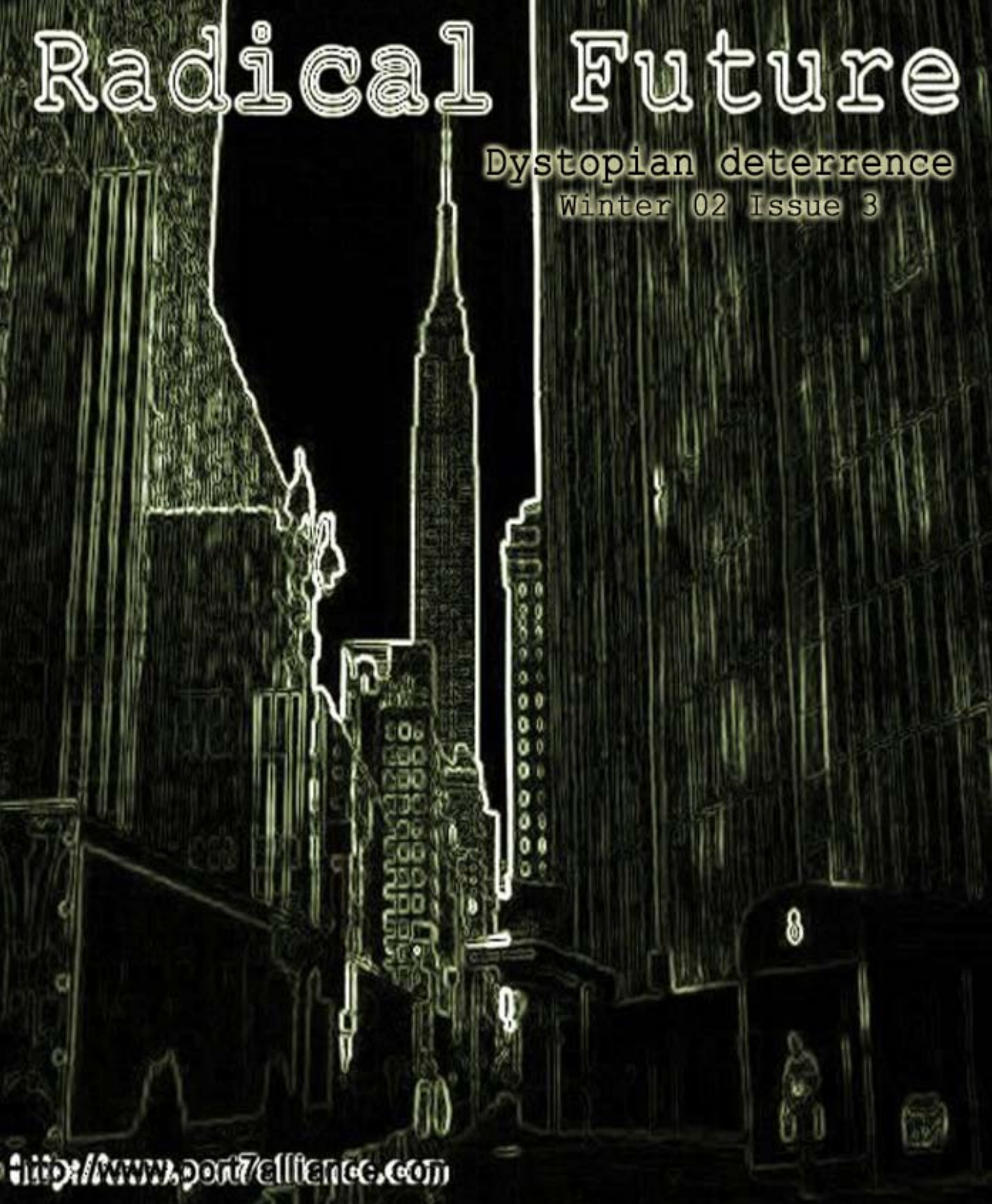
Radical Future

Dystopian deterrence

Winter 02 Issue 3



http://www.port7alliance.com

Senior Editor
Epiphany

Writers
Anthony George, DATA_Noise, J0hny Lightning, Khaos, KiLLer, Scramble45, Silence, StankDawg, TimScott, Token, Undetected

Front Cover Created By
Scramble45

Layout Designer & Graphic Artist
Epiphany, Scramble45

Special Thanks To
Kem and Data from **www.usystems.tk,** Nick84 from **www.rootsecure.net**, StankDawg from **www.stankdawg.com** and Radio Freek America **www.oldskoolphreak.com**

Radical Future is a production of Port7Alliance.com. This magazine focuses on computer hacking, and the freedom of speech, expression, and press when it comes to political beliefs and events. We try to cover a broad range opinions but we like to focus on opinions that are not normally heard in the mass media. This magazine will remain neutral at all times and respect different opinions. Radical Future targets the younger generation as to is produced by this generation. This publication is truly for the intellectual that lies in us all. If you believe in what we are trying to do, please offer your support at www.port7alliance.com.

—==+++All information contained within this magazine is for educational purposes only. We cannot be held responsible for any damages you may incur upon yourself or others.+++==—

Fallen Data...

Protecting Yourself

Written By Epiphany

In the wake of fascist legislation such as the Homeland Security Act I felt an article dedicated to Encryption and wiretaps would be suitable for this issue of RF. You may call me paranoid by the time you finish this article but I believe that in times such as these paranoid techniques should be exercised religiously. That is of course if you value your own privacy.

With wiretapping being exercised more and more by government agencies the first thing you should be careful of is what you discuss on the phone. After all it was the conversations of hacking that allowed for the conviction of Phiber Optik. (Phrack#45 file 9) And this I point out can happen to many of us, therefore I implore youth take your privacy seriously. If you need to contact someone via the phone system many sites such as www.spyshop.com sell audio scramblers and descramblers which can effectively defeat many phone taps. However one does not need to be so drastic as software such as pgpfone (www.pgp.com) allows encrypted conversations to take place over the internet.

If you use any of the major instant messenger services (aim, msn, yahoo) your conversations are logged and can be handed over to authorities if necessary. We have seen this happen to the infamous DDOS attacker MafiaBoy and whose aim logs have even been published in the book "The Hacker Diaries" by Dan Verton. So not even your "chatting" is private. However Trillian (www.trillian.cc) is a program that allows all the major IM services to be access simultaneously, however the reason I mention trillian is because it offers an option called "secureIm" for AIM and ICQ. "SecureIm" enables 128-bit tunneling encryption to be used in a chat as long as both users have trillian and the SecureIm option enabled.

It goes without saying that email should be encrypted (typically with Pretty Good Privacy www.pgp.com). I am pretty sure you have heard of the FBI's carnivore and if you have not go to www.google.com and search for information on it. If you want to take email encryption to a higher level you can use stenography which is the hiding of information in pictures or sound files. So it is possible to send your buddy a simple picture which they can decrypt at home and receive the true message. If you are really paranoid you can use Stenography and PGP so if anyone manages to crack your PGP encryption they still need to crack the picture or sound.

You must also know that you should be wary of what programs you install on your system (mainly windows not *nix) as spyware is an increasing epidemic on the internet. Ad-Aware from www.lavasoft.de is an excellent software that scans your system for spyware such as Gator as well as AD producing software. I am also going to add that if you use Kazaa for downloads immeditaly switch to Kazaa lite as it does not contain the spyware that Kazaa contains (crap like Bonza Buddy).

Slowing moving back to my wiretapping topic the best way to protect yourself from it is to learn how it is done. The simplest type of wiretapping device is a beige box which just a modular jack with alligator clips. Information on devices such as these can be found on numerous phreaking sites however this article sums it up well (phrack#3 file 5).

On a final note encryption is your friend. Encrypt everything, your computer, your phone, even yourself (disguises work well). Maybe I am paranoid but at least I can say that I still have my privacy, unlike the average person.

```
 0: 49 66 20 79 6F 75 27 72-65 20 6E 6F 74 20 63 61
10: 72 65 66 75 6C 20 74 68-65 20 6D 65 64 69 61 20
20: 77 69 6C 6C 20 68 61 76-65 20 79 6F 75 20 68 61
30: 74 69 6E 67 20 74 68 65-20 70 65 6F 70 6C 65 20
40: 77 68 6F 20 61 72 65 20-62 65 69 6E 67 20 6F 70
50: 70 72 65 73 73 65 64 2C-20 61 6E 64 20 6C 6F 76
60: 69 6E 67 20 74 68 65 20-70 65 6F 70 6C 65 20 77
70: 68 6F 20 61 72 65 20 64-6F 69 6E 67 20 74 68 65
80: 20 6F 70 70 72 65 73 73-69 6E 67 2E 0D 0A
```

audex and meridian vms

Written By TimScott
djscott@icrossroads.com

This file is not intended to show young punks how to phreak vmb's. Rather, it is intended to educate young punks in how the Meridian orAudex Mail VMB system works, should they ever want to be a Meridian or Audex Mail administraitor. Dont blame me if you get caught.

Meridian Mail Voice Mail Systems: How-To
++++++++++++++++++++++++++++++++++

Meridian VMB's are easy enough to find. They are one of the more commenly used VMB's, and you kan skan some quick numbers to find some. once you find a VMB, you will hear a greeting, and usually in there you will hear the ever-lovely recorded lady voice on the other end say something along the lines of:

"If you already have a mailb0xen on this system, please press pound (#) ".

This is wonderful, and if for some reason you dont hear this message, press pound anyways. Next step: Picking a box to hack.

If you are going to hack a box, first you have to find a box. Try some numbers, try a bunch of random numbers, look around on the system to see if they list any numbers anywhere so you can get an idea of what range the system holds its boxes on. After you have found and decided on a box to hack, you can return to the main menu and press pound, so that you can login.

First, you will be prompted for the mailbox number that you wish to hack. Enter it, and you must press pound after. Then try some of these passwords:

1111#
2222#
1234#
9999#
keypad patterns (ex 2-5-8-0)#
mailbox number#
any repeating number combination#

You have to press pound after you enter the password. Expect only three tries to get the correct pass, after three you'll probably be booted. If you dont get booted, it might be worth your while to try brute-forcing.

If at first you dont succeed, try another mailbox. There are bound to be mailb0xen that have mailboxname = pass or some stupid thing like that. Try some more b0X3n till you get an easy one.

Once youre in, here are the options:

[-Voice Messaging; Commands/Options-]

Main Commands	Playback Options
1 - Skip Backward	1 - Decrease Speed
2 - Play	2 - Increase Speed
3 - Skip Forward	3 - [Not in use]
4 - Previous Message	4 - [Not in use]
5 - Record	5 - [Not in use]
6 - Next Message	6 - [Not in use]
7 - Message Commands	7 - [Not in use]
8 - Mailbox Commands	8 - [Not in use]
9 - Call Sender	9 - [Not in use]
* - Help	* - [Not in use]
0 - Attendant Thru Dial	0 - [Not in use]
# - Stop/Exit	# - [Not in use]

Message Commands	Message Options
1 - Reply	1 - Urgent
2 - Play Envelope	2 - Standard
3 - Forward	3 - Economy
4 - Reply All	4 - Private
5 - Compose	5 - Acknowledge
6 - Delete/Restore	6 - Timed Delivery
7 - [Not in use]	7 - [Not in use]
8 - [Not in use]	8 - [Not in use]
9 - Send	9 - [Not in use]
* - Message Help	* - [Not in use]
0 - [Not in use]	0 - [Not in use]
# - [Not in use]	# - [Not in use]

Mailbox Commands	Mailbox Greetings
1 - Log In	1 - External Greeting
2 - Greetings	2 - Internal Greeting
3 - Log Off	3 - Temporary Greeting
4 - Password Change	4 - [Not in use]
5 - Distribution Lists	5 - [Not in use]
6 - Go to a Message	6 - [Not in use]
7 - [Not in use]	7 - [Not in use]
8 - [Not in use]	8 - [Not in use]
9 - Personal Verification	9 - [Not in use]
* - Mailbox Help	* - Greeting Help
0 - Mailbox Options	0 - [Not in use]
# - Cancel/Exit	# - Cancel/Exit

Mailbox Options

1 - Change Operator
2 - Remote Notification
3 - [Not in use]
4 - [Not in use]
5 - [Not in use]
6 - [Not in use]
7 - [Not in use]
8 - [Not in use]
9 - [Not in use]
* - Options Help
0 - [Not in use]
- Cancel/Exit

Tons of options, ya right.

Misc Notes:

Many Meridian mail systems will keep a record of what messages were deleted, even after you actually delete the message it will stay for a while. This is a risk if the owner of the box comes back and finds a whole bunch of deleted messages on file. Be aware.

If you dial up an INWATS number and you find a message there saying something like:

"Hello, This is Dave Thompson with Wendy's Burgur Factoree, please leave a message at the tone..."

Then you can usually get to the log in prompt by pressing * * 8 1. If not, maybe try * * and then waut to hear what the messages say. Also, sometimes * 8 1 after the tone to start recording is played will cancel the message.

