it takes to compute this many keys. Let's start with one standard desktop computer with a 2 Ghz CPU. In a 24 hour period this system will compute 515,396,075,520 keys on average which means that this system alone would take 9,162,596,898 days, or just over 25 million years, to search the entire keyspace. Now let's compare that to the cost of running this system. Ignoring the trivial cost of the machine itself with today's national average of about 7 cents per kilo-watt hour it costs roughly forty dollars per year to run this computer (not including a monitor) which translates to 1 billion dollars over the course of the run. Obviously in this case money is not the major issue, the more pressing matter is that it will take 25 million years to crack the code.

Now the point of the distributed computing project is to speed this up by running the data across many computers, so lets take a big jump and assume we have 10,000 computers performing the exhaustive search. All together the 10,000 computers will process 5,153,960,755,200,000 keys every 24 hours and therefore will run the entire keyspace in 916,260 days, or just over 2,500 years. Obviously that's of no use so what happens if we jump to 100,000 computers? In that case we can search the entire key space in 251 years. In fact to even approach a realistic time frame we would need TEN MILLION computers in order to run the entire keyspace in just over 2.5 years. However now that we have our time frame in the realm of possibility (but not practicality) it should be noted that to run ten million computers for two and a half years we would now need to pay the power bill of 1 billion dollars plus the cost of all the computers, monitors and the salary of what is sure to be the largest computer support team ever devised. So then we have quite the conundrum that leads to the question what can be done to shift these values in a favorable manner?

Well, using current statistics we can assume that a 3 Ghz computer can search 449,280,000,000 keys per day, while a 4 Ghz system can do as much as 829,440,000,000 per day. With this data we can replace our 2 Ghz systems in the last example with 4 Ghz systems which now means we can run the entire key space in 15 million years on one system or 1,500 years using 10,000 computers. And once again to approach a realistic time frame ten million computers can process the entire keyspace in a year and a half. In fact if we needed to search the keyspace in one year using only 10,000 computers each computer would need to process 1.3 quadrillion keys a day which is about 3.5 orders of magnitude higher that what the best 4 Ghz cpu can do today.

Is it necessary to search the entire keyspace?

For the purposes of reviewing the feasibility of the exhaustive search it must be considered however if the goal was to only crack the encryption algorithm it would only be necessary to search the keyspace until the key is found, which could be as soon as less than 1 percent or as much as within the 99th percentile. Because of this there is a certain luck factor inherent with the algorithm. Again a massive amount of funding is required for the computing power but it could be possible, with luck, to run across the correct key very early in the sequence. Data encrypted by the algorithm is secure from anyone decrypting it live, or even for several years, however if data was stolen it would only be a matter of time before the key was found if those behind the theft had enough funding, computing power and patience to locate the key.

Supercomputers and Money

What about using a supercomputer? Well to compare a supercomputer to a large array of desktops there are two main things to keep in mind, they are cost and processing speed. As we ignored the cost of storage, maintenance, power and other items for the desktops we can do the same for a supercomputer since it uses less space and maintenance but more power, in the end these extra costs even out.

Looking at supercomputers we can go right to the top of the list to the inventor and long time leader in the field, Cray systems. Cray has two supercomputers at the top of their production called the XT3 and X1E. The first has a top processing power of around 450 Gflops or roughly the power behind 110 4 Ghz desktops and its big brother has a top speed of 140 Tflops or about the power from 350 4 Ghz systems. Now although this is more than impressive under normal conditions it would still take these monsters 141,000 and 44,000 years respectively to run the keyspace and to get enough of them running at once to search the keyspace in a year or less would cost more than the current national debt. Its also worth noting that there is no pricing available for these supercomputers, you have to place a order which is completely customized in order to get an estimate, but I estimate the cost of the XT3 at 5 million dollars and that of the X1E at 20 million dollars, also once the order is placed you have anywhere from 3 months to 3 years before its built, tested, delivered, installed and ready to go.

Does that make supercomputers less cost effective? Well, that mostly depends on your resources and point of view. To get equal computing power of the XT3 it would cost around fifty thousand dollars in desktop computers which is definitely cheaper than five million dollars, but over the long run when you consider storage space, power consumption, monitors, other components and lots of support personnel the scales of practicality definitely tip towards the supercomputer.

Consumer "Supercomputers"

Today's flood of technology has changed the definition of this word over the years. Initially this term was used to describe systems with a specific purpose or a specific brand however today a supercomputer is simply one of the fastest systems in relation to its overall processing speed. Some go further and reserve this title for the top 100 processing systems although with such a limitation that list can change monthly if not faster.

With the current flood of new technology at ever decreasing prices there are two very reasonable options to owning a super system from consumer sources. First, it's easy to build a quad CPU system from off the shelf parts and 8-16 CPU systems are slowly creeping up. These systems are used as a low price option for small businesses who need file servers and such and all the parts are readily available over the internet or from local suppliers and very basic computer knowledge is needed to assemble them. The leaders in these systems are the AMD Opteron's which excel in quad configurations and keeping in mind these are 64-bit CPUs their price of around $200 per CPU is very cheap. In fact a basic quad CPU system could be built for around $2500 (retail) which would include the CPU's, Motherboard, Case, a single Hard drive and about 4GB of RAM. The other major option is known as a

"Blade Server" within the industry. This is a large box ranging in size from one foot in each dimension to a 19-inch wide rack that is 10 feet high. The box itself simply has an array of location for the blades to plug into much like a graphics card or modem plugs into a normal motherboard. The difference here is that each "blade" has one or more CPU's along with dedicated RAM and other features, all starting under $1000 each. In this configuration you could have 100's of CPUs or more running in a space no larger than a washing machine.

Of course this assumes these pieces are bought retail although anyone with a tax-ID could find them cheaper in bulk which would therefore be able to compete and most likely outperform standard home computers in the long run no to mention there would only be the need to have a single person oversee the array which would require much less space and power.

So where does this leave us? Will the Engineers beat the Mathematicians?

It would appear that there is no reasonable way to run an exhaustive search of the entire 72-bit keyspace with today's technology costs and their related computing power. The only possible light at the end of the tunnel would be if technology took a huge leap forward so that within a short time 15-20 Ghz cpu's or more were on the market at today's 2 Ghz prices and then with a large enough cash flow you could setup a very large computer array.

All of the previous examples have dealt with the assumption that the 72-bit key is the goal to beat when in fact the RC5 algorithm can extend to a 128-bit key. The jump from 72 to 128-bit increases the number of keys to search by 10^{17} (that's 17 zeros added). Using the previous examples as a bench mark that means that it would take 100,000 4-Ghz systems 11 x 10^{18} (11,000,000,000,000,000,000) years to search the entire key space. And to bring the time frame to under a year you would need 11 x 10^{23} 4-Ghz systems. It's obvious these are huge numbers that prohibit current systems from running the keyspace however the question is if new computing technology can catch up quick enough to pose a threat to the algorithm.

Using a very liberal guess of what a 10-ghz CPU might process with today's processor architecture we could assume that it would process 200 billion keys per day or the entire keyspace in 550,000 years. This does mean that about 120,000 of these could search the keyspace in one year. Of course the limit of the RC5 system running at a 128-bit key would mean that our fictional processor would need to be 10^{7} as powerful and far beyond being able to guess at its power.

Will computing power ever catch up?

With new technology and theory ever evolving and quantum computing on the horizon its inevitable that computers will continue to move ahead in leaps and bounds however within the scope of RC5 this question only applies for as long as its being used therefore we need only look to the coming 5 or 10 years along with the past in order to form a benchmark and an educated guess of the near future.

A popular guideline for computing advancements is Moore's Law. This law observed by Gordon Moore in 1965 predicts that the number of transistors per square inch would double every year. The present day values have this doubling every 18-months, or a performance increase of over 1% per week. Of course as technology increases this guideline will be less useful as design features and processing architecture makes a simple 2-D measurement of the chip useless.

Where is RSA and what is the future of the RC system?

Although corporations do not discuss their specific security measures the customer list on the RSA website shows an impressive list of clients including credit unions, airlines, banks, various manufactures and many others. Aside from these clients that use network encryption to secure their data, RSA now offers portable devices for authentication that have such a low cost and ease of use that even an end user could employ them. The bottom line is that with RSA reaching far and wide the RC5 system is still a big part and does not look like its going to let up anytime soon.

As strong as the RC5 system seems to be it is by no means the end of the line for the algorithm. In the late 1990's the RC6 system was announced and was entered into the competition for the new Advanced Encryption Standard (AES) which was to replace the older Data Encryption Standard (DES) which had been broken many times and was no longer backed by the federal government.

Conclusions

With all of this in mind the final question and the only really important one is weather it is still safe to employ the RC5 system and for those that use it or might in the future the question is would you feel safe with it protecting your data? The bottom line is that RC5 still holds a great deal of use and it is near impossible for an exhaustive search attack to be effective by anyone with the current level of technology. Anyone employing it may wish to step up to the 96-bit key or higher since operations are underway to break the lower levels although even the lower levels show great strength. Of course any system based on an equation may eventually be broken by one as well so it is important to keep an eye on the current cryptographic information for any new methods that may make the RC5 system vulnerable.

Key Size	Maximum Possible Keys
32-bit	4,294,967,296
40-bit	1,099,511,627,776
48-bit	281,474,976,710,656
56-bit	72,057,594,037,927,936
64-bit	18,446,744,073,709,551,616
72-bit	4,722,366,482,869,645,213,696
80-bit	1,208,925,819,614,629,174,706,176
88-bit	309,485,009,821,345,068,724,781,056
96-bit	79,228,162,514,264,337,593,543,950,336
104-bit	20,282,409,603,651,670,423,947,251,286,016
112-bit	5,192,296,858,534,827,628,530,496,329,220,096
120-bit	1,329,227,995,784,915,872,903,807,060,280,344,576
128-bit	340,282,366,920,938,463,463,374,607,431,768,211,456

Figure 1

NUMBER SYSTEMS

By Jewstah
Editor-In-Chief, leet magazine

Number systems define a set of values used to represent quantity. Knowledge of these systems can help in many different fields of hacking. As you probably already know it is imperative that one should know these systems to see just how data is read, stored, and transfered in computers. Here is a simple guideline to understanding these systems, easily.

Decimal system:
Base 10 system, the name originates from the word 'deca' meaning 10. This system uses ten different symbols to represent values. The set values for this system are: 0 1 2 3 4 5 6 7 8 9 . 0 having the least value and 9 having the greatest. However in the Decimal system the digit on the left has more importance than the right. When doing a calculation, if the highest digit (9) is exceeded, then you must transfer over to the next column (left column).

Example of addition exceeding the base:
8+4
8
9 +1
10 +2 (note)
11 +3
12 +4

Note: When 9 is exceeded, you must go back to the beginning of the set (0), and carry a value of 1 over to the next column (left).

Positional values:

Columns represent powers of 10, this is expressed as columns of ones (0-9), tens (groups of 10), hundreds (groups of 100) etc.

```
237 =(2 groups of 100)  + (3 groups of 10)  + (7 groups of 1)
    =(100 +100)          + (10 + 10 + 10)   + (1 + 1 + 1 + 1 + 1 + 1 + 1)
    =(200)               + (30)              + (7)
    =(237)
```

Each column move left is 10 times the value before.

Binary system:

The binary number system uses two values to represent numbers. The values are, 0 and 1 with 0 having the least value and 1 having the greatest. Columns are used in the same way as in the decimal system, the left most column is used to represent the greatest value. The values in the set (0 and 1) repeat, in both the vertical and horizontal directions.

0
1
10
11
100
101
110
111

Note: Goto value lowest in set, carry over to left.

When it comes to computers, a binary variable capable of storing a binary value (0 or 1) is called a Bit. Just as in the decimal system, columns represented multiplied values of 10 because there were 10 values (0 - 9), in the binary system, columns represent multiplication values of 2 (0 - 1).

Rules for Binary Addition:

Operation	Result
0 + 0	0
0 + 1	1
1 + 0	1
1 + 1	0 and carry 1

Rules for Binary Subtraction:

Operation	Result
0 - 0	0
0 - 1	1 and borrow 1
1 - 0	1
1 - 1	0

Rules for Binary Multiplication:

Operation	Result
0 * 0	0
0 * 1	0
1 * 0	0
1 * 1	1

Hexadecimal system:

The hexadecimal number system uses sixteen values to represent numbers. The values are, 0 1 2 3 4 5 6 7 8 9 A B C D E F with 0 having the least value and F having the greatest. Columns are used in this system like the others, the left most column is used to represent the greatest value.

0 - F, 10 -1F, 10 - 2F, 30 - 3F ....

Hexadecimal is often used to represent values (numbers and memory addresses) in computer systems.

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Converting Decimal to Binary:
Continuously divide number until it is reduced to 0. On dividing by 2, if there is a remainder of 1, the corresponding binary number is 1, however if the remainder is 0 then the binary number will be 0.

Converting Binary to Decimal:
The decimal value of a binary number is equivalent to the sum of the decimal values of the binary digits.

