

Helping companies test the security of their information systems

Michael Yaffe
Michael.yaffe@coresecurity.com

Core Security Technologies
www.coresecurity.com

- Networks, Web Applications and IT infrastructure are:
 - More complex
 - More connected to support the extended enterprise of customers, partners, suppliers, prospects, employees and other stakeholders
 - Built with a 'make it work' philosophy prioritized over 'make it secure'
- Attackers are:
 - Organized and persistent
 - Motivated by financial gain, not notoriety
 - Well-funded and very smart
- Increasing pressure from CFOs, legislation and auditors
- So the questions every security professional should ask themselves;
 - What is the risk I am reducing?
 - Is this the highest priority risk?
 - Is this most cost effective way to reduce the risk?

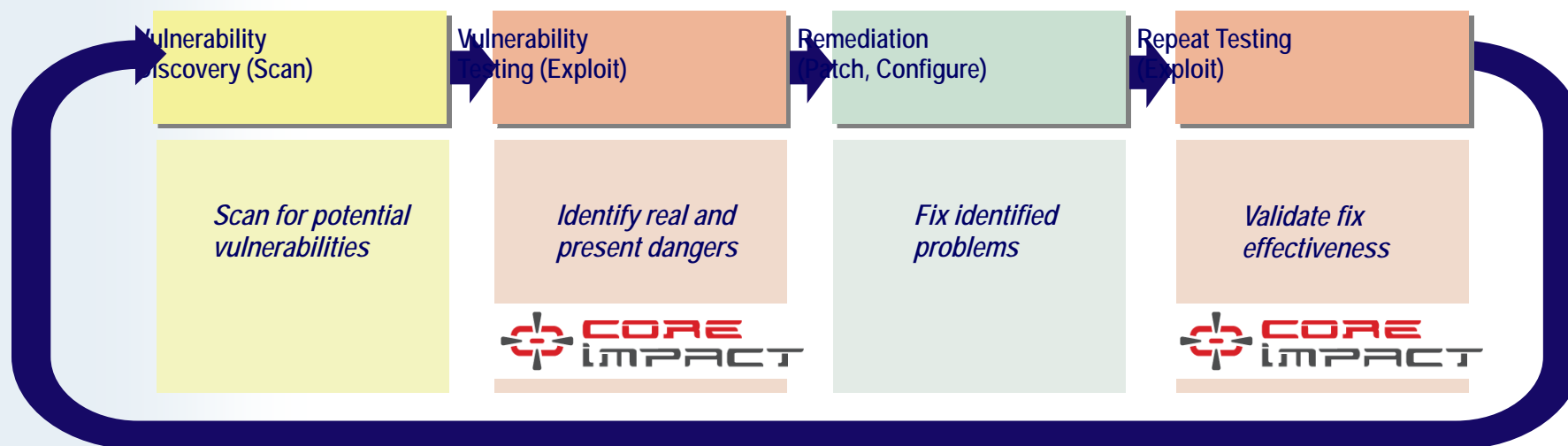
- Network Scanners (i.e. Nessus, Retina, Qualys, etc.) are used to try to identify ***potential*** flaws on your network
- Web Application Scanners (Watchfire, SPI, Cenxic, etc.) identify ***potential*** vulnerabilities (code issues) in applications
 - Gives you entire potential threat universe
- Vulnerability (network and/or web application) scanning does not:
 - Show or *exploit* linkages between information systems and assets
 - Reveal the impact of loss of information assets (only shows the "outer layer" of the onion) such as theft of intellectual property, leakage of internal communications, etc.
- Being 100% patched is unrealistic
 - Patches can break critical applications
 - Money is wasted in dealing with false-positives and unnecessary patches

Where IMPACT Fits In

www.coresecurity.com

CORE IMPACT provides “real-world” security testing

(traditionally the most substantial and challenging aspect of vulnerability management)