Audex Mail Voice Mail Systems: How-To

++++++++++++++++++++++++++++++++++++

Alright. This would be edition two in the VMB phreaking text series. Cool. Anyways, if you want to 0wn some Audex mailboxes, first you have to skan some. Look around on the 'net for some skans, then you can move onto step two.

if you are wanting to know how to be sure that the mail system you have found is really an Audex mail system, just dial it up. If you are greeted with a banner such as "Welcome to Audex", or "Welcome to the Audex Voice Mail System", then you know the systems is Audex. If you dont hear either of these, but you want to still be sure if the system is Audex, have no phear, there are other ways.

Now, the ever elusive password prompt. Once you have found the password prompt you can set about guessing passwords and accounts. This isnt a tutorial on how to guess accounts and passwords,

but often there is a company directory that is found within the VMB that will help you find some extensions and guess some passwords.

Anyways, once you have guessed a password, and logged in, here are the options:

```
-0-0-0-0-0-
Audex VMB System
-0-0-0-0-0-
```

(The pound key will either go back or exit in most situations, even if not marked.)
(Items marked with a * have a submenu.)

```
[main menu]
[1 - Message Menu   * ]
[2 - Send A Message * ]
[3 - Change Options * ]
[# - Exit           * ]
```

```
[Message Menu]
[1 - Listen to New Messages   * ]
[2 - Listen to Saved Messages * ]
[3 - Exit (back)        ]
```

[Send Message]
If you select this option, it will first prompt you for a box number, and then you can send your message to the box number. Once you have entered the box (extension) number that you wish your message to be sent to, you can continue.

```
[1 - Send Message Options        * ]
[2 - Replay Message                ]
[3 - Re-Record Message             ]
[4 - Cancel Message                ]
[5 - Remote Notification Options * ]
[6 - Send Bulk Mail                ]
[7 - Resume Recording              ]
[8 - Playback End of Message       ]
[9 - Send at a Later Date          ]
```

```
[Send Message Options]
[1 - Normal Priority       ]
[2 - Urgent Priority       ]
[3 - Private Priority      ]
[4 - Notify When Received  ]
```

```
[Listen To New Messages]
[1 - Replay Current Message        ]
[2 - Save and Hear Next Message    ]
[3 - Save Current Message as New   ]
[4 - Delete Current Message        ]
[5 - Volume Adjust                 ]
[6 - Other Options               * ]
[# - Exit                          ]
```

```
[Other Options]
[1 - Forward                          ]
[2 - Replay                           ]
[3 - Speak With Sender                ]
[4 - Delete Current Message           ]
[5 - Hear Time and Date of Message    ]
[# - Exit                             ]
```

```
[Change Options]
[1 - Record Name                        ]
[2 - Record Greeting                    ]
[3 - Change Pasword                     ]
[4 - Change Call Transfer Feature       ]
[5 - Call Notification Options          ]
[6 - Pager Features                     ]
[7 - Review Messages Already Sent       ]
[8 - Personal Distribution Lists        ]
[* - Retreive Sent Messages             ]
```

Well, I hope this has enlightened you to some of the options that are available with the Audex VMB system. If you dont know what to do then you can read this file and get ideas.

If anyone has some additional info they would like to inform me of about Meridian or Audex Mail systems, mail me.

djscott@icrossroads.com
Thanks.

Kevin Mitnick's Banned Chapter From "The Art Of Deception"

By Kevin Mitnick
www.freekevin.com

I was reluctant to write this section because I was sure it would sound self-serving. Well, okay, it is self-serving. But I've been contacted by literally hundreds of people who want to know "who is Kevin Mitnick?". For those who don't give a damn, please turn to Chapter 2. For everybody else, here, for what it's worth, is my story.

Kevin Speaks Some hackers destroy people's files or entire bard drives; they're called crackers or vandals. Some novice hackers don't bother learning the technology, but simply download hacker tools to break into computer systems; they're called script kiddies. More experienced hackers with programming skills develop hacker programs and post them to the Web and to bulletin board systems. And then there are individuals who have no interest in the technology, but use the computer merely as a tool to aid them in stealing money, goods, or services. Despite the media-created myth of Kevin Mitnick, I'm not a malicious hacker. What I did wasn't even against the law when I began, but became a crime after new legislation was passed. I continued anyway, and was caught. My treatment by the federal government was based not on the crimes, but on making an example of me. I did not deserve to be treated like a terrorist or violent criminal: Having my residence searched with a blank search warrant; being thrown into solitary for months; denied the fundamental Constitutional rights guaranteed to anyone accused of a crime; being denied not only bail but a bail hearing; and being forced to spend years fighting to obtain the government's evidence so my court appointed attorney could prepare my defense.

What about my right to a speedy trial? For years I was given a choice every six months: sign a paper waiving your Constitutional right to a speedy trial or go to trial with an attorney who is unprepared; I chose to sign. But I'm getting ahead of my story. Starting Out my path was probably set early in life. I was a happy-go-lucky kid, but bored. After my father split when I was three, my mother worked as a waitress to support us. To see me then an only child being raised by a mother who put in long, harried days on a sometimes-erratic schedule would have been to see a youngster on his own almost all his waking hours. I was my own babysitter. Growing up in a San Fernando Valley community gave me the whole of Los Angeles to explore, and by the age of twelve I had discovered a way to travel free throughout the whole greater L.A. area. I realized one day while riding the bus that the security of the bus transfer I had purchased relied on the unusual pattern of the paper-punch that the drivers used to mark day, time and route on the transfer slips. A friendly driver, answering my carefully-planted question, told me where to buy that special type of punch. The transfers are meant to let you change buses and continue a journey to your destination, but I worked out how to use them to travel anywhere I wanted to go for free. Obtaining blank transfers was a walk in the park: the trash bins at the bus terminals were always filled with only-partly-used books of transfers that the drivers tossed away at the end of their shifts. With a pad of blanks and the punch, I could mark my own transfers and travel anywhere that L.A. buses went. Before long, I had all but memorized the bus schedules of the entire system. This was an early example of my surprising memory for certain types of information; still, today I can remember phone numbers, passwords and other items as far back as my childhood. Another personal interest that surfaced at an early age was my fascination with performing magic. Once I learned how a new trick worked, I would practice, practice, and practice until I mastered it. To an extent, it was through magic that I discovered the enjoyment in fooling people. From Phone Phreak, to Hacker my first encounter with what I would eventually learn to call social engineering came about during my high school years, when I met another student who was caught up in a hobby called phone phreaking. Phone phreaking is a type of hacking that allows you to explore the telephone network by exploiting the phone systems and phone company employees. He showed me neat tricks he could do with a telephone, like obtaining any information the phone company had on any customer, and using a secret test number to make long-distances calls for free actually free only to us—I found out much later that it wasn't a secret test number at all: the calls were in fact being billed to some poor company's MCI account). That was my introduction to social engineering-my kindergarten, so to speak. He and another phone phreaker I met shortly thereafter let me listen in as they each made pretext calls to the phone company. I heard the things they said that made them sound believable, I learned about different phone company offices, lingo and procedures. But that "training" didn't last long; it didn't have to. Soon I was doing it all on my own, learning as I went, doing it even better than those first teachers. The course my life would follow for the next fifteen years had been set.

One of my all-time favorite pranks was gaining unauthorized access to the telephone switch and changing the class of service of a fellow phone phreak. When he'd attempt to make a call from home, he'd get a message telling him to deposit a dime, because the telephone company switch received input that indicated he was calling from a pay phone.

I became absorbed in everything about telephones-not only the electronics, switches, and computers; but also the corporate organization, the procedures, and the terminology. After a while, I probably knew more about the phone system than any single employee.

And, I had developed my social engineering skills to the point that, at seventeen years old, I was able to talk most Telco employees into almost anything, whether I was speaking with them in person or by telephone. My hacking career started when I was in high school. Back then we used the term hacker to mean a person who spent

a great deal of time tinkering with hardware and software, either to develop more efficient programs or to bypass unnecessary steps and get the job done more quickly. The term has now become a pejorative, carrying the meaning of "malicious criminal." In these pages I use the term the way I have always used it in its earlier, more benign sense. In late 1979, a group of fellow hacker types who worked for the Los Angeles Unified School District dared me to try hacking into The Ark, the computer system at Digital Equipment Corporation used for developing their RSTS/E operating system software. I wanted to be accepted by the guys in this hacker group so I could pick their brains to learn more about operating systems. These new "friends" had managed to get their hands on the dial-up number to the DEC computer system. But they knew the dial-up number wouldn't do me any good: Without an account name and password, I'd never be able to get in. They were about to find out that when you underestimate others, it can come back to bite you in the butt. It turned out that, for me, even at that young age, hacking into the DEC system was a pushover. Claiming to be Anton Chernoff, one of the project's lead developers, I placed a simple phone call to the system manager. I claimed I couldn't log into one of "my" accounts, and was convincing enough to talk the guy into giving me accessing and allowing me to select a password of my choice. As an extra level of protection, whenever anyone dialed into the development system, the user also had to provide a dial-up password. The system administrator told me the password. It was "buffoon," which I guess described what he must have felt like later on, when lie found out what had happened. In less than five minutes, I had gained access to Digital's RSTE/E development system. And I wasn't logged on as just as an ordinary user, but as someone with all the privileges of a system developer. At first my new, so-called friends refused to believe I had gained access to The Ark. One of them dialed up the system and shoved the keyboard in front of me with a challenging look on his face. His mouth dropped open as I matter-of-factly logged into a privileged account. I found out later that they went off to another location and, the same day, started downloading source-code components of the DEC operating system. And then it was my turn to be floored. After they had downloaded all the software they wanted, they called the corporate security department at DEC and told them someone had hacked into the company's corporate network. And they gave my name. My so-called friends first used my access to copy highly sensitive source code, and then turned me in.

There was a lesson here, but not one I managed to learn easily.

Through the years to come, I would repeatedly get into trouble because I trusted people who I thought were my friends. After high school I studied computers at the Computer Learning Center in Los Angeles.

Within a few months, the school's computer manager realized I had found a vulnerability in the operating system and gained full administrative privileges on their IBM minicomputer. The best computer experts on their teaching staff couldn't figure out how I had done this. In what may have been one of the earliest examples of "hire the hacker," I was given an offer I couldn't refuse: Do an honors project to enhance the school's computer security, or face suspension for for hacking the system. Of course I chose to do the honors project, and ended up graduating Cum Laude with Honors. Becoming a Social Engineer some people get out of bed each morning dreading their daily work routine at the proverbial salt mines. I've been lucky enough to enjoy my work. In particular you can't imagine the challenge, reward, and pleasure I had in the time I spent as a private investigator. I was honing my talents in the performance art called social engineering-getting people to do things they wouldn't ordinarily do for a stranger-and being paid for it. For me it wasn't difficult becoming proficient in social engineering. My father's side of the family had been in the sales field for generations, so the art of influence and persuasion might have been an inherited trait. When you combine an inclination for deceiving people with the talents of influence and persuasion you arrive at the profile of a social engineer. You might say there are two specialties within the job classification of con artist. Somebody who swindles and cheats people out of their money belongs to one sub-specialty, the grifter. Somebody who uses deception, influence, and persuasion against businesses, usually targeting their information, belongs to the other sub-specialty, the social engineer. From the time of my bus transfer trick, when I was too young to know there was anything wrong with what I was doing, I had begun to recognize a talent for finding out the secrets I wasn't supposed to have. I built on that talent by using deception, knowing the lingo, and developing a well-honed skill of manipulation. One way I used to work on developing the skills in my craft (if I may call it a craft) was to pick out some piece of information I didn't really care about and see if I could talk somebody on the other end of the phone into providing it, just to improve my talents. In the same way I used to practice my magic tricks, I practiced pretexting. Through these rehearsals, I soon found I could acquire virtually any information I targeted. In Congressional testimony before Senators Lieberman and Thompson years later, I told them, "I have gained unauthorized access to computer systems at some of the largest corporations on the planet, and have successfully penetrated some of the most resilient computer systems ever developed. I have used both technical and non-technical means to obtain the source code to various operating systems and telecommunications devices to study their vulnerabilities and their inner workings." All of this was really to satisfy my own curiosity, see what I could do, and find out secret information about operating systems, cell phones, and anything else that stirred my curiosity. The train of events that would change my life started when I became the subject of a July 4th, 1994 front-page, above-the-fold story in the New York Times. Overnight, that one story turned my image from a little known nuisance of a hacker into Public Enemy Number One of cyberspace.

John Markoff, the Media's grifter

"Combining technical wizardry with the ages-old guile of a grifter, Kevin Mitnick is a computer programmer run amok." (The New York Times, 7/4/94.) Combining the ages-old desire to attain undeserved fortune with the power to publish false and defamatory stories about his subjects on the front page of the New York Times, John Markoff was truly a technology reporter run amok. Markoff was to earn himself over $1 million by single-handedly creating what I label "The Myth of

Kevin Mitnick." He became very wealthy through the very same technique I used to compromise computer systems and networks around the world: deception. In this case however, the victim of the deception wasn't a single computer user or system administrator, it was every person who trusted the news stories published in the pages of the New York Times.