Converting Hexadecimal to Binary to Decimal:
The best way to convert hexadecimal into decimal is to convert it into binary first, then from there convert the binary into decimal.

Gray Code:
This is a variable weighted code and is cyclic. It is arranged so that every transition from one value to the next involves only one bit change. The gray code is sometimes referred to as reflected binary, because the first eight values compare with those of the last 8 values, but in reverse order.

Decimal	Binary	Gray
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

The gray code is often used in mechanical applications such as encoders. Modulo 1 Arithmetic. This is binary addition but the carry is ignored.

Converting Gray to Binary:
Write down the number in gray code.
The most significant bit of the binary number is the most significant bit of the gray code
Ass (using modulo 2) the next significant bit of the binary number to the next significant bit of The gray coded number to obtain the next binary bit
Repeat until all bits of the gray coded number have been added modulo 2
The resulting number is the binary equivalent of the gray number.

ASCII:
ASCII is the American Standard Code of Information Interchange, and 8 - bit code, which only consists of 1 and 0. The 8 - bit code can be broken down into two smaller parts of 4 - bits. The plain text value of an 8 - bit ASCII code is the value obtained at the intersection of the two 4 - bit values. Refer to an ASCII chart for example.

I hope this brings you to a greater understanding of just how the information in computers work. Enjoy.

DIY Keylogger

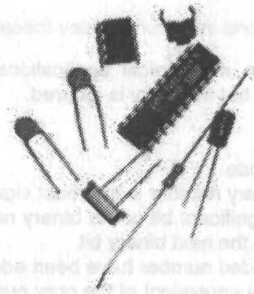
The hardware based keylogger is an excellent addition when performing physical penetration testing. The ease at which you can install them, and the fact that precautions are often not taken to prevent such an attack make them a relatively easy way to gain sensitive information. Unlike software keyloggers, which are detectable using anti-virus software and forensic analysis, hardware based keyloggers are almost completely transparent to the user. Unless the keylogger fails or the user regularly checks the back of his computer, these devices usually remain unnoticed. The following article will cover the production of your own hardware based keylogger using basic parts that can easily be acquired. If you aren't up to building your own keylogger, I would highly suggest taking a look at keelog.com. These keyloggers are cheap (Remember, many commercial keyloggers cost up to 100 USD just for a 128kb version. Keelog.com offers you 64kb, 128kb, and 256kb versions for under half the price [Based on $36.99 for the 128kb version vs. $89.99 for another 128kb commercial keylogger])

Overall I would highly recommend the people at keelog.com for any of your hardware based keylogger needs. In addition to PS2 keyloggers, they also offer keylogging modules designed to integrate into pre-existing PS2 keyboards for even greater stealth capabilities along with a new product for USB based keylogging (Which has not been released yet).

The following article is republished with permission from keelog.com. The original article can be found at http://www.keelog.com/diy.html.

Alterations have been made from the original publication

The Keylogger



What you Need

Before you start, go down this list and see if you have all the basic stuff needed to do this project on your own:

- a little bit of experience in electronics
- a soldering iron
- a microcontroller programmer supporting the Atmel 89C20XX family

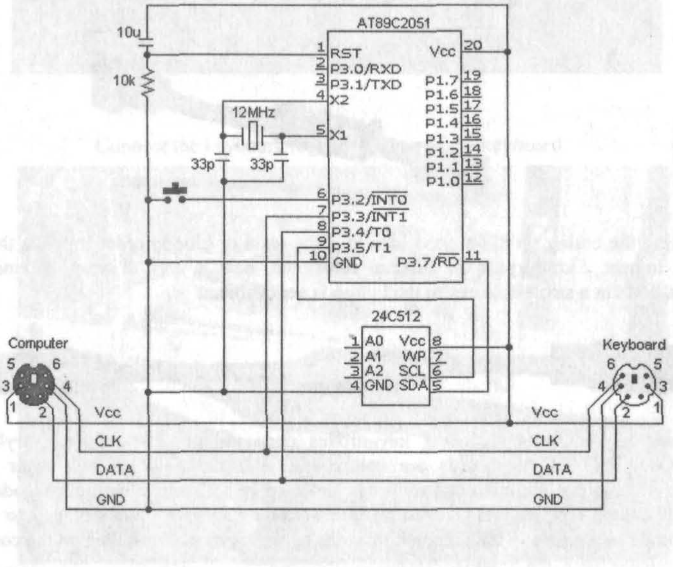
The biggest problem faced with building the device is the need for a programmer for the AT89C2051 chip. Purchasing one would probably be impractical since you will only need it once. If you know someone that has this type of programmer, you may want to borrow it or if you feel up to it, you may want to build your own (http://chaokhun.kmitl.ac.th/~kswichit/89prog/index.html). The following is a list of materials to build the keylogger:

- an Atmel AT89C2051 microcontroller (AT89C1051 or AT89C4051 will do as well)
- a 24C512 serial EEPROM chip
- a 12MHz crystal (as small as possible)
- two 33pF capacitors
- one 10uF capacitor (as small as possible)
- one 10kiloohm resistor
- a small push-button

You will also need casing for the device. A variety of materials can be used to encase the device. Materials such as heat shrink tubing and possibly even plumbing material may be used to encase the device. Be creative when finding material to encase the keylogger. The smaller less noticeable casing would probably be preferred due to the decreased likelihood of detection.

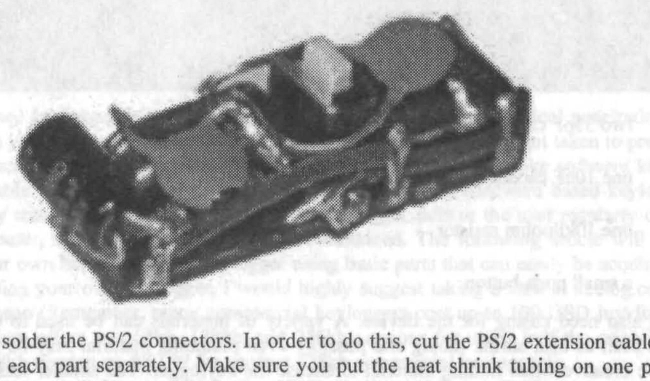
The first thing to do is program the microcontroller. The first step is to burn the AT89C2051 using the programmer you borrowed, purchased, or made. Use the following binary version (Downloadable from http://www.keelog.com/files/diy.bin) or the hex version (Downloadable from http://www.keelog.com/files/diy.hex) .You can also compile your own binary using the source code (Downloadable from http://www.keelog.com/files/diy.asm) and a 8051 compiler.

After flashing the device, you're ready for soldering. This is probably the most difficult part in the whole project since the keyboard logger should be made as small as possible. The electrical schematic below shows how connections should be made between components.

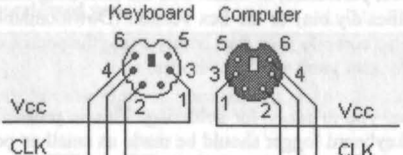


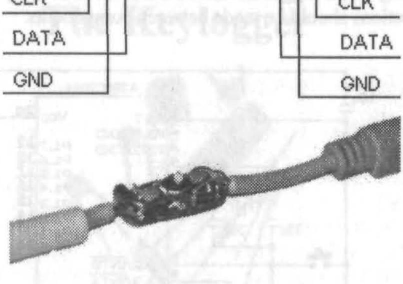
Solder the components together starting from the microcontroller and the EEPROM. Unused pins can be removed if needed. Make sure the push button is accessible and the 10uF capacitor is biased correctly (minus should be connected to pin 1).

Leave the PS/2 connectors for the end. Try to make the keyboard logger as compact as possible while avoiding short circuits since they will be very difficult to remove after the device is ready. The finished product should look somewhat like the prototype shown on the photo after the core is assembled.

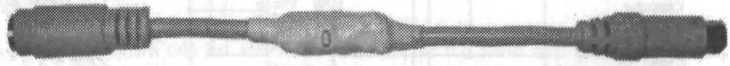


Now it is time to solder the PS/2 connectors. In order to do this, cut the PS/2 extension cable into two pieces and solder each part separately. Make sure you put the heat shrink tubing on one part of the cable. Be sure to connect all four used PS/2 pins (CLK, DATA, VCC, and GND) on both plugs (at the keyboard and at the computer).



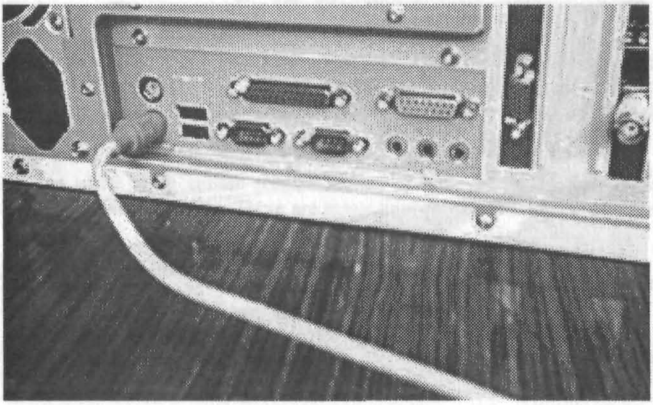


Before placing the casing on it's a good idea to place resin or glue in order to make the device more resistant to impact. Finally pull the thermal tubing on, heat it until it wraps around the soldered components, and cut a small hole out so the button is accessible.

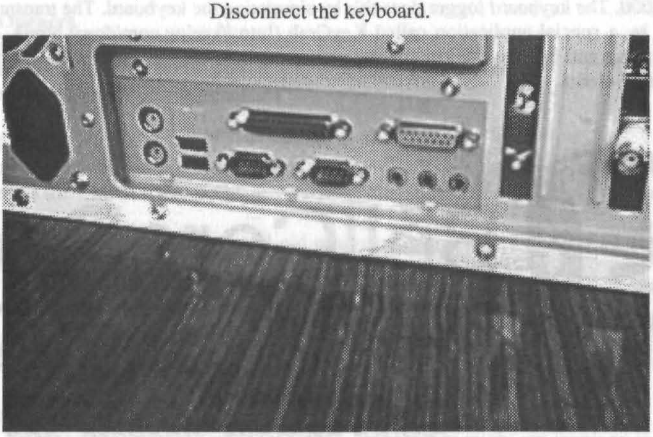


The keyboard logger starts recording key-strokes once plugged between the keyboard and the computer. Only PS2 PC keyboards are compatible with the device. The logger is completely transparent for computer operation and cannot be detected by software in recording mode. All data sent by the keyboard will be logged in internal non-volatile EEPROM memory (up to 65536 bytes). Recording mode is completely independent from the operating system installed on the computer.

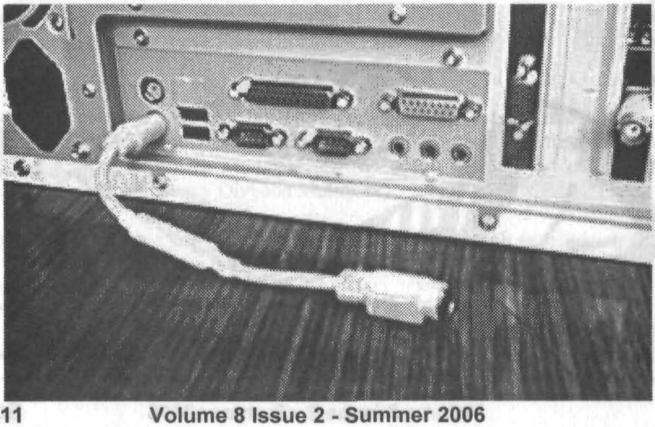
In order to install the device follow the steps listed below:
Find the PS/2 connector at the computer.



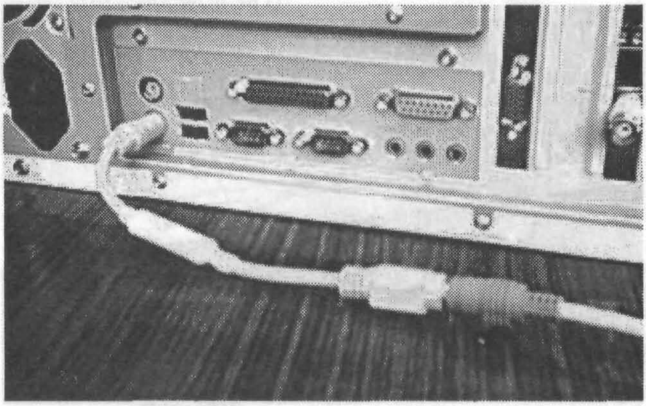
Disconnect the keyboard.



Connect the keyboard logger in place of the keyboard.



Connect the keyboard to the logger. On computer power-up data will start being recorded.



Once data has been recorded into the keyboard logger, it can be retrieved to a PC running Windows 9X/Me/XP/2000. The keyboard logger does this by simulating the keyboard. The transmitted characters are acquired by a special application called KeyGrab (http://keelog.com/down.html). After using the software to replay and capture the keystrokes, you're ready to reap all the sensitive information from the unsuspecting victim.