Scanning Vendors

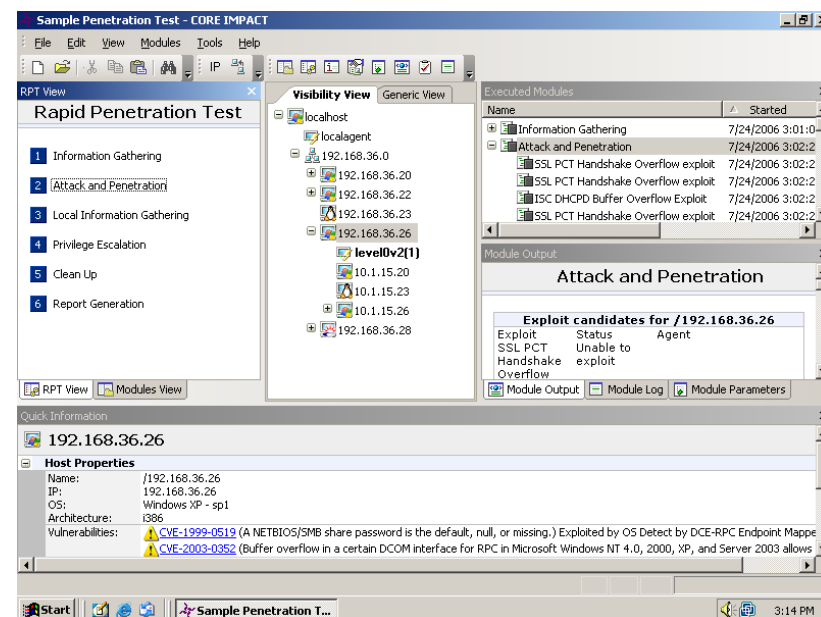
- eEye Retina
- GFI LANGuard
- IBM ISS
- Lumension PatchLink Scan
- NCircle IP360
- Nessus
- Nmap Security Scanner
- Qualys QualysGuard

Patch Management Vendors

- Big Fix Discovery
- Citadel (McAfee)
- Lumension PatchLink Update
- Shavlik
- St. Bernard UpdateEXPERT

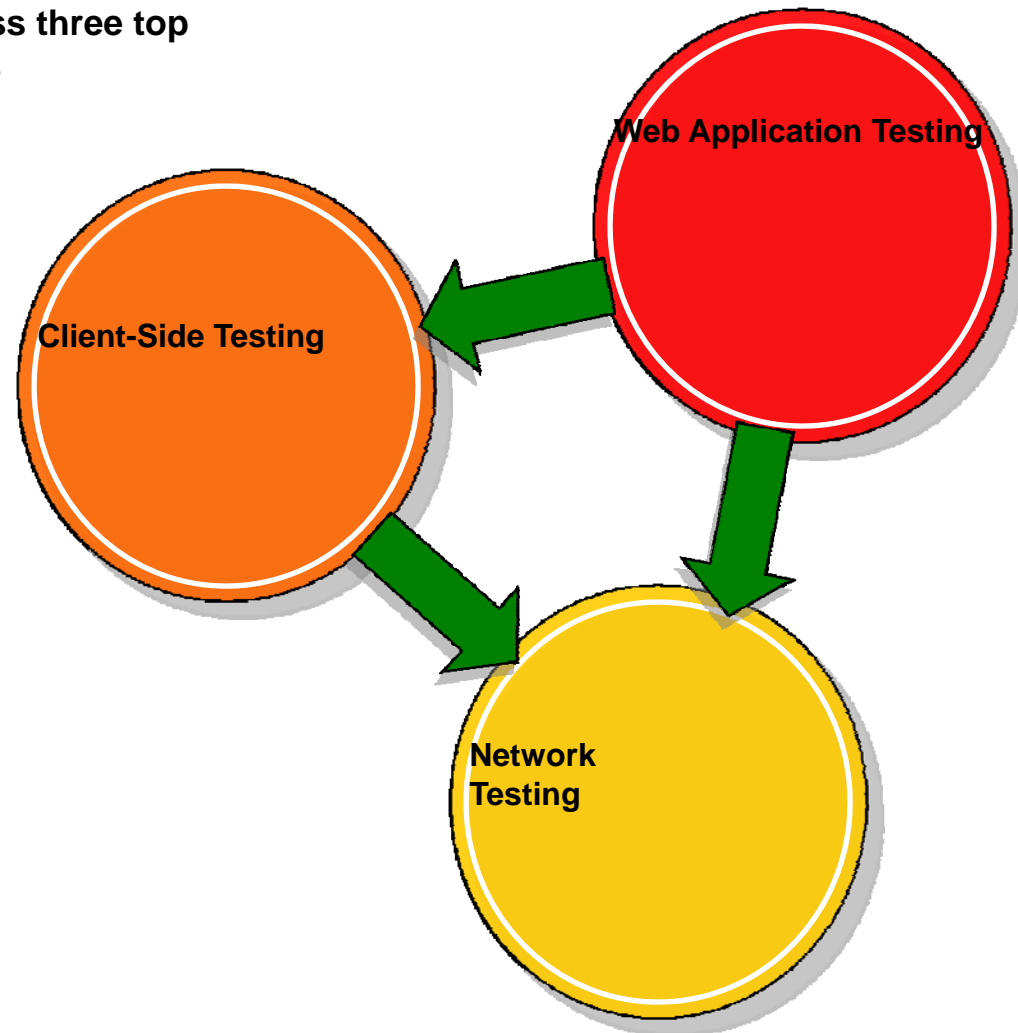
- Penetration Testing – Actively exploits vulnerabilities, evaluating and testing the effectiveness of security solutions by safely launching real-world attacks
 - Looks at your network from the perspective of an attacker
 - Without physically penetrating the host, application or network, there is no way to quantify / qualify an organization's true exposure
- Perform penetration testing against:
 - Servers, patches
 - Web Applications
 - IPS/IDS/Firewalls
 - Client applications/users
- Advantages
 - Enables you to be proactive with informed security decisions - confirm the (non) existence problem
 - Provides efficient, precise, cost-effective remediation information
 - Exploits vulnerabilities and exposes resources that are at risk