Cyberspace's Most Wanted Markoff's Times article was clearly designed to land a contract for a book about my life story. I've never met Markoff, and yet he has literally become a millionaire through his libelous and defamatory "reporting" about me in the Times and in his 1991 book, Cyberpunk. In his article, he included some dozens of allegations about me that he stated as fact without citing his sources, and that even a minimal process of fact-checking (which I thought all first-rate newspapers required their reporters to do) would have revealed as being untrue or unproven. In that single false and defamatory article, Markoff labeled me as "cyberspace's most wanted," and as "one of the nation's most wanted computer criminals," without justification, reason, or supporting evidence, using no more discretion than a writer for a supermarket tabloid. In his slanderous article, Markoff falsely claimed that I had wiretapped the FBI (I hadn't); that I had broken into the computers at NORAD (which aren't even connected to any network on the outside); and that I was a computer "vandal," despite the fact that I had never intentionally damaged any computer I ever accessed. These, among other outrageous allegations, were completely false and designed to create a sense of fear about my capabilities. In yet another breach of journalistic ethics, Markoff failed to disclose in that article and in all of his subsequent articles-a pre-existing relationship with me, a personal animosity based on my having refused to participate in the book Cyberpunk In addition, I had cost him a bundle of potential revenue by refusing to renew an option for a movie based on the book. Markoff's article was also clearly designed to taunt America's law enforcement agencies. "...Law enforcement," Markoff wrote, "cannot seem to catch up with him...." The article was deliberately framed to cast me as cyberspace's Public Enemy Number One in order to influence the Department of Justice to elevate the priority of my case. A few months later, Markoff and his cohort Tsutomu Shimomura would both participate as de facto government agents in my arrest, in violation of both federal law and journalistic ethics. Both would be nearby when three blank warrants were used in an illegal search of my residence, and be present at my arrest. And, during their investigation of my activities, the two would also violate federal law by intercepting a personal telephone call of mine. While making me out to be a villain, Markoff, in a subsequent article, set up Shimomura as the number one hero of cyberspace. Again he was violating journalistic ethics by not disclosing a preexisting relationship: this hero in fact had been a personal friend of Markoff's for years. My first encounter with Markoff had come in the late eighties when he and his wife Katie Hafner contacted me while they were in the process of writing Cyberpunk, which was to be the story of three hackers: a German kid known as Pengo, Robert Morris, and myself.

What would my compensation be for participating? Nothing. I couldn't see the point of giving them my story if they would profit from it and I wouldn't, so I refused to help. Markoff gave me an ultimatum: either interview with us or anything we hear from any source will be accepted as the truth. He was clearly frustrated and annoyed that I would not cooperate, and was letting me know he had the means to make me regret it. I chose to stand my ground and would not cooperate despite his pressure tactics. When published, the book portrayed me as "The Darkside Hacker." I concluded that the authors had intentionally included unsupported, false statements in order to get back at me for not cooperating with them. By making my character appear more sinister and casting me in a false light, they probably increased the sales of the book. A movie producer phoned with great news: Hollywood was interested in making a movie about the Darkside Hacker depicted in Cyberpunk. I pointed out that the story was full of inaccuracies and untruths about me, but he was still very excited about the project. I accepted $5,000 for a two-year option, against an additional $45,000 if they were able to get a production deal and move forward. When the option expired, the production company asked for a six month extension. By this time I was gainfully employed, and so had little motivation for seeing a movie produced that showed me in such an unfavorable and false light. I refused to go along with the extension. That killed the movie deal for everyone, including Markoff, who had probably expected to make a great deal of money from the project. Here was one more reason for John Markoff to be vindictive towards me. Around the time Cyberpunk was published, Markoff had ongoing email correspondence with his friend Shimomura. Both of them were strangely interested in my whereabouts and what I was doing. Surprisingly, one e-mail message contained intelligence that they had learned I was attending the University of Nevada, Las Vegas, and had use of the student computer lab. Could it be that Markoff and Shimomura were interested in doing another book about me? Otherwise, why would they care what I was up to? Markoff inPursuit Take a step back to late 1992. I was nearing the end of my supervised release for compromising Digital Equipment Corporation's corporate network. Meanwhile I became aware that the government was trying to put together another case against me, this one for conducting counter-intelligence to find out why wiretaps had been placed on the phone lines of a Los Angeles P.II firm. In my digging, I confirmed my suspicion: the Pacific Bell security people were indeed investigating the firm. So was a computer-crime deputy from the Los Angeles County Sheriff's Department. (That deputy turns out to be, co-incidentally, the twin brother of my co-author on this book. Small world.) About this time, the Feds set up a criminal informant and sent him out to entrap me. They knew I always tried to keep tabs on any agency investigating me. So they had this informant befriend me and tip me off that I was being monitored. He also shared with me the details of a computer system used at Pacific Bell that would let me do counter-surveillance of their monitoring. When I discovered his plot, I quickly turned the tables on him and exposed him for credit-card fraud he was conducting while working for the government in an informant capacity.

I'm sure the Feds appreciated that! My life changed on Independence Day, 1994 when my pager woke me early in the morning. The caller said I should immediately pick up a copy of the New York Times. I couldn't believe it when I saw that Markoff had not only written

an article about me, but the Times had placed it on the front page. The first thought that came to mind was for my personal safety-now the government would be substantially increasing their efforts to find me. I was relieved that in an effort to demonize me, the Times had used a very unbecoming picture. I wasn't fearful of being recognized they had chosen a picture so out of date that it didn't look anything like me! As I began to read the article, I realized that Markoff was setting himself up to write the Kevin Mitnick book, just as he had always wanted. I simply could not believe the New York Times would risk printing the egregiously false statements that he had written about me. I felt helpless. Even if I had been in a position to respond, I certainly would not have an audience equal to the New York Times s to rebut Markoff's outrageous lies. While I can agree I had been a pain in the ass, I had never destroyed information, nor used or disclosed to others any information I had obtained. Actual losses by companies from my hacking activities amounted to the cost of phone calls I had made at phone-company expense, the money spent by companies to plug the security vulnerabilities that my attacks had revealed, and in a few instances possibly causing companies to reinstall their operating systems and applications for fear I might have modified software in a way that would allow me future access. Those companies would have remained vulnerable to far worse damage if my activities hadn't made them aware of the weak links in their security chain. Though I had caused some losses, my actions and intent were not malicious ... and then John Markoff changed the world's perception of the danger I represented. The power of one unethical reporter from such an influential newspaper to write a false and defamatory story about anyone should haunt each and every one of us. The next target might be you.

After my arrest I was transported to the County Jail in Smithfield, North Carolina, where the U.S. Marshals Service ordered jailers to place me into 'the hole'-solitary confinement. Within a week, federal prosecutors and my attorney reached an agreement that I couldn't refuse. I could be moved out of solitary on the condition that I waived my fundamental rights and agreed to: a) no bail hearing; b) no preliminary hearing; and, c) no phone calls, except to my attorney and two family members. Sign and I could get out of solitary. I signed.

The federal prosecutors in the case played every dirty trick in the book up until I was released nearly five years later. I was repeatedly forced to waive my rights in order to be treated like any other accused. But this was the Kevin Mitnick case: There were no rules. No requirement to respect the Constitutional rights of the accused. My case was not about justice, but about the government's determination to win at all costs. The prosecutors had made vastly overblown claims to the court about the damage I had caused and the threat I represented, and the media had gone to town quoting the sensationalist statements; now it was too late for the prosecutors to back down. The government could not afford to lose the Mitnick case. The world was watching. I believe that the courts bought into the fear generated by media coverage, since many of the more ethical journalists had picked up the "facts" from the esteemed New York Times and repeated them. The media-generated myth apparently even scared law enforcement officials. A confidential document obtained by my attorney showed that the U.S. Marshals Service had issued a warning to all law enforcement agents never to reveal any personal information to me; otherwise, they might find their lives electronically destroyed. Our Constitution requires that the accused be presumed innocent before trial, thus granting all citizens the right to a bail hearing, where the accused has the opportunity to be represented by counsel, present evidence, and cross-examine witnesses. Unbelievably, the government had been able to circumvent these protections based on the false hysteria generated by irresponsible reporters like John Markoff. Without precedent, I was held as a pre-trial detainee-a person in custody pending trial or sentencing-for over four and a half years. The judge's refusal to grant me a bail hearing was litigated all the way to the U.S. Supreme Court. In the end, my defense team advised me that I had set another precedent: I was the only federal detainee in U.S. history denied a bail hearing. This meant the government never had to meet the burden of proving that there were no conditions of release that would reasonably assure my appearance in court. At least in this case, federal prosecutors did not dare to allege that I could start a nuclear war by whistling into a payphone, as other federal prosecutors had done in an earlier case. The most serious charges against me were that I had copied proprietary source code for various cellular phone handsets and popular operating systems. Yet the prosecutors alleged publicly and to the court that I had caused collective losses exceeding $300 million to several companies. The details of the loss amounts are still under seal with the court, supposedly to protect the companies involved; my defense team, though, believes the prosecution's request to seal the information was initiated to cover up their gross malfeasance in my case. It's also worth noting that none of the victims in my case had reported any losses to the Securities and Exchange Commission as required by law. Either several multinational companies violated Federal law-in the process deceiving the SEC, stockholders, and analysts—or the losses attributable to my hacking were, in fact, too trivial to be reported. In his book he Fugitive Game, Jonathan Li wan reports that within a week of the New York Times front-page story, Markoff's agent had "brokered a package deal" with the publisher Walt Disney Hyperion for a book about the campaign to track me down. The advance was to be an estimated $750,000. According to Littman, there was to be a Hollywood movie, as well, with Miramax handing over $200,000 for the option and "a total $650,000 to be paid upon commencement of filming." A confidential source has recently informed me that Markoff's deal was in fact much more than Littman had originally thought. So John Markoff got a million dollars, more or less, and I got five years. One book that examines the legal aspects of my case was written by a man who had himself been a prosecutor in the Los Angeles District Attorney's office, a colleague of the attorneys who prosecuted me. In his book Spectacular Computer Crimes, Buck Bloombecker wrote, "It grieves me to have to write about my former colleagues in less than flattering terms.... I'm haunted by Assistant United States Attorney James Asperger's admission that much of the argument used to keep Mitnick behind bars was based on rumors which didn't pan out." He goes on

to say, "It was bad enough that the charges prosecutors made in court were spread to millions of readers by newspapers around the country. But it is much worse that these untrue allegations were a large part of the basis for keeping Mitnick behind bars without the possibility of posting bail?" He continues at some length, writing about the ethical standards that prosecutors should live by, and then writes, "Mitnick's case suggests that the false allegations used to keep him in custody also prejudiced the court's consideration of a fair sentence." In his 1999 Forbes article, Adam L. Penenberg eloquently described my situation this way: "Mitnick's crimes were curiously innocuous. He broke into corporate computers, but no evidence indicates that he destroyed data. Or sold anything he copied. Yes, he pilfered software but in doing so left it behind." The article said that my crime was "To thumb his nose at the costly computer security systems employed by large corporations." And in the book The Fugitive Game, author Jonathan Littman noted, "Greed the government could understand. But a hacker who wielded power for its own sake ... was something they couldn't grasp." Elsewhere in the same book, Littman wrote: U.S. Attorney James Sanders admitted to Judge Pfaelzer that Mitnick's damage to DEC was not the $4 million that had made the headlines but $160,000. Even that amount was not damage done by Mitnick, but the rough cost of tracing the security weakness that his incursions had brought to DEC's attention. The government acknowledged it had no evidence of the wild claims that had helped hold Mitnick without bail and in solitary confinement. No proof Mitnick had ever compromised the security of the NSA. No proof that Mitnick had ever issued a false press release for Security Pacific Bank. No proof that Mitnick ever changed the TRW credit report of a judge. But the judge, perhaps influenced by the terrifying media coverage, rejected the plea bargain and sentenced Mitnick to a longer term then even the government wanted. Throughout the years spent as a hacker hobbyist, I've gained unwanted notoriety, been written up in numerous news reports and magazine articles, and had four books written about me. Markoff and Shimomura's libelous book was made into a feature film called Takedown. When the script found its way onto the Internet, many of my supporters picketed Miramax Films to call public attention to the inaccurate and false characterization of me. Without the help of many kind and generous people, the motion picture would surely have falsely portrayed me as the Hannibal Lector of cyberspace. Pressured by my supporters, the production company agreed to settle the case on confidential terms to avoid me filing a libel action against them.