Listen! Part Two

By ML Shannon

Welcome back. For you who have just tuned in, in Part One, I rewrote the original article on scanning, which was called The Ear, and shortened it to include only the most useful chapters. This was followed by the first half of a long list of services, organizations that use two way radio communications that you might be able to monitor.

Please be aware that while some entries contain known or believed actual frequencies, this is not intended as a frequency guide or listing. There are many available in the Sources section at the end of this article.

Agencies come and go and change frequencies as well as bands. What listings are there are only as a convenience.

Now, the second half followed by monitoring repeater input frequencies, online Internet scanners, Data signals, near-field monitoring, the trunked radio system, and a little technical stuff on radios.

PART TWO LISTINGS

Garage Door Openers
Try 3i5, 390 and 288-418 MHz.
Interesting article about these being interfered with near some military bases:
http://www.aaaremotes.com/fccpunoforga.html

Golden Age of Radio
On some commercial broadcast and international shortwave stations, you can hear old radio programs from the thirties to the sixties. They come and go from one station to another, so they are where you find them.
If you are really interested in these wonderful old programs, you can find a list of sources on my web site www.fusionsites.com/otr

GreenPeace
Aboard their vessels at sea, amateur HF frequencies may be used; at least this once was true. Also try 151.625, 462.575, 462.600, 462.625, 464.500, 464.550.

Homeland Security
Here is an area where some serious research is needed. Perhaps you might get involved in trying to find some good frequencies. Keep in mind that there has been some re-shuffling of agencies so some that were formally independent, such as the Secret Service, are now part of DHS.

Hot Air/ helium Balloons
Wouldn't it be fascinating to hear Steve Fosset in his next adventure?

International Short-wave broadcasting
All the many stations I heard as a kid and lots more; from practically every nation on the planet. And while some are weak and fade in and out, a new system used by some of these stations solves that problem. This is called Digital Radio Mondiale (DRM) which uses a type of transmission called COFDM (Coded Orthogonal Frequency Division Multiplex).

With this system, those shortwave stations that use it can be received with excellent signal quality. You can learn about DRM here: http://www.drm.org/indexdeuz.htm, or
http://www.owdjim.gen.nz/chris/radio/DRM/

I haven't tried DRM, preferring to spin the knob on my Icom R-8500 (Very nice radio) and tune in what I can.

Law enforcement Agencies

City, County and State

In many states including California, the Hiway Patrol uses 45 MHz as their main channels. They also have VHF for comms with their aircraft and UHF for various 'MARS' (Mutual Aid Radio Systems).

In San Francisco as well as many other areas, local police also have 'Low Band' but unless they use the trunked system, they will likely be between 460.050 and 460.550 MHz.

Law enforcement Networks.

State and nationwide common channels for law enforcement, firefighters and others

If a police vehicle from one city visits another, or even a different state, they may be able to access the local radio station on CLEMARS, California Law Enforcement Mutual Radio System, or NALEMARS, the national equivalent. Now, some cities have gone to the trunked system, but they may, as does San Francisco, still maintain some of the UHF 'PIC' (Police Instant Communications) channels which include CLEMARS. Try 154.92 and 154.935 for CLEMARS and 460.025 for NALEMARS.

Local government agencies

Public works, utilities, the dogcatcher. Normally not the most exciting transmissions to monitor, but in the trunked radio system even the Mayor or District Attorney have their own 'channels'. You never know...

International Short-wave broadcasting

All the many stations I heard as a kid and lots more; from practically every nation on the planet. And while some are weak and fade in and out, a new system used by some of these stations solves that problem. This is called Digital Radio Mondiale (DRM) which uses a type of transmission called COFDM (Coded Orthogonal Frequency Division Multiplex).

With this system, those shortwave stations that use it can be received with excellent signal quality.

You can learn about DRM here: http://www.drm.org/indexdeuz.htm, or http://www.owdjim.gen.nz/chris/radio/DRM/

Local government agencies

Public works, utilities, the dogcatcher. Normally not the most exciting transmissions to monitor, but in the trunked radio system even the Mayor or District Attorney have their own 'channels'. You never know...

Marine telephone.

From 155 to 156 including Coast Guard.

M.A.R.S.

Military Affiliate Radio System

http://public.afca.af.mil/LIBRARY/MARS1.HTM: "The program consists of licensed amateur radio operators who are interested in military communications. They contribute to the MARS mission providing auxiliary or emergency communications on a local, national, and international basis as an adjunct to normal communications."

See this link for a long list of emergency frequencies including M.A.R.S. (Most are HF; shortwave) http://www.ominous-valve.com/hurricne.txt

Media and remote relay

Get the news before anyone else does! Newspaper and TV reporters tend to be very chatty; they say a great deal about what is happening, obviously, to report to the 'City Desk' or whatever. An example is later in this book.

Often around 450- 453 with repeater input 5 MHz lower. (May be unlawful to monitor)

Medical Telemetry

These will usually be very short range transmissions, within a hospital or other medical facility and are sometimes on the 2.4 GHz no-license band along with wireless 802.11 computer networking.

I might mention that if you are into wireless, that using a directional antenna and a hi-power card such as the Senao, that it is possible to interfere with medical telemetry. So please, be careful what you point your antenna at, and use RMM; Radio Monitor Mode when applicable.

Military aircraft and Facilities.
"KC-1 this is Blue Leader, we got two thirsty Tomcats here. And check the oil, will ya'. Just like in the movies. Aircraft refueling, the SAC, fighters on training missions, maybe even transmissions from those stratospheric tankers that criss-cross the sky with Chemtrails. Bob Kelty's books are an excellent source and are available at Ham Radio Outlet. Much military traffic is in the 200-300 MHz area, but virtually any frequencies might be used.

Mobile Data Terminals, Law Enforcement
Probably unlawful to monitor, and most definitely illegal to reveal any information you intercept. Someone posted MDT data on a web site. As the story goes, he was raided by the feds, his house and all electronic equipment confiscated.

Some years ago, police MDTs used simple ASCII and with a 4 level decoder, it was easy to intercept their transmissions and display on the computer screen. Since then, many agencies have changed to a secure system, allegedly encrypted with the DES. While it is true that it is possible to derive a key for DES, it takes a specially built machine that costs a couple hundred thousand dollars. So, you aren't likely to do this with a fast Pentium.

Mobile Data Terminals, Private Business
The same laws apply as to revealing what you intercept. These terminals may be easier to 'crack' but I don't have current info on how it is done. The sounds, audio clips in .wav format are available from the publisher's new web site.

MURS
Multi-Use Radio Service
Private two way short-distance voice, data, or image communications for personal or business.
151.820, 151.880, 151.940, 154.570, 154.600

National Guard
Will vary from one location to another, but some frequencies are probably shared nationwide. A few you can try: 38.450, 148.175, 148.225, 148.450, 148.550, 148.545, 149.175, 150.200, 173.5375, 173.5875, 395.100

Networks.
State and nationwide common channels for law enforcement, firefighters and others

If a police vehicle from one city visits another, or even a different state, they may be able to access the local radio station on CLEMARS, California Law Enforcement Mutual Radio System, or NALEMARS, the national equivalent. Now, some cities have gone to the trunked system, but they may, as does San Francisco, still maintain some of the UHF 'PIÇ' (Police Instant Communications) channels which include CLEMARS. Try 154.92 and 154.935 for CLEMARS and 460.025 for NALEMARS.

Newsline
The Ham radio news program. Stories about amateurs being involved in emergencies individually or through RACES; Radio Amateur Civil Emergency Service or ARES, Amateur Radio Emergency Service and other newsworthy stories about ham operators.
A list of repeaters that may still broadcast NewsLine is here
http://www.arnewsline.org/nlsurvey2000/nlrepeaters.html

NexTel Direct Connect
NexTel has a simplex feature- direct from one radio to another. I have not verified this, but apparently is it ordinary FM and so is easy to monitor. One report is that Motorola incorporated FRS frequencies into the radios. If true, not a very god idea.

NOAA
National Oceanic and Atmospheric Administration, the weather channels.
162.400, 162.425, 162.450, 162.475, 162.500, 162.525, 162.550

NORAD
North American Air Defense Command. Check this site:
http://www.abovetopsecret.com/pages/mil_freq.html

Repeaters and Input Frequencies
Most commercial two way radio systems, including trunked, use repeaters.
The signal from the radio in a police car, or the hand held radios they have, are too weak to reach other police in different areas. So, these radios transmit on an 'input' frequency (offset) that is picked up by the repeater and rebroadcast at a much higher power.

On UHF, the offset is usually 5 MHz above repeater output. One of the San Francisco Police PIC (Police Instant Communication) channel repeaters is 460.075 so the input is 465.075. With the trunked system, the offset may be 45 MHz.

Now, suppose you don't want to listen to everything that is happening all over town, you just want to know if something is happening in your neighborhood. By programming these input frequencies into a separate bank, you can do just that. It works with the trunked system, too!

OnStar
Supposedly uses cellular for voice communications. Interesting article:
http://www.windley.com/archives/2003/01/16.shtml

OSCAR
Orbiting Satellite Carrying Amateur Radio. Try 145.9738.
See also AMSAT at http://www.amsat.org/amsat-new/index.php
Also: http://science.nasa.gov/Realtime/jtrack/Amateur.html

Pagers, Voice and text
NOTE: Unlawful to monitor. Voice pagers seem to be disappearing, replaced by text messaging. Pagers are all over the spectrum; 30, 50, 150, 454, and mostly around 929.

Pirate Stations
'Micro-Broadcasting' Low Power stations legal and otherwise.
Google has current information; these stations come and go frequently.

Public Transportation
Busses, trolleys and in San Francisco, cable cars.
Often in the 470-480 MHz band.

RadioSonde Telemetry
Possibly 400 to 407 MHz as well as above 1 GHz.

Railroads, freight trains, switch-yards, Amtrak
Mostly VHF with some UHF and also data transmissions. Many web sites are devoted to railroads and monitoring. See the Blacklisted site for .wav files. Also interesting is a decoding program that could apparently be modified to read the modern police MDTs. Or so I hear.

Receiver Local Oscillators
One of the ways countermeasures experts were able to zero in on the listening post, once a surveillance transmitter, bug, was found, was to calculate the local oscillator frequency based on the bug frequency and IF. So if you are bugged, go find the spy using this technique.
The LO from car radios can be detected by roadside sensors to determine what station the driver is listening to. Sneaky, no?

Remote Monitoring Stations
Many frequencies, satellite phones, and HF, amateur bands for long range. An interesting site: http://www.dxworld.com/antarctic.html

RTTY
Radio Teletype. Mostly on HF, and require a decoder, of which there are several available.

Satellite Telephone
Iridium and Globalstar among others.

SCADA
Supervisory control and data acquisition.

Scientific Expeditions

Search & Rescue, Private

Security guards; mobile patrols and base stations.
This can sometimes be very interesting! Such personnel do not usually have the training of sworn law enforcement officers, which includes being careful what is transmitted.
In the 540 area but many agencies are moving to high UHF.

Shopping Centers and Malls

Space Shuttle, *Voice*
Sometimes rebroadcast on the 2 meter ham band.

Space Station
According to National Communications magazine (www.nat-com.org) the International Space Station can sometimes be heard on 145.8, in the ham 2 meter band.

Spy Stations
Such as the enigmatic Spanish language 'numbers' stations on short-wave. More on this in Part Three.

Online Scanners
You live in South ElMonte and you want to know what is happening in Brooklyn?

Being able to listen to a radio via computer dates back to the mid-eighties when a local electronics store set up an RBBS with an operating scanner. (Anyone remember BBSs and 300 baud?) It didn't work too well much of the time but it was an innovation. And today, there are many web sites that have online scanners that scan local police departments and other services. A Google search will find many listings, but a good way to get started is through one of the Web Rings.
http://s.webring.com/hub?ring=onlinescanners
Fascinating.

Stock Car Racing
Ever wonder what the drivers and pit crews are saying to each other? Here is a place to start: http://w8akr.dynip.com:8080/info.htm. I don't know if it is difficult to get a scanner into the stands. Another situation where the little credit card size Alinco is useful.

Studio to Transmitter Links
Microwave, or maybe the 450 - 451 MHz band the media uses for two way radios. Can get very interesting as reporters often blab stuff they perhaps should not.

Surveillance Operations
Federal agencies are likely to use 406 - 420 MHz, but any frequencies are possible. Local police use their own regular comm frequencies, but with trunked systems, any of dozens of Talk Groups.

Surveillance transmitters
The chances of intercepting a real 'bug' are not good. But it could happen. It might be an inexpensive 'toy' that some kid hid in his school, or a transmitter that was never intended for surveillance such as a baby monitor that might have a range of several blocks. Or: it might be a real spy transmitter.
Bugs can transmit on virtually any frequency. The cheap 'Spy Shop' types are likely to be on or slightly above/below the commercial FM band. Others such as Cony may be around 144.050 or 300 MHz.