- Emulates attacker behavior
 - Launches real-world attacks safely and efficiently, demonstrating exactly what an attacker can do
 - Provides attacks against networks, applications and clients
- Industrializes penetration testing
 - Automates previously manual, expensive process with Core Impact Rapid Penetration Test (RPT)
- Provides important features:
 - Commercial-grade OS exploits
 - Innovative agent technology
 - Powerful user interface
 - Automation of repetitive tasks
 - Complete log of all activities
 - Standard and custom reporting
 - Remediation information



First product to integrate security testing across three top attack avenues, replicating multistaged attacks

- **Databases compromised during Web App testing ...**
 - can be farmed for email addresses and other personal info. to use in IMPACT Client-Side Tests, which assess end-users against social engineering attacks
- **Servers compromised during Web App Testing and end-user workstations compromised during Client-Side Testing ...**
 - can be used as beachheads from which to launch IMPACT Network Tests, which identify and validate OS and services vulnerabilities on backend systems



How Customers Use IMPACT



www.coresecurity.com

- Perform efficient, safe and cost-effective network, web application and client-side penetration testing
- Optimize the vulnerability management process
- Verification of security defenses (e.g., IDS/IPS)
- Prove security compliance with industry and internal regulations (e.g., FDIC, HIPAA, SOX, PCI, etc.)

"Penetration testing that goes beyond simple vulnerability scanning needs to be performed frequently. "

John Pescatore, VP Distinguished Analyst Gartner.

Helping companies test the security of their information systems

Michael Yaffe
Michael.yaffe@coresecurity.com

Core Security Technologies
www.coresecurity.com



A Brief History of Hacking

Dave Shackleford
CTO, Center for Internet Security
dshackleford@cisecurity.org

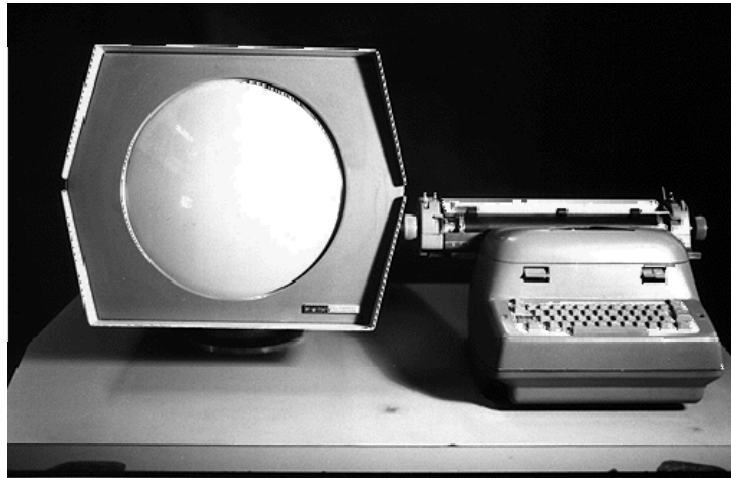


Caveat

- **Is this all 100% accurate?**
 - Ummm...no.
- **Do we have a completely accurate account of hacking and phreaking and whatnot?**
 - Ummm...no.
- **Many different accounts of how things “went down”**
- **Info presented here is based on widely agreed-upon data**
- **On with the show!**

Origin of the term “hacker”

- Started in 1959 with MIT's Tech Model Railroad Club
- Original terminology describes someone who is capable of doing anything with computers and is intellectually curious
- 1972: Alan Kay is quoted as saying “A true hacker is not a group person. He's a person who loves to stay up all night, he and the machine in a love-hate relationship...”**