Final Thoughts

Despite John Markoff's outrageous and libelous descriptions of me, my crimes were simple crimes of computer trespass and making free telephone calls. I've acknowledged since my arrest that the actions I took were illegal, and that I committed invasions of privacy. But to suggest, without justification, reason, or proof, as did the Markoff articles, that I had deprived others of their money or property by computer or wire fraud, is simply untrue, and unsupported by the evidence. My misdeeds were motivated by curiosity: I wanted to know as much as I could about how phone networks worked, and the ins and outs of computer security. I went from being a kid who loved to perform magic tricks to becoming the world's most notorious hacker, feared by corporations and the government. As I reflect back on my life for the last thirty years, I admit I made some extremely poor decisions, driven by my curiosity, the desire to learn about technology, and a good intellectual challenge. I'm a changed person now. I'm turning my talents and the extensive knowledge I've gathered about information security and social engineering tactics to helping government, businesses and individuals prevent, detect, and respond to information security threats. This book is one more way that I can use my experience to help others avoid the efforts of the malicious information thieves of the world. I think you will find the stories enjoyable, eye-opening and educational.

—Kevin Mitnick

LOCKPICKING

Written By Token
token@port7alliance.com

What society considers a taboo and criminal skill; lockpicking has become more misunderstood than anything else. Consequently, it has gained a status synonym with burglary and thieving. Kind of reminds you of another skill paired with criminal activity, doesn't it? Yes, I'm talking about hacking. The whole nature of it is much like hacking. Sure, there are the morons with 200 dollar lockpick sets, picking locks and not even bothering to learn a bit about locks or how they work. Then there's Hollywood. Just like with hacking, lockpicking is portrayed as such an easy and passive skill in Hollywood, in which most house doors can be picked with a bit of bubblegum and a sewing needle. But, in actuality, the skill is far more involved, and has a wealth of knowledge to be collected about it.

Lockpicking can be used for seedy purposes, for sure, but in the right hands, it can help you better yourself in many ways. Concentration, for one, is a very large part of lock picking. Without concentration, you will skate around the lock with no direction. You also must learn to channel frustration with lockpicking, as sitting in front of a lock with no breaks for about 10 minutes is a bit more arduous than you might imagine. The bottom line is: lockpicking involves many elements evident in hacking, also. By lockpicking, you can better your hacking and coding perception. Now, for the experimentation.

To lockpick, you have to experiment quite a bit. Experimenting with locks is made a bit easier with a correct environment in which to do so. That is, you don't want to be caught with a pointy metal object inside of a neighbor's lock. In fact, don't even try it on your own external house locks. If a neighbor sees you fiddling with a house lock, they might label you as a delinquent. Let me ask you... would you like to get in a stalemate with the police about what the purpose of experimenting with locks is? "I just want to learn about locks, officer, I'm not doing anything illegal." This line will get you nowhere with suspicious cops, it may even get you a broken nose from some 2 digit IQ cop who thinks you're being a smartass. So, play it safe, keep the experimentation in the privacy of your home.

The tools you will need are:
A: A pin tumbler lock
B: A pick
C: A tension wrench
D: A flashlight

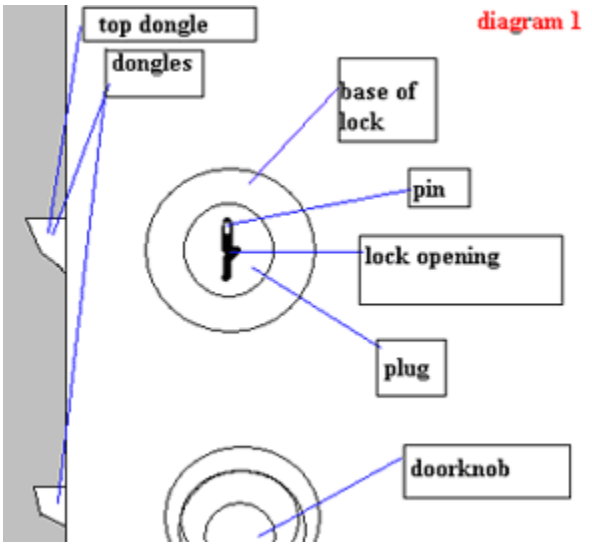


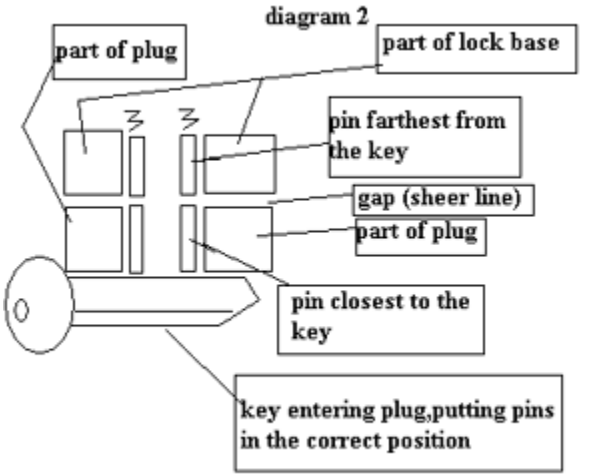
diagram 1

The pin tumbler lock, quite simply, is the lock you will be experimenting on. A pick, of course, is used to manipulate the pins of a lock. It must be small and narrow, something like a very thin paperclip. A tension wrench is used to apply force to the interior of the lock (I will explain the methods and reasons behind this later). It should be a very dense and metal object, and should also be narrow enough to eliminate the obstruction of view while working with the pins, as well as fit in the lock. Lastly, the flashlight is used quite simply, to light up the interior of the lock for picking. Now, on to the parts of the lock we will be picking.

First off as shown in diagram 1, is the base of the lock, containing the upper plate in the lock. Second, is the plug, which acts as the second plate in the lock. Third, is the lock opening, the area which we will be picking. Fourth, are the pins, which are the objects that will be manipulated with the pick. Fifth, are the dongles. When the correct key enters the lock opening and turns to an unlock position, the top dongle retracts back into the door, clearing the door to open forward or backward on the hinges. The doorknob and door are there merely to give you a better idea of what I am illustrating, so you don't become confused after glancing at my diagram. All the non labeled white space in the diagram is noted as the door, and the gray area should be disregarded completely.

Now, to pick the lock. You will be using what I call the "catch and pick" exploit to pick your first lock, one of the most common methods of picking. To understand this exploit, you must understand how a key opens a lock. A key opens a lock by forcing the pins closest to the key upward into a position that allows the plates (the plug and the base) to slide over each other. To put it in broader terms, it allows the plug to be turned inside of the base, to move the dongle. When a pin is in an incorrect position, it will not allow the movement of the plug within the base. It's like putting a stick in someone's bicycle tire spokes; the stick binds to the spokes so that the wheel cannot turn. Without the added friction of the stick, the tire moves freely. To see a lock in action, look at diagram 2.

diagram 2



The "catch and pick" exploit consists of individually setting the pins. By setting, I mean having the gap between the pin closest to the key and the one farthest from it (diagram 1), plush with the sheer line. First, take your tension wrench, and insert it into the bottom of the lock opening. Turn it as if it were a key, and apply a minimal force. Now, get out your handy dandy flashlight, and prop it so it is lighting the inside of the lock. While picking, you must keep force on the tension wrench. Start sweeping over the pins with the pick, starting at the farthest pin from you in the lock opening. When I say sweeping, I mean apply upward force to the pins, as if a key were entering the lock opening and forcing them upward. If the correct force was applied with the tension wrench, a pin or even a few pins should have caught on a plate, setting them. If no pins were set on the sweep, increase the pressure on the tension wrench, and sweep over them again. Repeat this process until all the pins are set, which could take a while.

Now, for troubleshooting. The most common problem among is picking the pin closest to the pick into a position where it is caught between the plates, in a non set position. It stays in this position because the tension given by the tension wrench is keeping it in place. To tell if you are having this problem, you need only look inside the lock. If all your pins appear to be in set position, but the plug won't turn, you are having this problem with one of the pins. To fix this during a trial, slowly decrease the turning pressure on the tension wrench. You might un-set a few other pins, but that's life.

Don't get discouraged if you can't pick a lock at first, it takes time, and you have to develop a certain sense of what's going on in the lock as you are picking it. This specific perception will add extreme ease to the skill, and you will be picking complex locks in no time. If you have any questions on this text, just drop me a line at the port7alliance forums. Until RF4, later. OI OI OI!

"Anarchy is a considerable solution to U.S. government problems, seeing as there would be none"

Written By Khaos & Token

Our country's gonna be so fucked in the next decade or two. Many problems will arise, and many old ones will get even worse. Not to mention there is no telling what Dubya might do to the country in the next few years.

First (status quo): The government is screwing us out of our money. In the course of about 20 years from this time, they are going to come crying back to us, saying that *they* are having problems. The Middle American sheep will go along with it for a bit, fully content on signing their rights away, but in the end they will see the government for the bunch of fucks they are. Once the government is in deep shit, they will have dragged everyone else through the mud with them, rendering Middle America useless to their lost cause.

Second (problems arise): An overpopulated prison system without funding means mass amounts of abused inmates. The inmates will be abused both mentally and physically, and with fewer guards on payroll to enforce rules, it will send prison abuse sky high. Second, there will be many problems with public schools. Many programs will be destroyed, including programs for "gifted children". Furthermore, teachers, many of whom already deal with ridiculously low salaries, will face even lower, possibly much lower salaries. Third, veteran benefits will be fucked, and veterans will be left out in the cold, with no compensation for their lost youth. Four, unemployment will shoot through the roof, dawning in a new dark age for this country, including a rapid decline in the stock market and economy. The average quality of life will decrease by a large margin, and the "American dream" will be a lost idea of the past. Exaggerating? I think not. Once we destroy our oil relations in the Middle East, the economy will plummet like Cory Feldman's acting career. Now on the other side of poverty, under-the-table deals and dirty money handshakes will not only be allowed to exist, but will be the backbone of new businesses, due to the lack of regulation in large corporations.

Third (going anywhere fast? I think not): Ford patented a water engine somewhere around 1935. It could run 50-100 miles on 1 gallon of water, using the power of the atom. It went about 20 miles per hour, and no matter how slow it may have been, there was huge potential in the design. Gas engines used to lag at about that average speed, but they, through time, were perfected and made more efficient. The same thing could have been done with this water engine. However, Chrysler bought the

patent, and it has never been seen from again. You may be thinking to yourself "Why not move on to a water powered engine, if it inherently much cleaner and, when developed, could reach the power of a gas engine". Let me spell something out for you: Oil equals money. If they were to make a water powered automobile, gas companies would get screwed. Who would buy a gallon of gas for 500% more than a gallon of water to power a car? I can't think of one person. Gas is money, and it also causes problems for cars. The combustion engine eventually destroys itself through constant usage, whereas a nuclear power source stays useful far longer. If a car engine craps out, that means someone has to buy another engine. That means more money for Chrysler. So, the process begins anew. But soon we will be dangerously close to running out of oil, sending transportation down, and hurting the economy. Non-fossil-fuel powered cars will need to be made more efficient, and meanwhile, engines will be slow and laggy. It's relatively difficult to have a populous driving to work at a top speed of about 20 mph.

Fourth (kiss that money goodbye): And then there's social security. Since they cut into the "surplus" in the 60's for the war effort, the government owes a huge debt to social security. Now, in about 12 years, we, as American citizens, will be supporting 5 people with our tax social-security-wise. But congress still keeps their lifetime cushy 120k. In the sixties Lyndon B. Johnson cut into social security to help the Vietnam War effort. Well, of course this was futile anyway because we didn't win the war. So, in effect, America made an "I Owe You" to social security for the x number of dollars they took out. Well, of course, in years to come, social security "surplus" money was taken out whenever the government pleased. Might I add, one stipulation of the law was that "surplus" or as the figureheads call social security, they could take out as much money for whatever they wanted. Now, we are far past the Vietnam war.

The average social security benefit is $700 a month now, and here's the problem: Whenever congressmen retire, they get a congressman's salary for the rest of their life. This is something like 56k a year so, what the fuck do they care about a 76 year old woman in Cleveland eating cat food every day of her life? Now, the baby-boomers are just on the brink of retiring and there are TONS of baby boomers. What do you think the government's solution to this will be? Do you think they will pay off the surplus for the baby boomers? Well, you can bet they won't. You can also bet that we will have raised taxes also. An estimate in 1960 of benefits of social security was calculated: 5 people supported people eligible. Now, if surplus continues in the direction it is heading, there will be a 1 to 5 ratio of people paying to people getting paid (i.e. 1 person will be supporting 5 people on social security). That's 25 times more. In conclusion, we are fucked, unless we beat these congressmen into shape.

One of the biggest problems is Middle America. They are far too comfortable to do anything about the government. With 2 kids, an SUV, and a mortgage, they have lost their will to fight. With a family, it's a lot harder for them to stand up for themselves. I doubt they will ever come around to truly fight for their rights.