An interesting trick used to hide bugs; prevent them from being found, is to transmit very close to the audio portion (Which is FM) of TV stations. A good radio, preferably a communications receiver with good selectivity much make them readable.

Taxicabs and Limos
As a former driver and dispatcher while in college, I can tell you that listening to these cabbies can get interesting. Drivers fighting over fares (passengers) and now and then being ripped off or even robbed. Some companies have duplex radios; operate through a repeater, so you can hear the cabbies yacking back and forth.

If you have a CAS system, you might hear the police investigating the incident. Interesting to hear both sides of the story!

Telephone company maintenance
I have always had more than a passing interest in telephones. Well once upon a time, many years ago, I believed that if I could find these 'secret' frequencies, I would be able to hear telco technicians tracing calls and maybe even talking about what they were hearing from the taps. Alas, no, I never heard anything 'fascinating'. Some old records list Bell Telephone Company maintenance on 151.9850, 152.6300, 152.6600 and 152.7800.

Television
No, not TV programs. TV stations in a given area don't broadcast on all of the available channels, which leaves large (6 MHz wide) slice of the spectrum unused. At one time there were government agencies that took advantage of this and set up some of their radio system within these empty channels. Tune through them carefully and you might be surprised to find some action.

Utilities
Gas, electric maintenance trucks, supervisors, base stations

Vehicle Tracking
Bumper Beepers.

Vending Machine Telemetry
These are gizmos that send out a signal when the machine needs maintenance or refilling. They do not transmit anything when they take your money but fail to deliver the product you paid for. A good hard kick is appropriate. That, they might transmit. Check

Vlink
The Vlink Personal Voice-Link System is a walkie talkie for kids.

Ch 1	916.875,	Ch 2	915.8625,	Ch 3	915.0000,	Ch 4	914.0875
Ch 5	913.3375,	Ch 6	912.0000,	Ch 7	910.9125,	Ch 8	910.2375
Ch 9	909.3375,	Ch 10	908.5000,	Ch 11	907.6625,	Ch 12	907.0000
Ch 13	906.3375,	Ch 14	905.6625,	Ch 15	904.5000,	Ch 16	904.0000
Ch 17	903.4875,	Ch 18	903.0000,	Ch 19	902.5000		

WeFax
Weather fax. Check Google- mostly HF. Requires a decoder, available from Optoelectronics.

Wildlife Animal tracking
Try 150.000-152, 160.120-161.325, 164.000-165 and 173.000-174 MHz.

Wireless Headsets
On or around 300 MHz as the military listed above, and also cordless phone frequencies. A pub across the street from where I once lived used them, and during their Halloween party, I used a modified cordless phone and broadcasted them some interesting sound effects. Howling wolves, cackling witches and the like. Some were so interesting that the club manager patched them into the music system. It was a blast!

Wireless Microphones
Here is an interesting list: http://www.rentcom.com/wpapers/telex/telex3.html

Wireless PA System input
Mostly the same as wireless microphones, but remember, you never know what you might find where.

What You Might *Not* Hear!
Signals on the airwaves may take forms other than the ordinary speech. They may be encrypted analog, digital, encrypted digital, or data. Right- digital is not necessarily encrypted.

Analog Scrambling
Let's start with encrypted analog transmissions which use Frequency Inversion. This is a method of processing an audio signal-speech- by taking the frequencies above a certain point called the baseline and substituting them or converting them to low frequencies and vice versa. The frequencies are switched or 'inverted'. Low becomes high and high becomes low. This is one of the signals you may hear on cordless telephone frequencies or certain brands of Baby Monitors.

What it sounds like
A bit like Donald Duck with a sort of metallic twang or whine. You can tell that this is Human speech and sometimes you think you can make out a word here and there. It may be possible to reconstruct this type of signal back into clear speech using another Frequency Inversion scrambler if it is the same kind; if the baseline frequency is the same and many of them do use the same one. And, there are decoding programs available on the Internet that have an adjustable base frequency.

Frequency Inversion, Variable Baseline
Also called "Rolling-Code" this is a form of Frequency Inversion scrambling in which the baseline frequency is changed many times per second. When this system was new, it sounded much the same as ordinary frequency inversion but with a loud 'knock' sound about two times per second. I haven't found a wave sample of this but if you happen to hear it you will recognize it.

Sophisticated software (Fast Fourier Series, I believe) and a powerful workstation or perhaps a supercomputer may convert some such scrambled speech back to "clear". This depends upon how often it changes. Since then, several 'levels' of FI have been developed by Transcrypt International, as well as other speech encryption systems.

Digital Transmissions

The method of converting analog speech to digital in two way radio systems is not unlike that which is used in the digital CDs you play on your stereo. Sound feeds into the front end of a circuit that opens a 'window' for a specified length of time (microseconds) where it is 'sampled' or measured. The frequency that is in the window at the time is given a digital (binary) number.

How long the window is open; the sampling rate, depends on the required frequency response. For music, the rate is much higher in order to be able to reproduce the entire range of hearing; 20 to 20,000 cycles. For two way radio, a bandwidth of 3000 cycles is sufficient so they have a 'splatter filter' that reduces or 'clips' the audio so it has a narrower bandwidth, and so the sampling rate is lower. To turn it back to sound, the process is reversed. An oversimplification but basically that's how it works.

Unencrypted Digital

This includes some cellular phones, NexTel and probably others. Digital speech sounds much like the background noise on your scanner; with the squelch open while tuned to an unused frequency.

Encrypted Digital

There are several digital encryption methods used, some more complex than others, the difference being in how secure, they are. This is based upon the 'keyspace' or length of the 'password'. None of them - as far as I know - can be converted back to normal clear speech by us hobbyists with our Pentiums.

One of the first methods used was the Data Encryption Standard; the DES, Developed by IBM years ago as 'Project Lucifer'. It used a keyspace of 56. The DES can be successfully attacked with a specially designed computer, such as the one developed by the Electronic Frontier Foundation several years ago. It cost them something like half a million dollars to build. Today, a group of hobbyists might be able to crack the DES as a joint effort, but for radio transmissions, I doubt it is being used much any more; New systems of encryption are in use by federal agencies. DVP or Digital Voice Protection is one, the military Fascinator algorithm is another, but they are secure enough that they won't be defeated for many years to come, after which the information won't be of much use to anyone.

Digital Scanners

Uniden has several scanners that can monitor some digital transmissions, such as APCO 25, used in trunking systems. But as to other digital systems such as NexTel or cell phones, and the above, not that I have heard of.

Data Transmissions

So far this article has been about voice transmissions but a great deal of what is being broadcast over the airwaves is data. Transmitting data by radio has been used since at least the days of World War II when there was wireless teletype (RTTY), and weather maps and documents were sent by 'wirephoto'. And the strange sounding signals I mentioned that you can hear on the HF bands.

In the VHF and UHF bands you will hear many data signals. Pagers such as Flex, ReFlex and Pocsag, Mobitex data terminals, police Mobile Data Terminals, Ardis, and others. Now some of these signals are not encrypted. They may use a proprietary system but some of them use plain old ASCII . Some years ago it was possible to decode police MDTs in some areas, because they used plain ASCII, but most of them have switched to a new system and I have no details on how it works.

NEAR FIELD Monitoring

This is similar to listening to input frequencies, except that there are none to program in, no banks to scan. A nearfield radio sweeps through a wide range of frequencies and locks on to the strongest signal it hears.

I started with the Optoelectronics Scout. I hear a 'beep'. It says 489.785 which I quickly punch into the ICOM R-8500, and I hear a firefighter being advised by the dispatcher that it is a false alarm, return to the Company. I look out the west window and see the ladder truck in the middle of the street, half a block away, getting ready to back into the garage. They hadn't even turned on the siren yet.

A few minutes later, it beeps again, and I punch in the numbers I see on the automatically backlighted display and hear a ham operator on 440. He is from New York, is coming off the Bayshore Freeway (US 101) and is asking if anyone is around to give him directions. I decide it is time for a break, grab my U-16 and go out on the street to assist him in finding the Hyatt at Embarcadero Center. He waves as he goes by and we decide to get together for an eyeball and some coffee after he is settled in.
Beep: A cab driver picking up at a bar down the street.
Beep: San Francisco Police are calling in a license number.

The Scout is an excellent product, but it does not demodulate the signal; it only beeps when it picks up something. But it can be interfaced to some scanners using something called Reaction Tuning. See the Opto site for details.

Now, the Xplorer, also from Opto, does have audio. And as well as displaying the frequency it has locked to, it also has a bar graph for signal strength and can decode DTMF, 'Touch-Tones'™
The Xplorer was, far as I know, the first radio of its kind, and while the one I have is very old, and subject to near constant intermod from powerful paging stations, a newer model is now available that gives the operator more control over what is received. And, Opto also has filters to restrict what is received.

Understanding wavelength and frequency
Frequency refers to the number of complete cycles of an alternating or time varying current in one second. Cycles, or Hertz per second.

This is easier to understand by seeing a sine wave on an oscilloscope display. The current flow starts at the horizontal line or 'baseline' and increases to the top of the curve, known as the peak. The current then reverses direction, flowing the other way, to the bottom of the curve, the negative peak. The measurement from the very top to the very bottom is known, logically, as peak-to-peak, usually just called PTP or 'peak'. This, then, is one cycle.

A pure signal such as Morse code transmissions, known as a carrier, would look like our sine wave here, but an AM or FM signal would be much more complicated because of the sound that is superimposed upon this carrier.

Wavelength refers to the actual physical length of a radio wave, referred to meters. Near the low end of the spectrum is AM radio which is about 550 megacycles, and here the frequency and wavelength are close to the same. Up the spectrum are international shortwave stations at 80, 40 (7 MHz) , 31, 20, 19, 15, 6 (50 MHz) and 2 (144 MHz) meter bands.

To convert one to the other:
Wavelength in meters divided into 300 yields the frequency in megahertz.

A few examples:
100 meters into 300 equals 3; that is 3 MHz.
500 meters into 300 equals 0.6 MHz, or 600 KHz; the low end of the commercial AM broadcast band.
2 meters into 300 equals 150 MHz, and etc.
An online converter is here:
http://online.unitconverterpro.com/unit-conversion/convert-alpha/frequency-wavelength.html

Intermod
There is a transmitter operating on 200 MHz and another at 300 MHz. Both are physically close together. So, out in space, the two signals 'meet' and combine which results in additional frequencies. Add 200 to 300 and you get a weak signal at 500. Subtract 200 from 300 and get another at 100 MHz. Additional signals are generated at the sum and differences of all the others; 500 plus 100, 500 minus 100 and etc. This results in dozens of these generated frequencies. Fortunately most of them are very weak but some, the first 'series' of 500 and 100 MHz are strong enough to interfere with reception of totally different frequencies.

A good example, are commercial paging systems. They have a higher output, stronger signal than most other services; a pager might use 1000 watts where a police repeater uses only 100. So the signals from the paging transmitters mix with many other signals and the result is that they can be heard in many different parts of the spectrum.

Dual conversion receivers help control this, but can not eliminate it completely, and with nearfield scanning, they become a serious problem.

The Trunked Radio System
I will use the San Francisco Police Department as an example here. Other systems may be different.
Before the trunked system went into effect a few years ago, they used conventional UHF on the 460 MHz band referred to PIC (Police Instant Communications) with which there were reception problems in certain areas. PIC consisted of about 14 frequencies, of which several were infrequently or rarely used, so most traffic was over only PIC 1,2,3,4 and 6.

Riding the cable car home from work one day, I saw a bunch of SFPD vehicles parked around the Huntington Hotel, so I hopped off and trotted over to see what was happening. It was a demonstration having to do with Pacific Gas and Electric and I stayed for a while, talking to the demonstrators and several bored looking cops.
"Uh, any chance you could tell me what Talk Group you're using"?
"Yeah, A-2."
"Thanks. I pulled out my list to see which numbers to punch in to my PRO-91 (This was before I got the PRO-95) to get A-2 and one of the cops asked, "What's that"?
I explained that it was a list of talk groups, and he asked if he could see it.
Handing it to him I mentioned that there are a lot of TGs I don't know about to which he replied with a laugh, "Hell, there's a lot of TG that WE don't know about."
There are TGs reserved for the Mayor, the District Attorney's office, emergency services and the list goes on; several hundred.

The new trunked system eliminated these problems almost completely; I talked to several SF cops, all of whom like it much better than PIC. Once they got used to it:

How it works.
The system consists of 21 or so individual frequencies which are shared by various services including police, county sheriff, parking and traffic, Department of Public Works (the people who blast you awake at 7 AM with a chorus of jackhammers) Animal Control, and others.

When someone on the system keys their radio, the computer picks up the signal and assigns it to the first available, unused, frequency. Regardless of what service it is; police or dogcatcher.
When the transmission ends, after a short delay, the frequency is clear and will be placed back in the "pool" waiting to be used by the next service that transmits.