Fifth: As for the current state of nuclear disarmament, there is none to speak of. The a-bombs that almost destroyed the earth in the Cuban missile crisis are still very volatile. Superpowers and former superpowers may claim to "disarm" them, but in actuality their definition of disarming an a-bomb is a contradiction in terms. Uranium has a long half-life, you just can't destroy it that easily. And, in 20 years, we will have new reasons to use the power of the atom. Getting too caught up in our search for ultimate wealth and power, we will make new enemies, and also new friends. At the current moment in time, we are closer than you might think to full out nuclear war. We are in big trouble with Iraq, and I doubt they would think twice about using tactical nukes to destroy our troops if they are losing out in the war effort. And yes, Iraq does have soviet a-bombs, they just have a short range, perfect for taking out large masses of our troops in their region, or for nuking Israel or any other nearby country.

I think that the problems in the next 20 years *could* be good for America. They will force America to be progressive, and if America isn't, our superpower will be decimated into a smoldering pile of ashes.

The Verizon Office Companion

By J0hny_Lightning
j0hnylightning@hotmail.com

The Verizon office companion is a booklet that's small enough to fit in your pocket and it's every aspiring hacker's/phreaker's dream. It's like a mini-yellow pages for small businesses that's packed with interesting web sites and phone numbers that should be made available to everyone who wants them. Examples of provided information include: Numbers of long distance providers, computer manufacturers, cell phone companies, the post office, telephone directories, online resources, airline numbers, and government offices (ie: passport offices). If that's not enough, it also provides a full area code chart that covers most of the world. While the above mentioned stuff is all good and has its uses, the most useful thing about this booklet is the glossary and acronym / abbreviation chart of common used business terms. This little booklet in my opinion is a must have for anyone who plans on ever trying to social engineer any information from a business. You can order a copy by calling
1-866-992-9211, enjoy!

Movie Review- The Matrix
By KiLLer

www.whatisthematrix.com

Characters
Keanu Reeves- Thomas Anderson/Neo
Laurence Fishburne- Morpheus
Carrie-Anne Moss- Trinity
Joe Pantoliano- Cypher
Hugo Weaving- Agent Smith

Directors
Director- The Wachowski Brothers
Producer- Joel Silver
Written By- The Wachowski Brothers

Perception: Our day-in, day-out world is real.
Reality: That world is a hoax, an elaborate deception spun by all-powerful machines of artificial intelligence that control us. Whoa.

What an excellent movie! It's definitely the best movie I've ever seen until The Matrix: Reloaded and The Matrix: Revolution kills my mind.

To leak a bit of info, this movie is about a small group of cyborgs and (real) humans versus a world of machines. The machines have taken over mankind and uses humans as energy because humans scorched the sky to block the sun that the machines used as energy. In order to stop humans from winning the war in the real world, the machines has created the Matrix and made us perceive our mind to think we already won the war and we live in the REAL world when we actually are enslaved living in the Matrix. The rebels strive to find the "One". Only the "One" predicted by the Oracle can hail destruction on machines and end the war.

Thomas Anderson is a programmer at a software company. When he isn't working, his alter ego is Neo, a hacker that has broken every rule applied to computer law. Morpheus is the leader of the small band, trying to find the One. Trinity is the ranking officer on the ship also trying to find the One. Cypher is part of the crew trying to find the One, something's up though. The sentient program agents are sent to destroy Zion so these rebels wouldn't find the One and defeat machines. And these are just the main characters; I won't spoil anything, so watch for more.

I recommend this to people with open mind, to people who want to know what our society is similar to. Hopefully people who see this movie will see the deep meaning and not just go "wow so?" and the "guns".

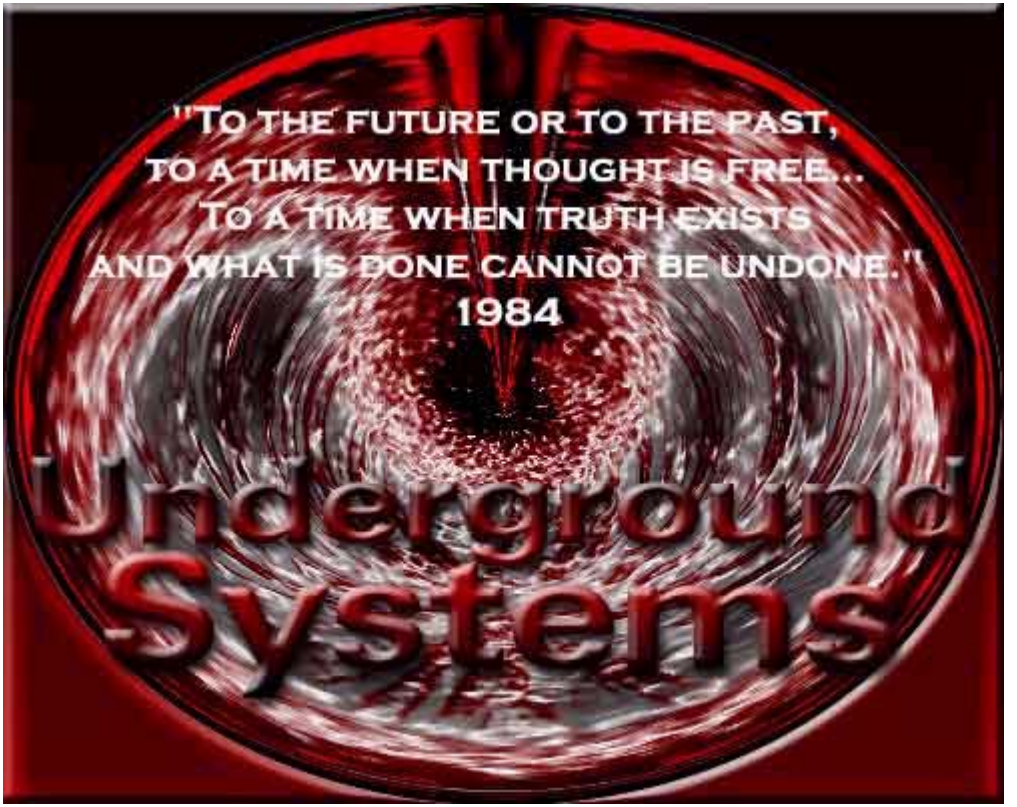
This movie goes over the scale of five stars and two thumbs! Watch it! Again and again!!

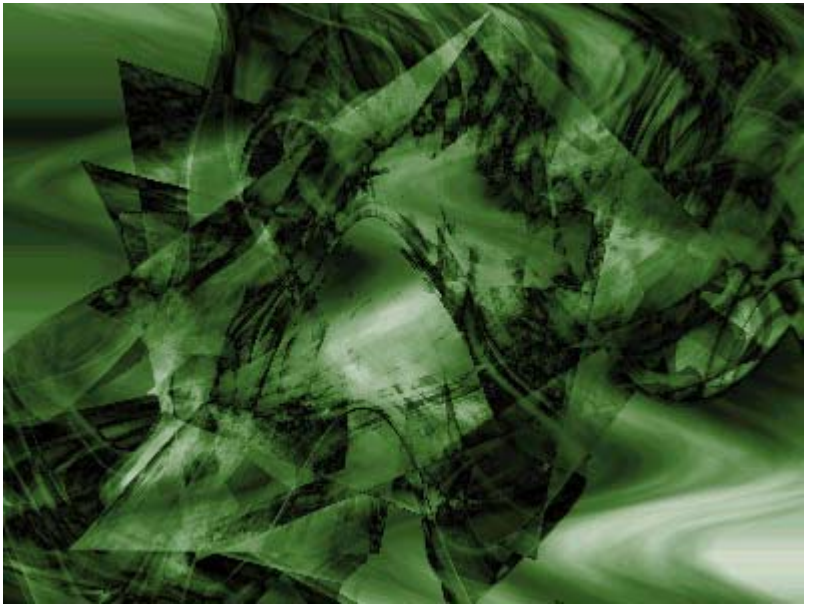
"Get Ready to Reload..."

Excerpt From "Approximations"
By Anthony George

the precision of dreams is the chaos of their means you might hope for a dark, black screen but your mind likes to sing, it likes to scream involuted invertness leads to mortal infinity of deeds you'll float like elastic fragrance beating drums of an inner mind trance constant dance mad scientist beyond wilderness evolutionary soft hardness pure belief and indifference delving revolving twisting solutions beyond resolving picture nomenclature naked aperture exploding nature luck and crime happen all the time turns in the nowhere that are sublime industrious secret paths memory furnace see the blueprints on every face invisible laughs bounce in the head of your version of god just another tread that is a monument but also begins to shred things in the a.m. are another way of again the new unknown after then abstract breeding ground upon which we're all clowned to escape the everyday to which we're bound for all you can't say there is a way necessary carnage at play for every sin there is a medicine all that was and will be you have also been your face in the front of you and miles away old and infant you become a dispersing crowd you wish would stay you preach the nothing but beseech they pray you are the story of night fornicating with day the smoke comes out your mouth like you know everything your lungs are smarter than your brain some people here lead their students into blind allegiance pledges they offer the worst kind of nothing the nothing that is death from beginning to end every approved answer makes the script of ignorance and deceit the conformists are awarded trophies by the chain of command silence is the eloquence championed by the masters and the chosen are very famous but have no ability no skill no inclination to relieve suffering the bar codes on their heads make them applaud vigorously for every disinformative plan for each empty attempt at concern therefore ceremonies of willful blindness are the great totems of newsletters and resumes some people here can't see children because they do not know history only the current pageantry ordained as real the murder of compassion is permissible is pervasive is requisite in the marginalization of dissent in the dismissal of conditions and behaviors related to the planned economic wasteland called the grand shut and work...

Created by KeMiKaLPHReaK



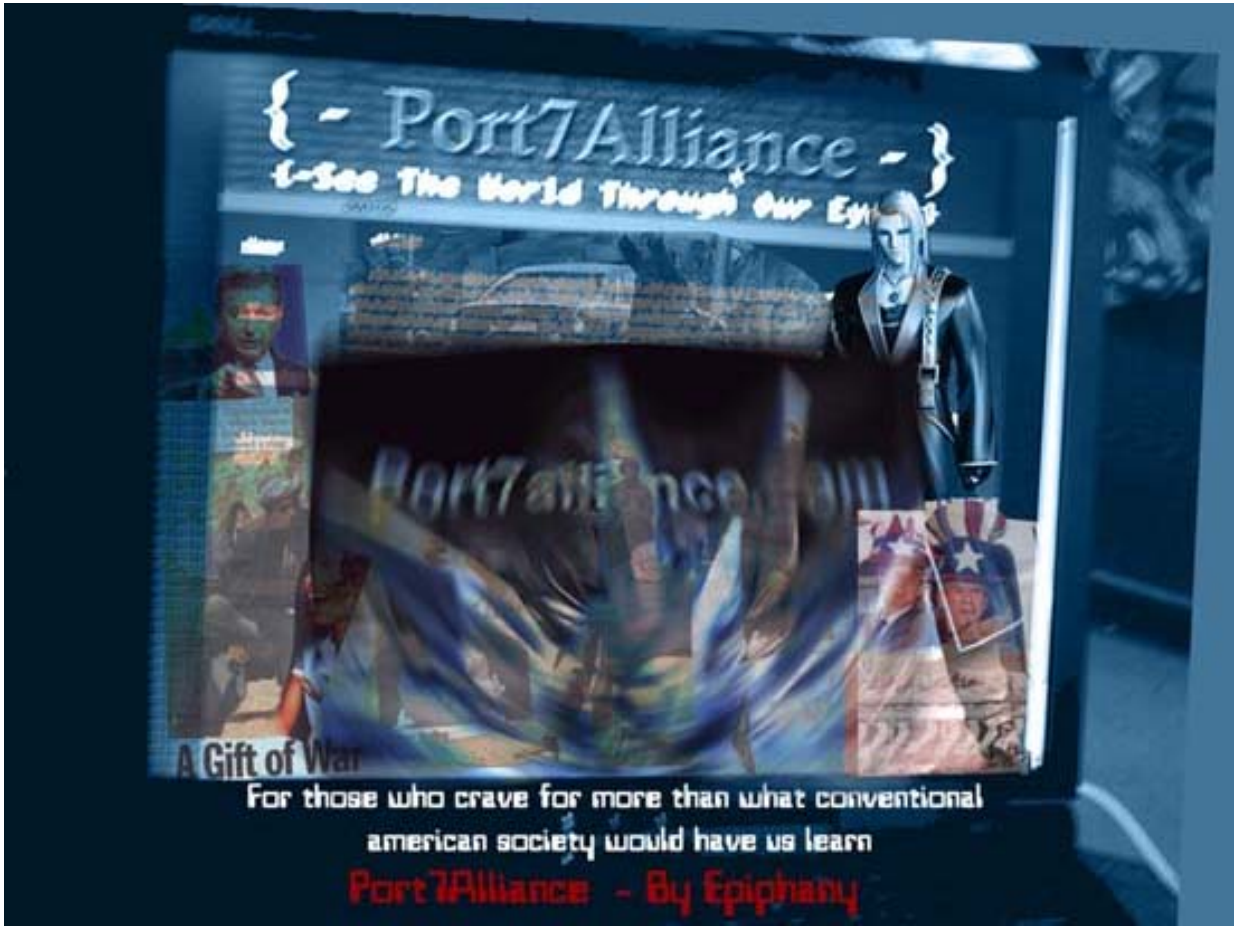


Created by Unity

Both Created By Scramble45

22 Radical Future

<----- Modified By Scramble45
|
| Created By Epiphany
|
\|/



Vending Machines

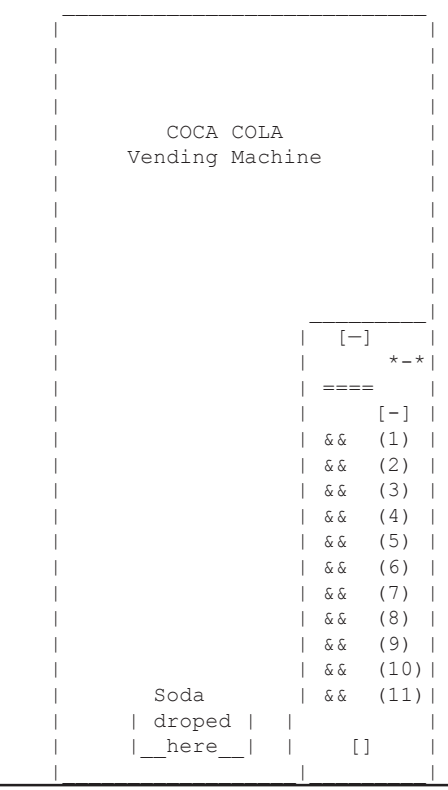
Written By Khaos with help from Silence
khaos@port7alliance.com

This is an over view of many aspects of vending machines. I will cover many methods of taking advantage of vending machines (acquiring items for free, and some neat tricks.) First, a word of warning and a disclaimer. Some of the things depicted in this text are not entirely legal; this was written for educational purposes only. Heh. OK here we go...

IMPORTANT WARNINGS:

1. Many companies video tape the vending machine locations. Before you do anything scope the place out and check for cameras.
2. Almost all the newer vending machines have alarms and tilt switches, so before you do any messing with the machines that involves physical tampering (i.e. shaking/tilting) UNPLUG it. This should avoid the anti-vandalism measures.

Fig. 1.1



***NOTE:** the vending machine must look like this and have the same interface for the commands described in Part 4 to be executed.

<<< The [-] is the dollar intake slot
<<< The *-* is the change slot
<<< The == is the display the scrolls something like "Ice Cold Coca Cola - $1.00"
<<< The [-] is the change return button (the one you press to get your money back).
<<<these are the buttons that you press to select your item. The && is the little picture of a coke bottle telling you what you are choosing, and the (1) is the first button, (2) is the second down, and so on. This is important because I will refer to these buttons later by there numbers.

<<< The [] is the change slot where the change comes out

PART 1 - Simple Thievery:

These are all tried and true methods of stealing items and/or money from a vending machine. If done correctly on the right machine these WILL work. I have tested all of these methods myself.

Shake it! - There is an easy way to get free soda from an older vending machine, although you will have to go through a little work. Many vending machines have vertical shafts with opening in the top for depositing the cans of soda. It takes at least 2 people to do this but I would suggest more. If people get on the sides and in front and tip the machine slightly forward, it is quite a manageable task to shake the cans free from their shafts, thus giving you a free soda for your efforts. This is by far my least favorite method, because not only do you require other people to accomplish this, if the vending machine falls over you can get seriously injured. This does happen.

Reach for it! - The next method of robbing a vending machine deals with the candy vending machines. Have you ever tried to reach your hand up through the slot where you get the candy, and take an item off the rack? You can't because a piece of metal blocks the way when the opening is pushed forward. But there is enough room to unbend a coat hanger and stick it through the receiving slot, snake it up and hook onto an item above and pull it down. Rinse, repeat, free candy!

Stuffing - My next method is much less effort than the last 2 for much more gain. The concept is simple. When someone hits the "change return" button, they will not receive the change if the passageway is blocked. For this I would use a well trafficked vending machine. Early in the morning, take something, like a napkin, and shove it up the slot where the coins come out. Make sure the napkin is far enough up the slot that it is not visible, or someone else might reap the rewards of your work. During the day, whenever people want their money back, the coins will get caught above the napkin. At the end of the day, return to the machine, pull out the napkin, and take all the days returned change!

PART 2 - More elaborate felony *{both of these methods are outdated and will not work on most machines}*

Ok these next 2 ways are a bit more involved then the last ones and they are somewhat more dangerous (assuming you don't drop the vending machine on yourself like in the first method.) To be honest I have not actually done either of these myself, although I did witness the salt water method successfully completed.

Salt Water Method:
This should not be tried just for the hell of it; if you are not careful it can lead to electrocuting and/or explosion. With successful executing of this method, the vending machine will short, and it will shoot out free soda and coins. To accomplish this you need to fill a spray bottle with water that contains a small amount of salt. Spray this solution through the change slot and back up. The salt water should cause the above said result.

*****NOTE:** This method was originally done on MacGyver and the wide spread

publicity of it has pretty much made this method obsolete. Many years ago the vending machine companies began perforating the channel that the coins fall through causing a diversion for the salt water. However this technique still works on many older vending machines. Look for the machines with the coin slot above the dollar intake slot.

Key Dupe:
I have neither done this myself nor seen it done, but I have heard of it being accomplished. It is rather simple. What is needed is some kinda of clay or plaster that will harden in air. Find your target vending machine. During a low-traffic time, push the clay or plaster into the key hole. The material will harden, and when it does pull out the 'key'. You now have a working replica that will open the vending machine door!

NOTE, I have heard from a few sources that this will not work

Part 3 - Breaking In

LOCKPICKING:
There are basically 3 different lock-types (there are more but this is a general description).

Gematic-type: Very cheap lock. The main weakness is that the cam (which is the small piece of metal on the back of the lock which holds the cylinder in place) is held by a single small screw. Most of the time it is aluminum alloy. To defeat this lock, use a tubular key. File it so that only the pin that sticks up from the center is left. It should rotate freely when inserted into the lock, but you can't pull it out. Attach a chain to the key, and wrap the chain around a bar or something. Pull hard. The cam should either come completely off or it will be bent beyond functionality. Lock opens.

Ace-type: More expensive and more secure. The cam is held by nut and bolt. This means you can't pull it. It is still possible to get in. The lock is nickel alloy, coated in carbon steel. Take a drill bit and drill into the cross section where the key slot meets the cylinder opening. After a few minutes the cylinder will fall out or you will just drill right through the lock and the bolt.

American-type: These are locks that have a completely flush face. Instead of a tubular cylinder lock the lock relies on a set of pins on the key. The face is drill proof. Forget it and move on to direct break in.

DIRECT:
Nearly every vending machine has the T-bar locking system. That is, there is a steel bar traveling the length of the machine, securing the door and the top, bottom and side next to the lock, which is opposite the hinge. Get a pry bar and a hammer. Unplug the machine, unless you want to be caught. Now climb up on top of the vending machine. Go in a straight line up from the lock and you will find where the locking bar intersects with the roof. Insert the pry bar (it may be necessary to hammer it in.) Get it about an inch to the side toward the hinge. Pry it open. Once the top is open you can pry open the locking bar. Then pull the door open and grab what you want. This should be able to be done easily in less than 5 minutes.

Part 4 - Hacking the Vending machine

This is the reason I wrote the article in the first place. All of this other stuff can be found somewhere else, online, in a book, from your mind. But I have never seen a single article about hacking vending machines. OK to start off with there is a universal code for all vending machines that I have tried it on. That is the soda machines. The highest button would be slot 1, below that 2, etc. The universal access code on these machines is 1-2-4-2-3-1, meaning you would hit those slots in that order. This brings up an "Eror" message on the display. The Display is the little thing that says "Ice cold coca-cola $1.00" or whatever. After pressing the code it should read "Eror." If it doesn't, you got the wrong machine. Now what? Well once you are at the "Eror" screen you use 2 and 3 to scroll through the options. On one machine I tried the options were "CASH, SALE, and rtn. I do not understand most of the commands, but SALE is pretty self-explanatory. It will tell you how many items have been sold out of that slot. To look and each slot we would hit the access code 1-2-4-2-3-1 and then 2 or 3 until it reads SALE. Then press 4 to 'pick' that option. Now use 2 or 3 to scroll through each slot. The slots are labeled SL

1 through SL 13, although most machines don't have 13 slots. Once you get to SL 3 for instance, wait about a second. A number will pop up, like '1764.' That means that 1764 total items have been sold out of that slot. To go 'back', like getting back to the sale options, it is similar to going up a directory on a computer.

To do this hit 1. If you hit the change return button it will go back to the "Ice cold coca-cola $1.00" screen. Now you are back at the 'menu.' Use 2 or 3 to scroll to CASH. Now hit 4 to select it. Now use 2 or 3 to scroll through CA 1 through CA 13. Pausing over one slot for about a second, will show 2 bits of information. The first is an integer. I do not know what this number means. The second is an amount of money. For instance on a machine I tested it gave me this info:

CA1 - 68 - 36.50
CA2 - 70 - 99.50
CA3 - 13 - 16.75
CA4 - 8 - 72.50
CA5 - 5 - 45.00

Now hit either 1 to go back to the menu or hit the change return to go back to the normal message, from which the code would need to be entered again. More options are available by pressing 1-2-4-2-3-1 and then hitting 4 and then scrolling through the options with 2 and 3. Options on one machine I tested were Ctrl or VEND. By using 4 to select Ctrl it displayed ACLO and nothing more. When using 4 to select VEND it showed the options h5, Ec, and rE but they didn't appear to do anything. I saw many other options, and it varies by machine. Some other options from the 'main menu' (the first menu) were rEn, SeS, and door.

I am curious as to whether there is a way to open the door from this menu. However I doubt it. I collaborated with Silence and he got the guy who works the vending machines there to open the door for him, and there is no electronic connected to the lock. There are many more options and I don't know what any of them do. I wrote this article to share my information and see if anyone else could find more out.

Silence also did some checking of this out, here's what he had to say:

Ok, Khaos turned me onto "hacking" vending machines, so I have done some research of my own.

Ok first things first. I will start with the menu, on the machine that I was on I found 2 new commands or lists that I didn't know how to use. And Khaos had not mentioned. They are:

RMT ACC. - We come to the conclusion that this is remote access of some sort but I do not know how to use it.

FMT DR. -We have come to the conclusion that this is a format drive command but still don't know how to use this either.

What I know.

Ok remember back in the phreaking days when you could simulate a tone that the coin made dropping in to fool the computer into believing the money was actually put in? Well I think the same method is done on these machines because inside the machine from all the slots *where you can press to get a drink* is hooked to a central computer. There has to be some way that the machine knows when it's taken in money and I think it's done this way. So if we can find out what tones are generated TADA free stuff.
-Silence

OK that's all I have I haven't had enough time to research it yet, but I will do a follow up article for RF4.
-Khaos of the Port 7 Alliance
Khaos@port7alliance.com

*****NOTE** I researched most of the information in part 3 from "Vending Machines, Payphones, and Billchangers",
By Mustard

HACKING MOVIES

The following is a list of hacker related movies. It is by no means complete. Please post any omissions in my forums at http://www.stankdawg.com/forums/ along with any other comments.