Now, to avoid the possibility that when a police officer has an emergency situation and needs to call the dispatcher and not end up talking to the dogcatcher, the system has a number of 'channels' called Talk Groups. When a radio is set to a particular TG, it hears (and transmits) only to other radios that are tuned to, operating on, that TG. Regardless of the frequency being used.

Now, again using San Francisco as an example, the police have radios , Motorola, that can operate on any of three sets of TGs, with each set having 16 TGs. There are two rotary switches, the first labeled for the set, A, B, C, and the second numbered from 1 to 16. Total of 48 TGs.

All 16 of the A TGs are used and are assigned to particular areas of the city or for special events. So if you want to monitor the police, you have to select the TGs for your area plus some of those used for special events

As of this writing, none of the C TGs are in use and many of the B TGs are used only under special situations. One of them is to track bank robbers using the RAT system. And the raid on a suspected crack house I heard. That was interesting. Especially what I could hear in the background! Remember background sounds while monitoring.

The trunked system provides a great deal of privacy that the old PIC system did not. With at least the 32 talk groups to choose from, they can quickly select one that normally isn't used much if at all..

So, this makes it difficult for the bad guys to stay on top of what the cops are doing - they can switch to any of the 48 TG as they wish - while still making it possible for we scannists with trunking radios to know what is going on in our neighborhoods, and to be able to call in the '20' of a bad guy we happen to spot. It doesn't happen that often but one I remember was for a 211-221; a guy with a gun who car-jacked; yanked a woman out of her vehicle at a red light and stole it. I got a call from the watch commander thanking me for being an "alert citizen". Using the right trunked TGs makes it possible to stay on top of what is happening in your neighborhood.

IMAGE MANIPULATION IDENTIFICATION

Keyed by: primate

Inspiration

I was inspired to write this by StankDawg from his article in BL411 V8I1 named: "The Art of Electronic Deduction". It was a great article, one which I believe if he had the time and some help could expand into a larger publication which would include his lessons in metadata and digital forensics. His article sure was a good indepth look at basic foot printing applications for images and small bits of visual information. I understand what he is saying, and will help elaborate with some of my own ideas on image manipulation and identification. Stank, write up some more? I am sure BL411 would love a sequel as well as the readers.

Intro

There is a big deal going on about digital photography and image manipulation. Especially with the media altering images and publishing them as such. Many pictures flood the internet and media everyday, constantly being created with Adobe Photoshop or the free, open source software known as the Gimp. It is so easy, anyone can do it. All one must do is to read the free online manuals, of which there are many. I myself have created images so life like, you would think it is real. Want some blood in the picture? How about we get rid of those freckles and that glare? Let's add some piercings and tattoos.

The possibilities are endless. Your imagination is the only firewall toward artistic creation. Digital photo manipulation is not photography. The first stage, taking the picture is photography in the purest sense, but then photo manipulation goes off into the deeper realms of art. I mean not to say that photography is not an art in itself, but when you take it to the next level and actually paint on and around your picture, that my friend is even more artistic and creative. This then makes for a less real picture though, which is the predicament here. What do we do when we can not tell the difference if something is real or not? What do we do when a picture or now even video is submitted for evidence into the court room?

This is the digital age and digital media can be hacked. It can no longer be automatically accepted as truth. Images, video, and audio are all data types that we can no longer trust with just our sense of sight. We must use intuition and deduction, never seeing and believing automatically. For if we were to do so, we would create a very unholy, unreal reality for ourselves. This is what media has been since its invention, manipulation, not of only human language but now images and sound.

You may now refer to your Orwellien dictionary for the doublespeek of 'manipulation'. If you were to be framed in the court room and you are the defendant, let's say, you are going to want to get a computer programmer to take a look at the pictures integrity. They will be able to pretty much tell automatically by looking at the code and/or the pixels of the image itself if it is real, manipulated or not. Then you will be able to throw the evidence out of court or defend it to the best of your ability and truthfulness, that is, if you really are innocent.

It can go the other way too, and you can create your own evidence that the prosecuters will probably not be too happy about and have to test for integrity as well. A predicament like this reminds me of cases in court history from the 1800's and back where either of the two parties would create forged and adulterated documents making claims which backup their word as evidence. This was done simply because it was easy and no one could tell the difference, like now.

Using technology to manipulate data is liken to forging documents in the 1800's, and this is the dichotomy of the digital era as it was in the past. This digital era will not end and will always evolve as long as we humans are here and kickin'. You need to keep your eyes open and use your innate human abilities of intuition and deduction! Look at ads, newspapers, billboards, cards, signs, posters, books, magazines, and especially the internet. Rip them apart with your mind, believe nothing and keep your mind open. You will see.

Electronic Deduction

Well, Stank said it good, "Your powers of intuition and deduction should be something that you always have turned on. Think of it as the hacker's version of "spidey-sense". As the type of people who question everything and believe nothing until we have confirmed it with our own eyes, analytical skills play a huge part in most hacker's personalities. When you see anything on the internet, or anywhere else for that matter, it should always be studied and questioned." That is totally right. Think for yourself, question authority. Our powers of intuition and deduction are very powerful indeed. Most normal people of normal level intelligence use but a fraction of this power because they know not of it or are simply lazy due to being preprogrammed by culture.

We hackers are by nature self meta-programmers and can reprogram ourselves because we realize the actual programmability of the human brain. Ok fellow hackers, let us turn on our powers always. Never blink, eyes wide open, take it all in. I do not think that myself elaborating past Stanks "Art of Electronic Deduction" is necessary, for his article is expandable to all aspects of foot printing not only screenshots and small pictures, but any other type of visual information which one can gather. I do think however that he could himself elaborate more on metadata and forensics, since not all of us have this knowledge.

We do not need anymore visual foot printing examples, so let's learn how to identify those pesky manipulated photos…

Manipulation Identification

It is so easy when your brain has been trained, just look at the pixels in different resolutions. You will want to copy the image from where ever you can and open it with Photoshop or Gimp. Your not going to look at the image's code, believe is or not, you will be looking at the actual image and this is where your brain comes in, use it. Looking for fakes can not only be done on your computer with the software that probably created it, but also in print and other visual media; as long as you can get close to it or use a magnifying glass.

Zooming for Pixel Patterns

In either program you can zoom in and out. I suggest zooming all of the way out and then in to the suspected areas, again and again. Zoom in and out fast and slow too, record the whole image at every possible resolution in your brain. If you don't pick up on it being a fake by the time you are finished copying it in your head, it might just be real. If you find faults or questionable pixels, look harder. PS and Gimp both have loads of different brushes and I believe you can make your own custom brushes too.
Take a look at them, do you see any of their patterns in questionable areas? If you spot a pattern in any of the pixels, whether it be a brush or not, that is a dead give away to photo manipulation.

Check the Color Codes

If the image is black and white, it will be more difficult to tell if it was manipulated. Good luck there, it's tuff to tell because of the natural flatness of B+W. It is easy to mix and manipulate black pixels together. Yet in color, you can catch a fake easily. Zooming into the pixels and comparing visually their colors to each other through out the whole picture is one of two techs you can do. The other is to use the "eye dropper" tool in PS or Gimp. Click individual pixels and look at their color codes, compare the codes instead of just the colors to each other.
Look for patters and irregularities. Real photos have a smooth realness to them in color and tone, manipulated photos obviously do not and if anything are pixelated at those questionable spots when zoomed onto. Remember, if the photo you are looking at is doctored, the person whom did it inevitably
left tracks of their doing. Spot them at high resolutions.

Double Doc and Reverse Psych

Sometimes we can't get a copy of the original fake photo, if that isn't an oxymoron. And sometimes they are double doctored, where someone takes an already manipulated photo and either adds their own crap or tries to use reverse psychology to trick your brain into believing what you can't see. Imagine someone wants to release and get credit for a picture like the faked tourist on top of the WTC building before impact.

If they were smart, they would have create a diversion or purposely placed manipulation, like people jumping, or in windows. Look for anything to coax your mind which is obvious and would be picked out before the main manipulation (the standing person themself). The main idea is to not stop at the first manipulation you find, keep looking. Use what you previously learned in electronic foot printing deduction. Good luck!

Shouts to: StankDawg for a great concept, elwood the arcitect from europe, and mrprva77 who told me to RTFM.

The Care and Feeding of Your Amiga 3000

A well balanced diet for your Amiga will keep it strong!

By MobbyG

My first Amiga was an A500 model with only 512K ram. After some updates and tweaks, that A500 ran like a champ for many years and served me well! After some technical mishaps I had to get rid of it and upgraded to a PC machine. But I missed my Amiga days and soon decided to get a new Amiga. While trolling around in the news groups and on the web, I found someone in Massachusetts that sold Amigas second hand and had an A3000. I always wanted a higher end Amiga. So I emailed him and sent him $300 and wham! I had a stock Amiga 3000 desktop at my house in a few days.

Now since it was almost 10 years old when I got my A3000, the man, Darius, sent me a few tips on how to keep my A3000 in top form. Some of which I have also found online, and I want to share with you should you come across an A3000 and want to bring it back up to top form! One of the first things to do, is open up the A3000 and check the battery on the motherboard!

This is a NiCad 3.6v, 60mAH battery, that is soldered to the motherboard between the Paula Audio I/O and the Denise Enhanced 1280 hires chips, which are next to the system expansion bus on the motherboard. If you're looking at the mobo from the front it would be on the left hand side, and look like a small barrel, usually red, blue or green. These batteries are known to leak acid when they get older. The acid will leak down and also corrode the copper traces on your motherboard and that can lead to much more nasty things, such as your A3000 not working anymore! So care should be taken to inspect the battery and remove/replace it as soon as you can! I would suggest, replacing it even if the person you got it from says it's new. Just to be safe.

Replacement batteries are not hard to find. A quick search online and you can find a few stores that carry them. Your local electronics store should, or if your in a pinch, try "Cell" Shack...er..Radio Shack. They may have some in the back or can order it for you, but you may pay more then you would find an independent place, or try one of the advertisers here in this fine mag.

I have read of people trying to use cordless phone batteries, but you do that at your own risk. I recommend getting a proper replacement.

Removing the battery shouldn't be too difficult. Simply snip the 3 legs that hold it to the mobo if it's already leaking. You can later desolder the pegs in the holes for installation of the replacement later when you get one. To desolder it you do need to remove the motherboard from the case, and there are a lot of screws so, get a dixie cup or something to put those screws in to keep them from spilling all over the rug and dissapearing, untill your wife or girlfriend vacums the rug.

After replacing the battery, bootup and let it run for a few hours to charge up the battery. Then shutdown and reboot to check and see if the battery is helping to power the RAM keeping the settings in place as well as the clock on time.

Now what if the motherboard already has some of the acid on it? Well, clean it of course! Battery acid cleaning kits or some simple kitchen chemistry to whip up something to neutralize the acid and clean it up. Take special care or small traces and leads from componets near the battery terminal, not not break them.

Once the battery is taken care of, another trouble spot is usually the LEDs on the front. They are on a small thin board which are prone to breaking. I should know, I broke mine! Since breaking the board means breaking the trace to the LEDs, I simply took a small piece of wire from an old transistor radio that died and ran a jumper. Quick and easy.

Next thing is to check your Kickstart ROMS. This requires removing the power supply and floppy drive as well as the hard drive if it came with one. Get a seperate Dixie cup and put those screws in there to keep them safe. You'll find the ROMS just to the left of the keyboard and mouse/joystick ports. Make sure they are seated properly in the sockets. The A3000 had some heat issues and I have seen this cause the chips to "pop" out. Just simply give them a little push to make sure they are in all the way. If your particualr motherboard rev is the kind with the ROMS soldered down, then you can skip that part.

The A3000 came with v2.04 of the Kickstart. But 3.1 Roms are still regularly avaialble through Amiga dealers online and can be found on eBay as well. I suggest upgrading to 3.1 if you get an A3000 with the stock 2.04. Simply for the benefits, plus being able to upgrade the OS to 3.9.

From there we check the FAST RAM. There were 2 kinds that could be used on the A3000. ZIP and DIP. Sounds like a british comedy group I know, but that is what they were called. Now all of my experience was with ZIP ram, which basiclly are small chips, with tines like "tinfoil". Well they seemed like that to me. Bent every easily and could snap off with little or no problem. But nowadays, these are pretty cheap and you can beef up your ram quickly. Check your favorite Amiga dealer for availability and pricing. There was also a device that would sit in the ZIP slots and allow you to install SIMM memory modules. Never used this, so check with your dealer once again for info on how well these work. But, you want to check that the ZIP chips are insterted and not bent over or anything, or any have broken tines on them. If they do, a pair of needle nose pliers will get the job done for removing broken ones from slots or giving you the a little more control on straightening the tines. The ZIP ram sockets can be found on the far right of the motherboard, just below the keyboard jack.