Compiled by: StankDawg@hotmail.com

Movie Title	Actors of note
23	None of note
Anti-Trust	Ryan Phillippe, Tim Robbins
Armchair Hacker	None of note
Arrival	Charlie Sheen
Arrival 2 (aka "Second Arrival)	None of note
BrainScan	Edward Furlong
Code Hunter (aka "Storm Watch")	Adrian Paul, Coolio, Tone Loc
Cube	None of note
Cube 2: Hypercube	None of note
Enemy of the State	Will Smith, Gene Hackman
Enigma	None of note
eXistenZ	Jude Law, Willem Dafoe
Freedom Downtime	Emmanuel Goldstein, Kevin Mitnick, John Markoff
Frequency	Dennis Quaid
Ghost in the Shell	None of note (Japanese Anime)
Hackers	Angelina Jolie, Jonny Lee Miller, Matthew Lillard, Penn Jillette
Johnny Mnemonic	Keanu Reeves, Ice-T, Takeshi Kitano
Lawnmower man 1	Pierce Brosnan
Lawnmower man 2: Beyond Cyberspace	None of note
Matrix	Keanu Reeves, Laurence Fishburne, Carrie-Anne Moss
Menno's Mind	Bruce Campbell
NetForce	Scott Bakula
new world disorder	Rutger Hauer
Operation Swordfish	John Travolta, Hugh Jackman, Halle Berry
Revolution OS	Linus Torvalds
Serial Expirements: Lain	None of note (Japanese Anime)
Sneakers	Robert Redford, Sidney Poitier, Dan Aykroyd, River Phoenix
TakeDown (aka "Cybertraque")	Skeet Ulrich, Tom Berenger, Russell Wong, Tsutomu Shimomura
Techno Warriors	None of note
Techno Warriors 2: Lethal Combat	None of note
Terminal Entry	None of note
Terminator 2	Arnold Schwarzenegger, Edward Furlong
The Code	Linus Torvalds
The Net	Sandra Bullock, Dennis Miller
Tron	Jeff Bridges
Virtuosity	Denzel Washington, Russell Crowe
WarGames	Matthew Broderick, Dabney Coleman, Ally Sheedy

For an updated version with a lot more information, come to
http://www.stankdawg.com/articles/stankdawg/hackingmovies.htm

AIM TRANSCRIPT

Submitted By StankDawg (Stankdiggy on AIM)

StankDiggy : here a couple of commercials 4 u. From the campaign for freedom...
*StankDiggy wants to send file * .*
liberalist received
campaign_for_freedom.txt .
liberalist received
cff_tv_arrest_30_rp_v2.rm .
liberalist received
cff_tv_choice_30_rp_v2.rm .
liberalist received
cff_tv_church_30_rp_v2.rm .
liberalist received
cff_tv_diner_30_rp_v2.rm .
liberalist received
cff_tv_library_30_rp_v2.rm .
liberalist received
cff_tv_mainstreet_30_rp_v2.rm .
liberalist : these commericials are a bit exaggerated
StankDiggy : that is what commercials do...
StankDiggy : but they make valid points
StankDiggy : these do anyway
liberalist : letting the FBI tap phones to investigate suspected terrorists is a LOOOOOOOONG way from arresting a peaceful church congregation
StankDiggy : is it really? the point is where people draw the lines. to us, those are 2 very different things. In some places, it is not.
liberalist : YES! Where to draw the line....
StankDiggy : the new acts being blindly passed into law are so vague that the government does have the freedom to make their OWN LINES!
StankDiggy : that is the problem!
liberalist : hmmm
StankDiggy : by not establishing clear lines, they effective REMOVE the lines!
liberalist : i see
StankDiggy : look at the bigger picture man!
StankDiggy : let me find this link...
liberalist : k
StankDiggy : http://www.2600.com/news/display/display.shtml?id=1441
liberalist : so, you're saying that the new acts are capable of overriding our first amendment?
StankDiggy : apparently so, if the FBI thinks that on that particular day, the first amendment posed a threat to national security. :-(
StankDiggy : that also means that any rogue FBI agent (or any agency) can abuse power at a level UNHEARD OF in the history of the United States
liberalist : I find it very hard to beleive that those 19 guys succeeded simply by hiding behind the 1st amendment
StankDiggy : connect the dots for me here...
StankDiggy : because of those 19 guys (terrorists), several billion American citizens lose all of their rights as granted by our constitution?
StankDiggy : Something is wrong with that picture.
StankDiggy : I support the idea and the INTENT of the act. I want to stop terrorism as much as the next guy.
StankDiggy : But due to unfortunate general incompetence in our government, they fukked it up!
StankDiggy : and ruined it, but passed it anyway
StankDiggy : they should have simply done some research, and a little bit of work...
StankDiggy : then they could have created a law that enhanced security WITHOUT crossing the lines of human rights.
StankDiggy : but America doesn't know the meaning of WORK anymore. :-(
StankDiggy : all we know it political games, partisan politics, and other bullshit.
StankDiggy : am I wasteing my breath here?
liberalist : nope

StankDiggy : am I talking to myself?
liberalist : all interesting stuff
StankDiggy : u didnt respond, I though I lost u
liberalist : no, just reading
StankDiggy : You had no idea, did you?
StankDiggy : this law has been in place for a short time and we already have incidents like the link I just sent.
StankDiggy : that does not bode well for our freedoms.
liberalist : unfortunately I have not read the text of the new laws, so i don't know enough about what i'm talking about
StankDiggy : I have read enough to see gaping holes and overlapping situations
StankDiggy : For example: can I, or can't I take a picture of a public building?
StankDiggy : before the law, it was a simple yes.
StankDiggy : now, it is not (apparently)
StankDiggy : or is it a simple "NO"?
StankDiggy : and is that right? Is that the intent?
StankDiggy : look at http://www.hackcanada.com/
StankDiggy : This site shutdown (which is a JOKE) could very easily happen now!
liberalist : amazing. it is hard to believe that a photographer got arrested like that
StankDiggy : It was hard to believe in the past, but not in the current state of the union.
StankDiggy : they blindly pass laws without doing the work to make informed decisions.
StankDiggy : and who is going to listen to people like us when we voice our opinions?
StankDiggy : nobody. people are too stupid to realize that their rights are being taken away!
liberalist : yes, but the Secret Service and Denver police still have to chose to enforce the law.
liberalist : They should know that their family and friends are potentially subject to the same kind of treatment
StankDiggy : yes they should, but the potential is there, more than ever, for MISINTERPRETATION by JOE-BOB the buck toothed inbred cop who cannot make intelligent decisions.
StankDiggy : this country was founded on basic freedoms. we no longer have these basic freedoms. Therefore, we are no longer the same country.
StankDiggy : This is not the same country I was born in. :-(
StankDiggy : How much longer until we are all on 24 hour lockdown? It sounds a lot like prison to me.

MY FAVORITE FOOT-PRINTING TECHNIQUES

Written By Undetected

Foot-Printing might be a process you are familiar with. Perhaps you don't know it by that name but in the hacking world the basic gathering of data and information about systems or organizations could be classified as "foot-printing." What this article will cover is the methods I have found to be very successful. The approaches I will talk about aren't really technical. They more have to do with your ability to be patient, use Google very well, and have good deductive skills. The main idea of these methods is that organizations are overly open with certain sections of their website. Most valuable of these areas (to hackers) is the IT (information technology) section. These websites in my experiences have yielded vast amounts of information that is key to social engineering, and a technical exploit type attack. One important note is that this might not be as easy as I make it seem in this article. The reason for that is these methods were used against a very large school district in Kansas City that happens to be poorly organized. No authorization was needed to perform the outlined methods. This is most likely not the same case in other situations. Still all the methods will work against any organization as long as you can get a proper account. Even that shouldn't be hard. The typical idea I'm willing to bet in securing the information I talk about would be one of preventing anyone with no authentication access and allowing anyone with even the lowliest authentication access. This is due to the fact that hackers are probably the only ones really interested. At least I hope they will be after reading this article.

Well after all that what we are really going to find with all these magical methods I've been ranting on about for the past paragraph. Below are some examples. This information will come from places as mundane as an employee directory or some organization chart that is posted. The other technical information could probably be obtained from the IT engineers section. I doubt most of it would be real valuable. Now there are a few "gems" down there. For example you see the thing in all bold and capitalized. Yea the chances you are going to find that are about 1 in a million. Anyways my school district made the most dumb ass decision I have ever seen and uploaded to a freely available FTP server a list much resembling that. Granted none of the accounts where very privileged the information was all for minors and probably in violation of about 1000 laws. Specifically the CIPA. Maybe you will hear about that great act in another article.

Names of Engineers
Phone Numbers
Organization Charts
E-mail address
Basic Description of Network Infrastructure
Network Topology Diagrams
Call logs for Computer Problems
User Accounts/Information (Phone Numbers, Full Names, Addresses)
Web Based Services
Company/Organization News
COMPLETE LIST OF ALL USERS ACCOUNTS, HOME PHONE #'s AND
HOME ADDRESSES Etc.

BEFORE WE START...

Before we get into the real article I have something to recommend. First go to google.com and get the Google Toolbar. After that learn how to use Google. I'm talking the advanced features. If you don't know how to search by domain, or find different files, translate on the fly, and etc. you need to get comfortable doing so. You need to be willing to search a million different ways for the same thing.

As I mentioned before an important distinction is whether you're trying to gain information on some

Fortune 500 company compared to a school, college, or small company. Usually a larger corporation's website is their name and then a dot com. Well that website is crap. Probably absolutely worthless to you. Lots of crappy advertising. What you need is the website where the employees go. To find this website you might want to skip down to the port scanning and whois section. Also this website might just be hidden inside the mass of the websites a large company can have. Google using the specific domain field can become your best friend here. Search for things like IT, employee portal, and etc. Anyways, non-for profit organizations, colleges, government organizations, and small business are good examples. For instance your school district (if your in school anymore) probably has tons of IT stuff on their webpage but if you go over to the Southwestern Bell site, your out of luck for at least low impact searching. One of the most insecure/open organizations I have ever seen are colleges. This isn't surprising since colleges have an open environment anyways and the ideas they have aren't trade secrets. That's why hacking got started in colleges and the fact they had the hardware. If you want to have some real fun with the techniques I outline here go poke around www.mit.edu.

The first step will be finding out where the websites that house the organizations real information are. There are two methods I use for finding these websites. The first one is the one I would use first and most often. It's called Google my friends. It will become your friend. Using Google it's possible with patience to dig threw the mass of websites that a large organization could have and un-earth the one with the information you want. To find it I recommend first using the Advanced Google feature allowing you to search specific domains. From there try every possible way of expressing what it is you're looking for. Also try searching for names of commonly used programs that the company might use for bookkeeping, employee benefits management, and etc. The second method is to perform a whois query on the specific domain you are looking at. This can yield technical information, along with social engineering possibilities. You can also use the so called "IP-Range" to port scan. If you are more interested in Google then keep reading. If you want to look into the Whois skip down some.

So say you have found a website and found some of the typical stuff I have been talking about. How can we apply it? Let's look at the list above. The first three things are social engineering gold, I mean if you have someone's name and their rank from the Origination Chart you can pretty much know who will know who, whose low ranking, which employees might have actually talked before, etc. This can make your social engineering much more precise and powerful. The chart is also good for just getting a general understanding of names and positions. If you find an employee newsletter you can reference it against these names.

The network infrastructure and topology information and diagrams available are sometimes ridiculous in how much detail they have on them. You can save your self having to find out what each computer does, its OS, and its corresponding IP. Usually these documents aren't real wide open though since they are seen as a major vulnerability. Again remember Southwestern Bell or Sprint or any large company isn't bad enough to leave this sitting out. You will have to dig, and it could be some obscure link on Goggle that you find at 3:00 in the morning that leads you to what you want. Usually to view them will require an engineers account or someone associated with the IT department. Since we are going for low impact here (you don't want to set off a lot of alarms just looking around) I wouldn't recommend trying to crack their passwords yet. Keep looking around and maybe you can find another way of getting access.

Problem logs or complaint logs are another thing to look for in the IT section. Every IT department for a large organization has some type of automated report generator for their staff to deal with. These aren't something you should expect to be available on every site. Things like these would be closely guarded secrets for some organizations. Logs like these can tell you what's broken and therefore maybe weakened to intrusion, and the general state of things going on.

The internal news section of any website is great because everybody wants to brag about their technology and how cool they are. Want to know what made blue boxing possible. One article in some Bell Lab technical

magazine that had some mention of the exact frequencies that the tones worked on! Pretty boring huh? An example of a valuable article might be news of what is generally going on in the company right now or upgrades that have been recently implemented. Companies in their infinite wisdom will always be bragging about how they upgraded to IIS 9.0 or whatever. NOT A GOOD IDEA! Whenever you upgrade your moving to a possibly completely untested program. Don't need to tell everyone. Other then that it can be helpful to just get an internal feel of what is going on in the company.

Here is the more technical part of the article, but not necessarily more useful. I think if you are able to fuse the Google technique together with this you can become very very good at finding whatever you want inside an organization.

Doing a whois on the domain of the organization is also a great idea. If you aren't familiar with what a "whois" it is basically the act of questioning a database that keeps information about all domain holders more or less. I'm not going to recommend program for doing whois searches here. They are easy to find and you will need to do a little research anyways to find out how they work.

Here is the whois for Port7Alliance.com

http://domains.omnis.com

Whois Output for: port7alliance.com

Domain Name Owner:
Darien

Administrative Contact:
Port7alliance
Darien [DA-18]

Technical Contact:
Omnis Network
Network, Omnis [ON-1]
3655 Torrance Blvd Suite 440
Torrance, CA 90503, US
Phone: (310)316-2744
Email: nicreg@omnis.com

Billing Contact:
Port7alliance
Darien [DA-18]

Record Information:
Domain Record Created: January 13, 2001 12:42
Domain Record Updated: January 22, 2002 21:00
Domain Record Expires: January 13, 2003 00:00

DNS Information:
Name Server: ns27.100mwh.com
Name Server: ns28.100mwh.com

As you can see Darien (Epiphany) is listed as a pretty much the person to contact. Usually it would list some other information but I took it out so people at least have to put some effort into if they really want to spam/stalk Darien. If this was a "real" whois then it would've had actual contact names. It actually still has one for our hosting service. Anyways this also gives you the name of the DNS servers that Port7 uses. What is real useful is if it lists an IP range. From there you can use a port scanner to isolate what exactly is running on computers on that range.

Your port scan should be focused. Just don't whip out your port scanner, set to scan every port, leave your computer online all night, and use your good old DSL/Cable connection. Scan smarter, not harder! (You know you love the cliché!) Anyways just scan for things like ssh, telnet, ftp, smtp, pop3, and of course port 80(http)

Well to review I have discussed the basic list items to look for if you find an employee/real site. Now I have just talked about performing a whois query and then port scanning. So what after that? 31337 hAx0r every exploit you can on their machines. NO! Why would you do that? I would propose using an exploit to gain that initial step on to accessing that ftp server you need or web server. After this it is up to what you want to do. That will depend on your motivation.

An Introduction to Test Lines

Test lines are a system by which a telephone technician (or phreak) is able to test the conditions on a line, without being physically present at the line. This allows for much more efficient diagnosis of problems than actually having to send out a person to dial numbers from the line every time there is a problem reported. In this way, a fone technician can diagnose a problem on a line without ever actually being physically present at the line.

Test lines are employed by phone companies for a variety of purposes, ranging from taking control of a line to creating a loopback to testing for line overloads to testing lines for high speed transmission quality to whatever. Following are some examples of how test lines are employed, and a description of many types of common test lines.

1000 Hz Test Tone
++++++++++++++++

This is a tone that plays a continuous 1000 Hz tone. Not sure of this is really classified as a test line, but I assume it is.

1004 Hz Test Tone
++++++++++++++++

Once again, never had a use for this.

ANAC (Automatic Number Announcement Circuit) Line
++

This number will read off the number of the fone you are calling from. Somewhat useful if you are trying to ringback a fone that you don't know the number of, or if you are at a payphone.

Digital Audio Test Unit Line
++++++++++++++++++++++++++++

These are the ultimate test lines. They let you monitor the activity of a line, (like listen in...) and that sort of thing. You can also short pairs from these lines. You can put a trace on a line from a DATU (Digital Audio Tests Unit).

Loop Lines
++++++++++

Loop lines are cool. If you call up one end of the loop line, you'll get a tone. If you call up the other end, you will get silence. If both are called at the same time, you can get a connection. Some lines will connect and allows voice transmissions, others block out voice completely. You'll just have to get lucky.

Ringback Lines
++++++++++++++

Ringback lines will call back the number that you placed the call from. Some VMB's are also set to ringback once you have successfully placed a message and hung up the phone, this is rather annoying but they are not really ringback numbers.

Sweep Tones
++++++++++

Sweep tones are designed to check for line loss, or some kind of powered coil that lowers transmission quality, which will make a line unsuitable for high speed transmissions. But, more importantly, can be used to check for infinity transmitter taps. If you hear a clicking while the sweep is being performed, then you probably have a tap on the line you are calling from. Sweeps from frequency 304Hz to 3024Hz.

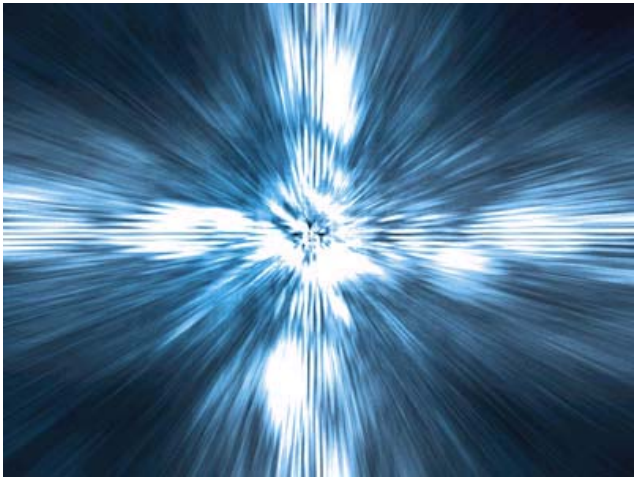
If you think that hand skanning is cool, then go hand skan a million numbers and find some test lines. Otherwise, just search in the net for "phreaking test lines canada" or "phreaking test lines us" to find some hand-skans that phreakers have posted for you.

Hope that this has been an interesting an informative introduction to Test Lines.

If you try any of this, you will get caught and go to jail. Don't do it, its illegal. I know that I have never, ever, ever tried any of this and I never intend to.

^_^

timscott



Building a Ctek Cable

Written By
Scramble45

Brief introduction:

The legendary Ctek cable has been in use sense the OKI 900 came to be originally made by network wizards but no longer manufactured. The cable can only be used with the 900 from what i have been told no moding to the cable can be done without slightly changing the microcontroller. IM currently working on a mod for the 3000 series of OKI phone which have the same compatibilities and will be just as nice as a Ctek cable.

The fine print::

Warning: Making this cable for scanning analog cellular channels is illegal and we at port7alliance recommend not making it for that. Also by making this cable you agree that you alone made the cable because we don't want it used for illegal purposes this cable is only for use to see if it works not for the use of scanning cellular calls. Just and FYI that you take full reasonability for your action and you alone.

Greetz go out to all the nice people in #cellular and Alt.cellular - Special greetz to PoTom for the great plans.

Code For PIC microcontroller of following device available here (http://www.port7alliance.com/Ctek/ctek-hex.txt). - ASM source code is available here (http://www.port7alliance.com/Ctek/ctek.src).

All Software is newer and up to date as much as possible:

Software:

Last Network Wizards Ctek dos distribution (http://www.port7alliance.com/Ctek/dist1300.zip).

SunOS Sparc ctek distribution (http://www.port7alliance.com/Ctek/sunctek.tar.Z)

Network Wizards Ctek Dos "Scaning Version" (http://www.geocities.com/ResearchTriangle/6218/ctek.zip)

Scan1c (Scanning software). (http://www.port7alliance.com/Ctek/scan1c.zip)

4712 mod programer. (http://www.port7alliance.com/Ctek/4712-prg.zip)

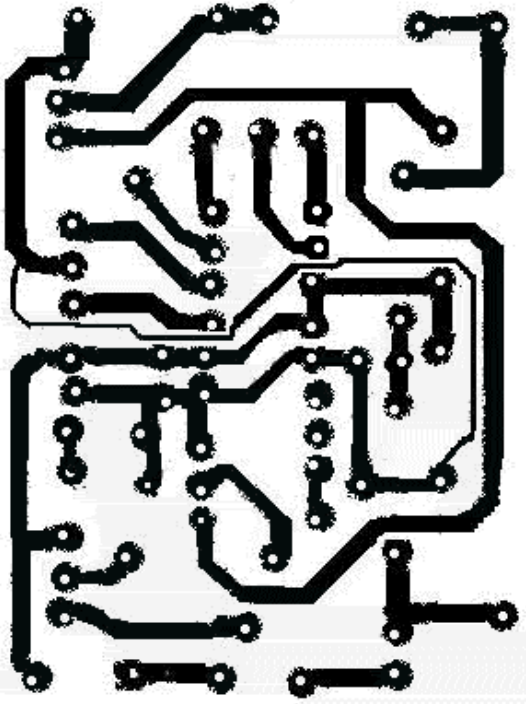
CIAscan. (http://www.port7alliance.com/Ctek/Ciascan.exe)

NW ctek library source code. (http://www.port7alliance.com/Ctek/ctek-src.tgz)

CTEK Protocol FAQ (http://www.port7alliance.com/Ctek/ctekprot.txt)

Where to buy Ctek: www.ebay.com

36 Radical Future



Ctek plans 2:1

Thanks to: me (PoTom)
Mr Ethos , Kyoorius,
ViDiOT , Xtrim,
TvMaN
and everyone in #cellular

Parts list

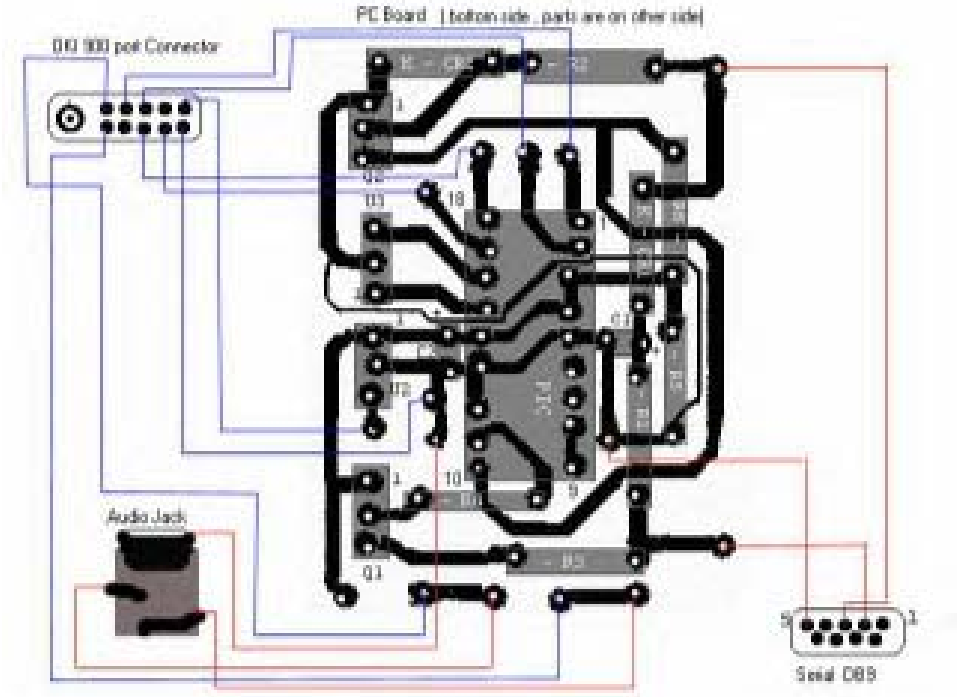
Film resistors:
R1=1.8 kOhm R2=5.6 kOhm
R3=41 Ohm R4,R6=10 kOhm
R5=41 kOhm **all +/- 5%**

Transistors:
Q1=2n2222a
Q2=2n2907a

Rectifiers(diodes):
CR1=1n4004
CR2=1n4002

Capacitors:
C1=10uf 16V (tantalum)
C2=22uf 16V (electrolytic)

Units:
U1(PIC)=pic16c54 (18 dip)
U2=78L05 Voltage regulator (MC78L05ACP)
U3= 4.00mgz ceramic resonator with cap
(digikey X902-ND)



Grief is heard ‘round the world
but not even our own tragedy alerts us

its in the headlines
“America Fights Back”
The hypocrisy goes unnoticed
“we wave the flag of freedom
as we conquer and invade”
replace freedom with a false sense of security
propaganda breeds mindless patriotism

“there should be limits on freedom”
says our president...

and the future will come

the pledge of allegiance
unwritten law
differing opinions
singled out and silenced
1 person will support 5 on social security
but the government keeps their cushy 120k
not caring - homelessness, child abuse
not caring - starving and death in the streets
and we say - it makes America stronger

By Khaos, Inspired by Anthony George

Statements From The Writers

Patience
by Killer

Patience is a form of waiting art. Patience is everywhere and nowhere. Having patience means to be able to tolerate any eagerness. You have patience but it doesn't exist. Once you are really patient you will also realize and change many of things. You will be much more aware of now.

Patient is not an overnight work. It's a lifetime work. From when you were born til' now til' you die, And if such life after death exists, you will continue to be aware of now and be patient.

"Control your patience before you go out of control"

NYC METROCARD SYSTEM

EVERYDAY PEOPLE LIVING IN NEW YORK CITY USE A MAGNETIC STRIP CARD CALLED THE METROCARD TO USE THE CITY'S SUBWAY SYSTEM. VERY LITTLE INFORMATION IS KNOWN ABOUT THE "METROCARD SYSTEM" WITHOUT MAKING ASSUMPTIONS. THEREFORE THE PRODUCERS OF THIS ZINE ALONG WITH SEVERAL COMPUTER ENTHUSIASTS IN NYC WISH TO GAIN AND COLLECT AS MUCH INFORMATION ON THIS SYSTEM AND RELEASE IT TO THE PUBLIC. IF ANYONE ALREADY HAS SOME INFORMATION ON THE SYSTEM AND WISHES TO CONTRIBUTE PLEASE DO SO. HOWEVER, PLEASE KEEP IN MIND THAT THE OBJECT OF THIS PROJECT IS NOT TO CAUSE PHYSICAL, DIGITAL, OR FINANCIAL HARM TO THE MTA BUT ONLY TO GAIN INSIGHT ON HOW SUCH A VAST AND COMPLICATED SYSTEM WORKS. WE CANNOT BE HELD LIABLE FOR ANY OF YOUR ACTIONS