All these things together, when done, will make sure you have many more years of happy times with your Classic Amiga 3000. If you want info on what hardware and specs of the Amiga 3000, please visit the Big Book of Amiga Hardware at *http://www.amiga-hardware.com.*

A Source List for New England Technological Enthusiasts, and Other Like-Minded Individuals

by Tom from New England <ticom@digivill.net>

Nothing beats going on a road trip in a random direction to see what interesting places are out there, especially if you are a technological enthusiast. The best is when you come across some out-of-the-way army/navy, electronic, or bookstore that you can rummage though looking for neat stuff to buy for your place. I compiled this list of places for the benefit of technological enthusiasts living in or visiting the New England area, along with comments about particular establishments that stand out.

Of course no list like this is ever complete, and in particular I have not been in upstate New York, Northern Vermont and New Hampshire, or Maine recently to check out places that might be up there. If you happen to know of a place that is not on this list, please send the information to Blacklisted! 411.

Army/Navy Stores

Military surplus type Army/Navy stores have gotten more rare in recent years as the government isn't surplusing out as much as it used to, and the rush of stuff that came from overseas in the late 1980s and early 1990s is slowing down. There are a number of mail order and Internet outlets where you can buy military surplus, but I prefer to support local businesses as much as possible. I also like to examine stuff before I make a purchase; going though bins of surplus gear looking for the one that's in the best shape.

Amherst Drop Zone
227 Russell St.
Hadley, MA 01035
413-585-5800

Army Barracks
http://www.armybarracks.com/

361 S.Broadway
Salem NH 03079
603-893-4864

328 Newbury Street
Boston, MA 02115
617-437-1657

234 Essex Street
Salem, MA 01970
978-825-1201

257 Main Street
Northampton, MA 01060
413-585-9330

Route 16
347 White Mountain Highway
Conway, NH 03818
603-447-6323

Payne Plaza
456 Payne Rd.
Scarborough, ME 04074
207-885-0680

1053 D Riverdale Street
W. Springfield, MA 01090
413-733-8300

Battle Zone
371 Boston Post Rd
Orange, CT 06477
203-795-8387

Bill's Military Surplus
81 Whiting St.
Plainville, CT 06062
(860) 410-0700
A lot of reasonably priced foreign military surplus.

The Duffle Bag
21 Front St.
Patterson, NY 12563
845-878-7106
http://www.theduffflebaginc.com/
The first Army/Navy store I visited, back in the early 1980s when it was "The Militaria Mart" in Brewster, NY.

Jamrozys War Relics
State Highway 28
Arkville, NY 12406
845-586-2265

Joey's Army/Navy Store
20 Depot St.
Watertown, CT 06795
860-274-3278

Maine Military Supply
http://www.mainemilitary.com

735 Wilson Street
Brewer, ME 04412
207-989-6783

80 Moosehead Trail
Newport, ME 04953
(207) 368-5460

Computer/Electronic/Industrial Surplus

You never know what type of interesting tech stuff you might find at these places. Generally speaking, I've had better luck overall at P&T Surplus.

P&T Surplus
198 Abeel Street
Kingston, N.Y. 12401
845-338-6191
A little out of the way, but usually worth the trip.

Pratt & Whitney Surplus
400 Main St # 1.
East Hartford, CT 06118
860-565-6850

Book Stores

The Book Barn
41 West Main Street
Niantic, Connecticut 06357
860-739-5715
http://www.bookbarnniantic.com/
Probably the best bookstore in Connecticut.

Toadstool Books
The Colony Mill Marketplace
Keene, NH 03431
603-352-8815
http://www.toadbooks.com/
Another favorite bookstore of mine. While you're at The Colony Mill Marketplace, go have something to east and drink at Elm City Brewing Co.

Eclectic

MilSurp (and Air Guns)
Route 7
Pownal, VT

Military Specialities
2543 Berlin Tpke.
Newington, CT 06111
860-666-4275

Thames Army Surplus
241 Thames St.
Groton, CT 06340
860-445-4902
A wide and eclectic variety of military surplus and collectibles.

Trash American Style
12 Mill Plain Rd.
Danbury, CT 06811
203-792-1630
http://www.trashamericanstyle.com/
"Vinyl records, CD's, cassettes, videos, books, clothes, body jewelry, posters, patches, pins, hair dye, rings, knick knacks, geegaws, bricabrac, etc etc etc. New and used. WE ARE NOT A HEAD SHOP!" I've been going here since the early 1990s when my friend Marcus told me about it. This was one of a handful of places that sold Cybertek.

Electronic Supplies/Parts

Cables & Connectors
2307 Berlin Turnpike
Newington, CT 06111
860-665-9904
http://www.cablesandconnectors.com/

"You-do-it" Electronics Center
40 Franklin Street
Needham, MA 02494
781-449-1005
http://www.youdoitelectronics.com/

Radio Communications (ham, CB, scanner) Dealers

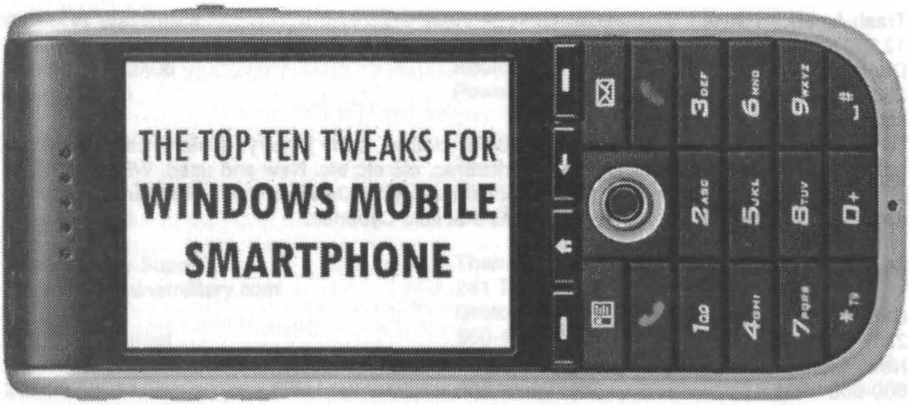
Ham Radio Outlet
224 N Broadway, Suite D12
Salem NH 03079
603-898-3750
http://www.hamradio.com/

J&S Radio Sales
1147 Main Street
Willimantic, CT 06226
860-456-2667

Lentini Communications
21 Garfield St.
Newington, CT 06111
860-666-6227
http://www.lentinicomm.com/

Rogus Electronics
250 Meriden - Waterbury Tpk.
Southington, CT 06489
Rogus deals exclusively in used radio gear, and has an eclectic stock of used electronics equipment. If I'm looking for something odd or somewhat unusual, I visit here and he often has it.

New England Area Ham - Electronic Flea Market Calendar
http://web.mit.edu/w1gsl/Public/ne-fleas
The definitive list of ham/electronic fleas for New England.



THE TOP TEN TWEAKS FOR WINDOWS MOBILE SMARTPHONE

by Unic0der
unicoder@blacklisted411.net

Maybe some of you guys still remember my article about Motorola phone modding in the Summer 05 issue of Blacklisted!411. At that time the Motorola Razr V3 was the "latest and greatest", and everybody wanted to own one (okay, not everybody, but lots of people ;-)).

This year we have a very similar situation, but this time in the area of Smartphones. Since the introduction of Microsofts Push E-Mail technology in the AKU2 service pack of Windows Mobile 5 and the introduction of the highly anticipated QWERTY Smartphone Motorola Q Windows Mobile Smartphones have become the ultimate tool for both businessmen and technology enthusiasts. But seriously, what would a phone be without some nice little hacks? Yep, just a phone, not a "smart phone". ;-) That's why I am here today to present you "The Top Ten Tweaks for Windows Mobile Smartphone" that will help you to make your kickin' Windows Mobile Smartphone even better.

Fasten your seatbelts, start your phones and let the hacking begin ...

Attention! Please note that it absolutely makes sense to write down all original settings before you do any registry changes so that you can go back to your original registry values if something does not work in a way you want it to. Please do also keep in mind that some of the tweaks (like overclocking your phone) will void your warranty and that I and the Blacklisted!411 magazine are not responsible for any data loss or damage to your phone that you might cause by applying one of the following tweaks. All modifications are done <u>at your own risk</u>.

1. Application unlock (decertify) your phone

This is what one forum poster at MoDaCo [1] called "the mother of all tweaks" and it really is, because an application unlocked phone is a precondition for many tweaks featured in this article. But before I tell you how you can easily decertify your phone you probably want to know what the so called Application lock is:

What is the Application Lock and why does it make sense to disable it?

The Application Lock is a security feature of Windows Mobile that places significant restrictions on the APIs that can be called by software. Programs that have not been signed and approved by authorities trusted by Microsoft are simply not allowed to access certain somewhat "security critical" APIs. This makes sense because that way possible phone viruses or hazardous programs cannot call premium-rate numbers on their own or delete important system files. And don't forget: Microsoft and the greedy certification authorities earn lots of money by selling these certificates as part of their Mobile2Market program. That's why most Windows Mobile Smartphones are shipped with certificate security enabled by default.
The bad thing about this situation is that certification is simply not an option for most hobbyist or open source software developers as it is a long and costly process. Therefore most programs in the Windows Mobile world are not signed and require the application unlock tweak that enables full access to all APIs and registry entries for unsigned programs.

So let's disable the friggin application lock ...

To decertify your phone the first thing you have to do is to install a certified registry editor. Pretty ironic, right? I recommend RegEditSTG [5], a modified version of the free PHM registry editor that was signed by the Windows Mobile device manufacturer HTC to help them with their ROM development. If the download link [5] does not work for you simply google for "RegEditSTG" and you will have no problems to find an alternative download location. ;-)

After you have downloaded RegEditSTG the application unlock process can ultimately start:

1. Simply put the *.zip file with RegEditSTG.exe in it with ActiveSync into a folder on your phone (but not onto the memory card).
2. Unzip the file with the *.zip program that comes with your phone.
3. Start RegEditSTG and change the following Registry Keys:
   HKEY_LOCAL_MACHINE\Security\Policies\Policies\00001001
   → Change the value data from "2" to "1"
   HKEY_LOCAL_MACHINE\Security\Policies\Policies\00001005
   → Change the value data from "16" to "40"
   HKEY_LOCAL_MACHINE\Security\Policies\Policies\00001017
   → Change the value data from "128" to "144"
   HKEY_LOCAL_MACHINE \Security\Policies\Policies
   → Add a new DWORD value "0000101b" and set the value data to "1"
4. After you have done all these steps close the registry editor and reboot your phone. That's it. Your phone is now totally application unlocked. J

Note: I know that the application lock is a security feature that makes sense when it comes to hazardous software. But as far as I know there are no viruses for Windows Mobile "in the wild" (at least at the moment) and as long as you don't install any cracked software on your phone you don't have to worry about anything. ;-)

2. Overclock the processor with OmapClock *(for all phones with a TI OMAP processor)*

You think that you're cool with your super-hyper-mega and whatnot else overclocked PC? Forget about it, you are not, because overclocking phones is the new big thing for the real freaks. ;-) And the good news is: You don't even need a soldering iron, a good set of screwdrivers or a master's degree in Computer Science to make your phone faster. All you need is a Windows Mobile Smartphone with a Texas Instruments OMAP processor (about 80% of all Windows Smartphones have one in them) and the little freeware utility OmapClock 0.2 [6].

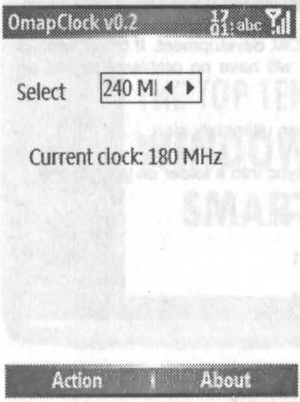
As you can see in *Fig 2.1* OmapClock 0.2 has a really simple user interface: Just select the clock rate you want your phone to run at and press "Action". That's it. If you don't like the GUI you can also control OmapClock via command line arguments (*Tab 2.1*). To create and edit shortcuts so that they can contain command line arguments I recommend the free Total Commander [7].

```
OmapClock -clock <freq> [-confirm] [-launch <path> [-restore]]

-clock <freq>
 Sets the clock rate of the processor in Mhz

-confirm
 Require acknowledgement to change the frequency

-launch <path>
 Launch a program

-restore
 Restore the original clock rate after the termination of the program
launched with "-launch <path>"
```

Tab 2.1: Command line arguments for OmapClock 0.2

Here are some examples for shortcuts with command line arguments:
"\Program Files\OmapClock\OmapClock.exe" –clock 220
"\Program Files\OmapClock\OmapClock.exe" –clock 235 –confirm
"\Program Files\OmapClock\OmapClock.exe" –clock 235 –launch "\Program Files\TCPMP\player.exe" -restore

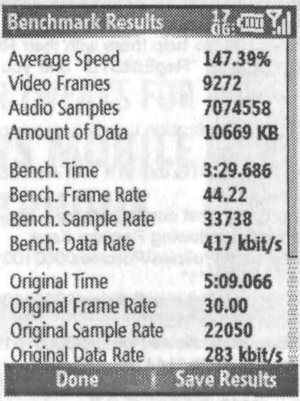
Note: Most phones processors can run up to 20% faster then specified. Keep in mind that going above these 20% may seriously damage your phone.



OmapClock v0.2

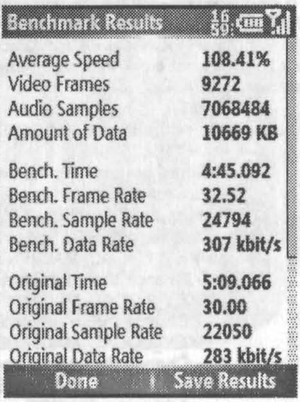
Select 240 MI ◂ ▸

Current clock: 180 MHz



Benchmark Results

Average Speed	147.39%
Video Frames	9272
Audio Samples	7074558
Amount of Data	10669 KB
Bench. Time	3:29.686
Bench. Frame Rate	44.22
Bench. Sample Rate	33738
Bench. Data Rate	417 kbit/s
Original Time	5:09.066
Original Frame Rate	30.00
Original Sample Rate	22050
Original Data Rate	283 kbit/s



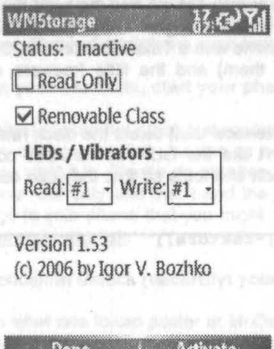
Benchmark Results

Average Speed	108.41%
Video Frames	9272
Audio Samples	7068484
Amount of Data	10669 KB
Bench. Time	4:45.092
Bench. Frame Rate	32.52
Bench. Sample Rate	24794
Bench. Data Rate	307 kbit/s
Original Time	5:09.066
Original Frame Rate	30.00
Original Sample Rate	22050
Original Data Rate	283 kbit/s

Fig 2.1 (left): The user interface of OmapClock 0.2
Fig 2.2 (middle): TCPMP [8] Benchmark running with the default 180Mhz of my phone
Fig 2.3 (right): The same benchmark with 240Mhz. Can you see the massive performance increase?

3. Use the Smartphone as Mass Storage Device *(Windows Mobile 5 only)*

Another freeware application that you don't want to miss once you had it on your Windows Mobile Smartphone is WM5torage [9]. This clever program allows you to export the flash memory card inside your Smartphone as USB Mass Storage Device – effectively turning your Smartphone into a flash card reader (*Fig 3.1, Fig 3.2*). You always had your USB Pendrive with you? Throw it into the trash can! Now you have your phone with WM5torage. ;-)



WM5torage

Status: Inactive

□ Read-Only

☑ Removable Class

LEDs / Vibrators

Read: #1 Write: #1

Version 1.53
(c) 2006 by Igor V. Bozhko

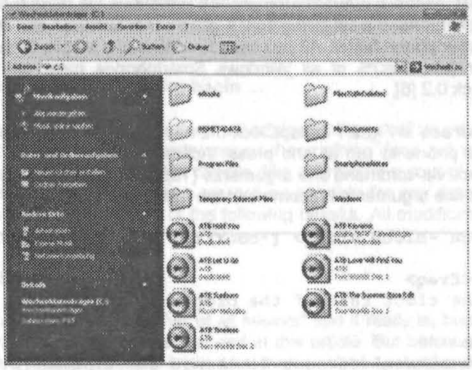


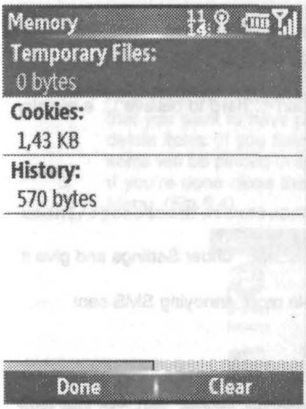
Fig 3.1 (left): WM5torage in action
Fig 3.2 (right): Access your storage card without ActiveSync just like a normal USB Pendrive

4. Store the Temporary Internet Files on your Storage Card

This tweak is my personal favorite as my phone (i-mate SP5) has built-in WiFi which makes web surfing on the phone very comfortable and useful. The only huge problem with the SP5 and most other Windows Mobile Smartphones is that they offer only a very limited amount of internal storage resulting in annoying "low storage" popup messages when the free storage space gets close to zero. Unfortunately the built-in Internet Explorer stores all Temporary Internet Files into the precious internal memory of the phone and does not allow to set a cache limit for them or to move them to the storage card where probably more free space is available. As you may guess this is a very unfortunate situation as today's websites are often several megabytes big. You can literally see how your internal memory is eaten up by the Temporary Internet Files within seconds. Let's put an end to this and let a little registry tweak rescue the situation:

To move your Temporary Internet Files to the Storage Card ...

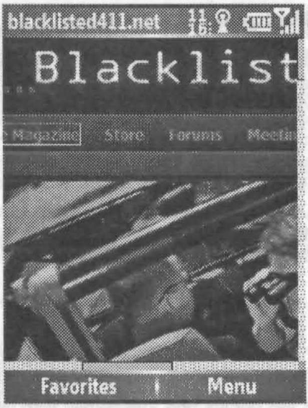
1. Start Internet Explorer (on your phone ;-)), go to "Options → Memory" and clear the Temporary Internet Files. (*Fig 4.1*) That way you make sure that nothing is left back in your internal memory.
2. Start your registry editor and navigate to the key HKEY_CURRENT_USER\Software\Microsoft \Windows\CurrentVersion\Explorer\shell Folders\Cache.
3. Replace the original value of Cache with "\Storage Card\Temporary Internet Files".
4. Close the registry editor and reboot the phone. The directory for the Temporary Internet Files will be created on the Storage Card next time you surf the web. (*Fig 4.2, Fig 4.3*)

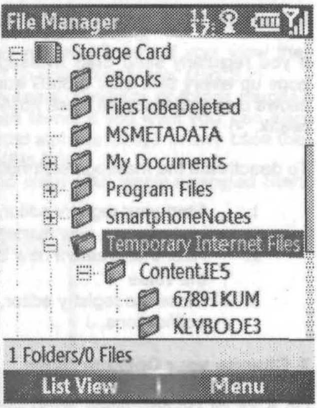

Memory

Temporary Files:
0 bytes

Cookies:
1,43 KB

History:
570 bytes




File Manager

- Storage Card
  - eBooks
  - FilesToBeDeleted
  - MSMETADATA
  - My Documents
  - Program Files
  - SmartphoneNotes
  - Temporary Internet Files
    - Content.IE5
      - 67891KUM
      - KLYBODE3

1 Folders/0 Files

Fig 4.1 (left): Don't forget to clear the Temp Files before you do the registry tweak
Fig 4.2 (middle): Visiting www.blacklisted411.net immediately after the tweak
Fig 4.3 (right): As you can see the Temporary Internet Files are now on the Storage Card

5. Enable Page Up Page Down in Internet Explorer

Another must-have registry tweak for Internet Explorer is the "Page Up Page Down" hack that allows you to map functions like "page up" or "page down" to the number keys of your phone. I think I don't have to explain how useful this is, so let's start off with the tweak without any further delay:

1. First start your preferred registry editor and navigate to `HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer`.
2. If the entry is not already there* create a new key with the name "KeyMaps".
3. For "page up" and "page down" create the following two DWORD values under KeyMaps: Add a new DWORD value "50" and set the value data to "1" (this will set key "2" to page up) Add a new DWORD value "56" and set the value data to "2" (this will set key "8" to page down)
4. But that's not all you can tweak here. You can also set a couple of other functions (*Tab 5.1*) to any number key you like (*Tab 5.2*). For example adding a new DWORD value "53" with the value data "12" will give you the ability to activate full screen mode in Internet Explorer when you press the number key 5 on your phone.
5. Last but not least close the registry editor, restart the phone and test the new key mapping.

Function	Value Data
Page Up	1
Page Down	2
Top	3
Bottom	4
Left	5
Right	6
Horizontal Top	7
Horizontal Down	8
Default Layout	9
Desktop Layout	10
One Column Layout	11
Full Screen Toggle	12
Show Pictures Toggle	13

Tab 5.1: Functions corresponding to Value Data

Key	0	1	2	3	4	5	6	7	8	9
Keycode	48	49	50	51	52	53	54	55	56	57

Tab 5.2: Keys and corresponding Keycode (DWORD) values

*Note: If you are using the latest Windows Mobile 5 version with AKU2 update you may notice that page up and page down are already set to the number keys 2 und 8 by default. Good to know that Microsoft has realized that this is a really important tweak. ;-)

6. Turn off the Message Sent Notification for SMS

If you regularly send SMS messages you are perhaps annoyed by the "Message Sent" notification that pops up every time after a SMS was successfully sent. As Microsoft has not built a control into the OS that allows one to deactivate these notifications the cure for the disease is again ... hard to believe ... a registry tweak. ;-)

To deactivate the message sent notification ...

1. Start your registry editor, navigate to `HKEY_LOCAL_MACHINE\Software\Microsoft\Inbox` and create a new key with the name "Settings".
2. After that create a new String Value with the name "`SMSNoSentMsg`" under Settings and give it the value "1".
3. Close the registry editor, reboot the phone and you will see: No more annoying SMS sent notifications. J

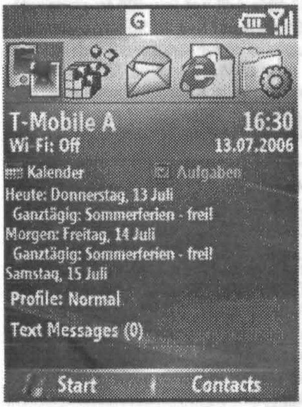
7. Change your Operator Name

On a lot of Homescreens, including the default one that comes with Windows Mobile, you can see your Operator Name displayed whenever you are logged into your cellular network (*Fig 7.1*). This fun tweak allows you to change this text (e.g. "T-Mobile A") to anything you want, like "Hack The System" (*Fig 7.3*).

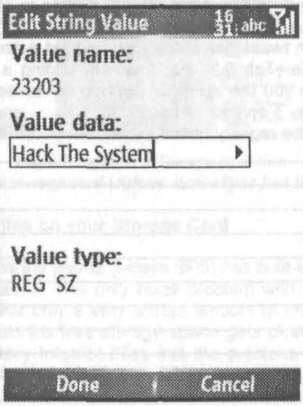
To change your Operator Name ...

1. Start your favorite registry editor and navigate yourself to `HKEY_LOCAL_MACHINE\Software \Microsoft\RIL\OperatorNames` (this is where the alternative operator names are held).
2. Then create a new value of type String. The name of this value needs to correspond to the operators number* of your cellular network (in case of T-Mobile Austria this is 23203).
3. The text you set for the value data of the newly created value will be your new operator name. (*Fig 7.2*)
4. Close the registry editor, reboot the phone and enjoy your new operator name. (*Fig 7.3*) J

*Note: If you don't know your operators number I suggest googling for it or asking your network operator.



T-Mobile A 16:30
Wi-Fi: Off 13.07.2006
Kalender Aufgaben
Heute: Donnerstag, 13 Juli
Ganztägig: Sommerferien - frei!
Morgen: Freitag, 14 Juli
Ganztägig: Sommerferien - frei!
Samstag, 15 Juli
Profile: Normal
Text Messages (0)

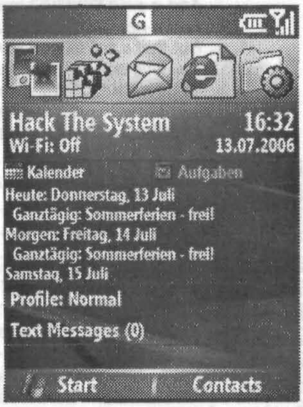


Edit String Value

Value name:
23203

Value data:
Hack The System

Value type:
REG SZ



Hack The System 16:32
Wi-Fi: Off 13.07.2006
Kalender Aufgaben
Heute: Donnerstag, 13 Juli
Ganztägig: Sommerferien - frei!
Morgen: Freitag, 14 Juli
Ganztägig: Sommerferien - frei!
Samstag, 15 Juli
Profile: Normal
Text Messages (0)

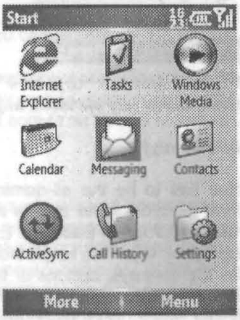
Fig 7.1 (left): My Homescreen before the tweak; Operator Name is "T-Mobile A"
Fig 7.2 (middle): This is how the tweak works ... 23203 is the Operator Number of my Cellular Network "T-Mobile Austria"
Fig 7.3 (right): My Homescreen with the new Operator Name "Hack the System"

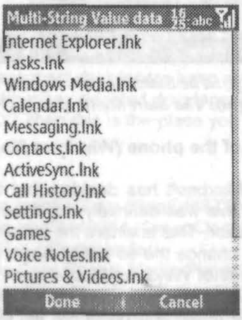
8. Change the hard-coded Start Menu order

You may have noticed that when you spark up your Start Menu a number of items are pinned to the top of it (like Internet Explorer, Tasks, Windows Media, ...) (*Fig 8.1*). Unfortunately Microsoft was not clever enough to build a function into the OS that allows one to change this predefined order of items. I know this is pretty lame, but I have good news for you: The following registry tweak lets you not only choose which items are pinned but also allows you to change the order of them.

To change your Start Menu order ...

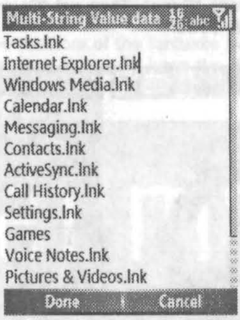
1. Start your favorite registry editor and navigate to `HKEY_CURRENT_USER\Software \Microsoft\Shell\StartMenu` where you will see a key named "Order". If you view the contents of this key, you'll see the list of items that are pinned on your Start Menu. (*Fig 8.2*)
2. Now you can change the order of all items or add your own items (shortcuts or folder names) that you want to have pinned at a specific location of the Start Menu. If you want you can also delete items (If you delete all items the start menu will be sorted alphabetically). In any case the items will be pinned in exact order you enter them in the list. (*Fig 8.3*)
3. If you're done close the registry editor, restart the phone and enjoy your newly-arranged Start Menu. (*Fig 8.4*)




Multi-String Value data

Internet Explorer.lnk
Tasks.lnk
Windows Media.lnk
Calendar.lnk
Messaging.lnk
Contacts.lnk
ActiveSync.lnk
Call History.lnk
Settings.lnk
Games
Voice Notes.lnk
Pictures & Videos.lnk

Fig 8.1 (left): The Start Menu before the tweak
Fig 8.2 (right): The hard-coded Start Menu order as shown in the registry


Multi-String Value data

Tasks.lnk
Internet Explorer.lnk
Windows Media.lnk
Calendar.lnk
Messaging.lnk
Contacts.lnk
ActiveSync.lnk
Call History.lnk
Settings.lnk
Games
Voice Notes.lnk
Pictures & Videos.lnk

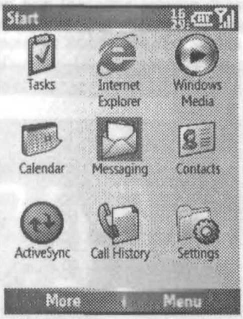


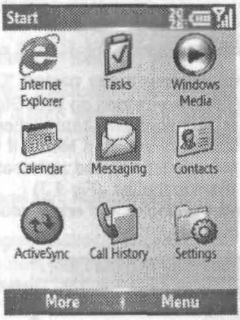
Fig 8.3 (left): Let's put Tasks on top of the list
Fig 8.4 (right): After the tweak: As you can see Tasks is now the first item in the Start Menu

9. Turn off the Grid View *(Windows Mobile 5 only)*

In Windows Mobile 5, the latest version of Microsoft's Smartphone OS, a completely new Start Menu style called "Grid View" (*Fig 9.1*) was introduced while the old sort of "list like" style was quietly discarded. To be honest I prefer the new style, but from reading hundreds of forum posts I know that there are lots of people out there who still prefer the old skool style from Windows Mobile 2002/2003. While Microsoft has again forgot to implement a user-accessible control to switch between the two styles (at least that's the case in most phones) a little registry tweak does the trick again.

To bring back the old skool style ...

1. Start your registry editor, navigate to `HKEY_CURRENT_USER\Software\Microsoft\Shell\StartMenu` and select the key "`GridView`".
2. For the original old skool style set the value of GridView to "0".
3. *To complete the tweak close the registry editor and reboot your phone.* (*Fig 9.2*) (Note: To revert to the Grid View style redo the whole procedure and set GridView to "1")



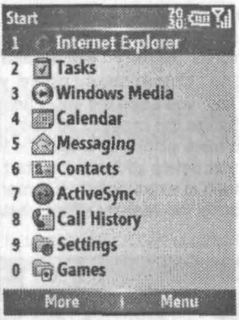
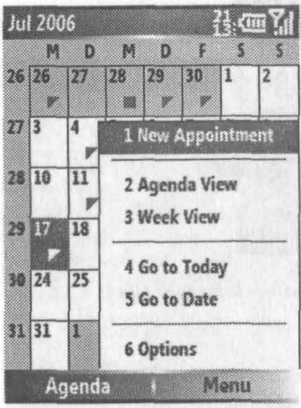


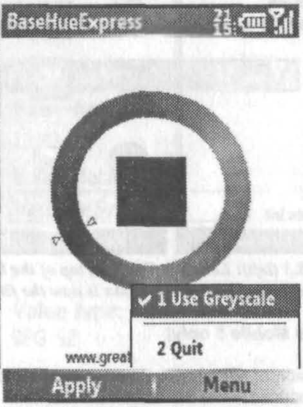
Fig 9.1 (left): The Start Menu in default Windows Mobile 5 "Grid View" style
Fig 9.2 (right): The Start Menu after the tweak. Looks very old skool, hugh? ;-)

10. Change the BaseHue of the phone *(Windows Mobile 5 only)*

Just like in Windows XP Microsoft has decided that blue has to be the all-dominant color in Windows Mobile 5 (*Fig 10.1*). While this was definitely not the worst decision some people may still want to use a more unobtrusive system color. This is where the little freeware program BaseHue Express [10] comes into play that allows its user to chance the so called BaseHue of the OS. This single hue value has impact on most user interface elements of Windows Mobile such as the softkeys, buttons or the taskbar. To change this hue go on and run BaseHue Express on your device, choose a color from the color wheel (there is also an own wheel for greyscale hues) and press the left softkey "Apply" (*Fig 10.2*). And booooom, the magic will happen and all colors affected by the BaseHue will be automatically changed. (*Fig 10.3*) J

Hint: To restore the original system color go to "Settings → Home Screen", set "Color Scheme" to "Guava Bubbles" (or any other available color scheme) and press "Done". Then set "Color Scheme" to "Default" and press "Done" once again. Voila, back is your blue Windows.





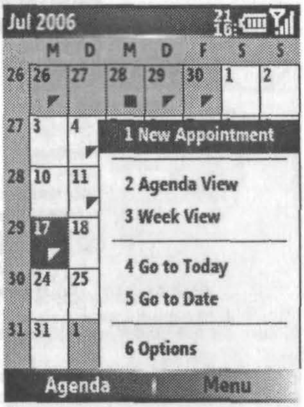


Fig 10.1 (left): The Calendar in standard colors
Fig 10.2 (middle): The Interface of BaseHue Express; (Greyscale is beautiful ;-))
Fig 10.3 (right): The Calendar after the tweak in a smooth all-greyscale style

Final words

As you can see Windows Mobile Smartphones are very tweakable due to the fact that they have a system registry just like your Desktop Windows. And due to their affinity to Pocket PCs some of the tweaks featured in this article do even work on Pocket PCs (notably tweak 1, 2, 3 and 10). Pretty cool, hugh?

And you know what? There are still hundreds of more tweaks out there, many of them for specific Smartphones like the Motorola Q. You just have to find them. ;-) Therefore I have - to make things a little bit easier for you - compiled a small list with the biggest Windows Mobile communities where you can find all these other hacks and get help if something does not work in a way you want it to. But that's not the only place where you can get technical support:

If you have any further questions regarding this article or Windows Mobile in general don't hesitate to send me a mail (unicoder@blacklisted411.net) or post your questions into the "Article Discussion" section of the Blacklisted!411 forums.

Happy hacking!

Windows Mobile communities around the globe

[1] www.modaco.com (Probably the biggest and most active Windows Mobile community in the net)
[2] www.xda-developers.com (The place where most developers hang out)
[3] www.airfagev.com (A pinoy community with many devoted developers)
[4] www.qusers.com (You have a Motorola Q? Then this is the place you have to go...)

Links

[5] http://www.spv-developers.com/content/regeditSTG.zip (RegEditSTG)
[6] http://forum.xda-developers.com/viewtopic.php?t=40284 (OmapClock)
[7] http://www.ghisler.com/smartphone.htm (Total Commander)
[8] http://tcpmp.corecodec.org/ (TCPMP / The Core Pocket Media Player)
[9] http://www.modaco.com/index.php?automodule=downloads&showfile=1702 (WM5torage)
[10] http://greatbal.blogspot.com/2006/04/basehue-express-for-wm5-devices.html (BaseHue Express)

Shouts

Special thanks go to all folks who found these nice registry tweaks, especially to all the friendly guys over at MoDaCo.com and to the creators of the fantastic freeware apps featured in this article, notably Intruders, Igor V. Bozhko and Greatbal. You guys keep the Windows Mobile community alive and kickin'! J And to Steve Ballmer and Bill Gates: Thanks for creating Windows Mobile. ;-)

The Black Market

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

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

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 I'm 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

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

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.

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.

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.

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

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.

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.

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

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

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

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

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

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.

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

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.

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

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.

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

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

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.

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.

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

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

ADD A CONVERSATIONAL USER INTERFACE to your web site or Windows-based software applications with Foxee™, the friendly interactive arctic blue fox agent character! In the real world not everyone who navigates your web site or software are expert hackers, and some users need a little help. Foxee is a hand-drawn animated cartoon character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports 10 spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information for Foxee at www.foxee.net!

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."

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.

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!

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

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

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!

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

Extreme Pizza - 14141 Jeffrey Road, 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

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

Florida

(407 Area Code) - Orlando

The computer room in the Grand Reserve Apts. at Maitland Park

Last Friday of the month, 12:00pm - 1:30pm

Hosted by: Whisper

Georgia

(678/770/404 Area Codes) - Duluth

Meetings are the first and third Tuesday of every month, in the cafe of Frys Electronics. They start at 6:30 until we get kicked out, and then continue elsewhere. Visit our site at *www.HackDuluth.org and sign up on the forums to receive* emails about the group.

Hosted by: P(?)NYB(?)Y

Illinois

(217 Area Code) - Urbana

Espresso Royale Caffe. 1117 W. Oregon St., Urbana, IL 61801. At the corner of Goodwin and Oregon, across the street from the Krannert Center for the Performing Arts. Every second Friday of the month, 8 PM

Hosted by: r3tic3nt (r3tic3nt@gmail.com)

Iowa

(515 Area Code) - Ames

ISU Memorial Union Food Court by the payphone. First Friday of each month, from 5:00pm onward.

Hosted by: Omikron

Minnesota

(612 Area Code) - Minneapolis

Spyhouse coffee shot at the corner of 25th South and Nicollet Ave. Look for the Blacklisted! 411 magz on the table.

Last Friday of the month, 5:00pm - 8:00pm

Hosted by: Thea DeSilva

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

Texas

(713 Area Code) - Houston

In front of Rocfish on Westheimer/Kirkwood. Last Sunday of every month, 7:00pm till close.

Hosted by: MuertoChongo

(915/325 Area Codes) - Blackwell

John's Detectors, 501 W. Main St. Third Friday of every month. 7:00pm until...? For more information, visit our site at www.johnsdetectors.com

Hosted by: Wirechief

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

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

Start up your own meeting and enjoy the benefits! Contact us right away!!

meetings@blacklisted411.net

History Of Blacklisted 411

Started as one of the first disk based hacker magazines in 1983, Blacklisted! 411 has evolved into one of the most widely distributed hacker magazines to date. Since its creation, the staff at Blacklisted! 411 have strived to publish original and controversial articles on a variety of subjects. With the beginning of 2006, Blacklisted! 411 will present new ideas and concepts for the entertainment and education of the security/hacking community. Shown below are some cover shots of past issues ranging from 1994 to 2005.

Blacklisted! 411
The Official Hackers Magazine!
After 6 years, we're finally BACK!
The premier issue of Blacklisted! 411

1994

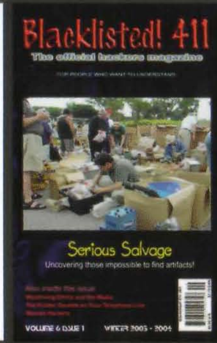
Blacklisted! 411
The Official Hackers Magazine!
Uh, not so "Secret" Air Base?
What is he doing in there?

1995

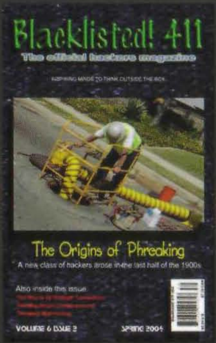
1996

1997

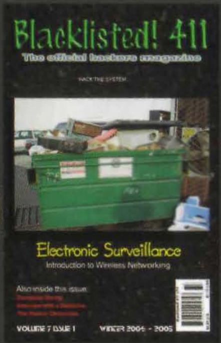
1998


Blacklisted! 411
The official hackers magazine
Serious Salvage
Uncovering those impossible to find artifacts!
VOLUME 6 ISSUE 1
WINTER 2003 - 2004

2003



2004



2005

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