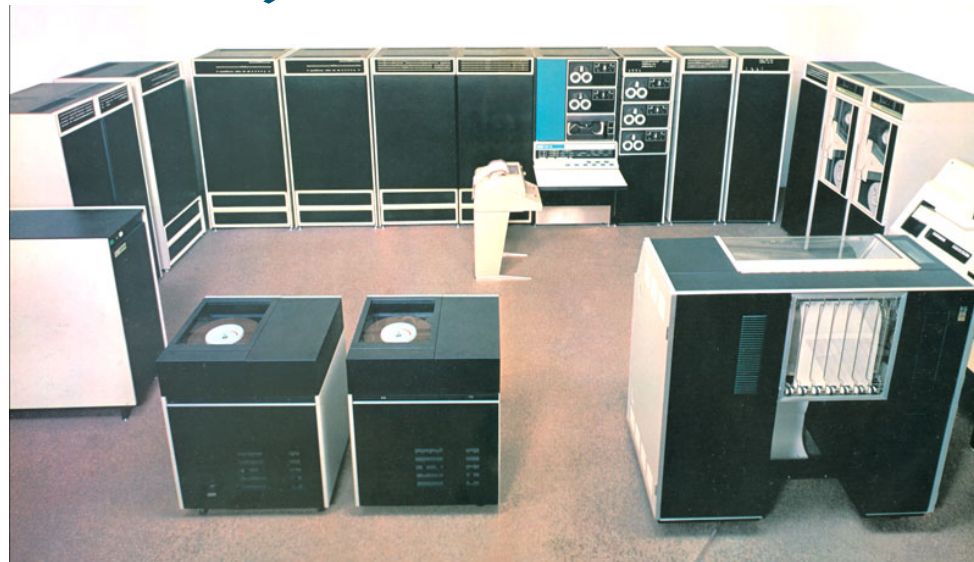


The DEC PDP-1

**Taken from http://en.wikipedia.org/wiki/Hacker_definition_controversy

1967: The MIT Hackers Rebel

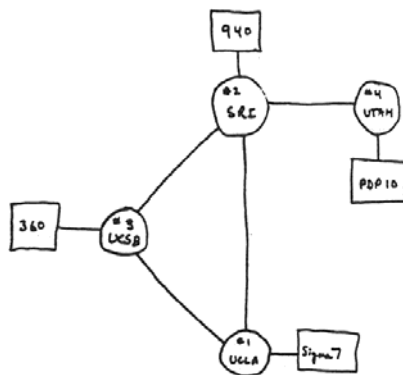
- MIT hackers don't like DEC's OS for the PDP-10
- They write their own, called Incompatible Timesharing System (ITS)
- ITS was written in Assembler (of course!)



The DEC PDP-10

1969-1971: Dawn of the ARPAnet

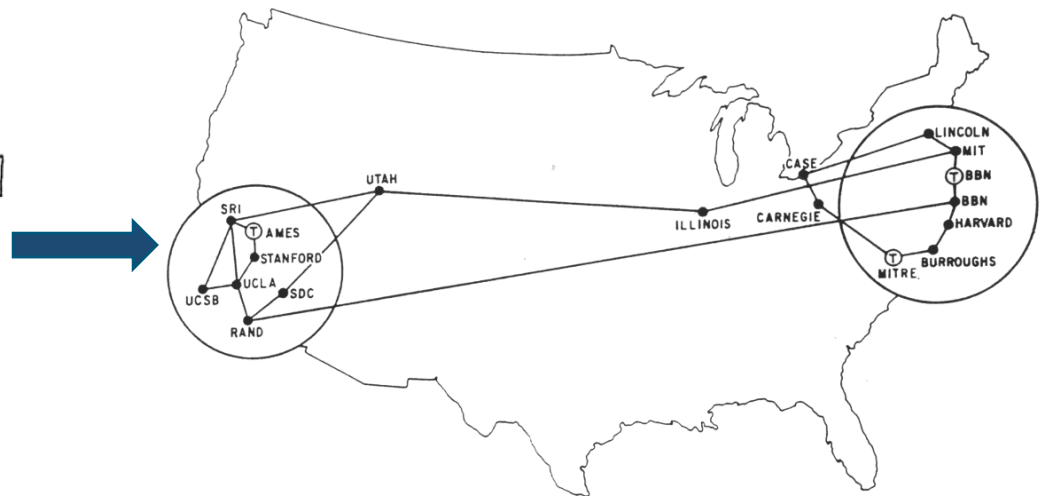
- **Connectivity! Hackers at universities and research institutions could communicate**
- **Almost all early hacker culture discussions started here**



THE ARPA NETWORK

DEC 1969

4 NODES



MAP 4 September 1971

1969-1970: UNIX is Born

***** Obligatory UNIX Slide *** ☺**

- Ken Thompson, at Bell Labs, wrote the Uniplexed Operating and Computing System (UNICS) in 1969 and revised through 1970
- Working with Brian Kernighan and Dennis Ritchie, the code was updated and revised, eventually rewritten in C (1973)
- This quickly became the preferred operating platform for hackers, particularly the later BSD variety



1971: Phreaking



John Draper

- “Phreaks” = Phone + freaks
- People who experiment with public telephone networks and telecommunications gear
- John Draper (aka “Captain Crunch”), along with Joe Engressia (“Joybubbles”) found that free whistles in Cap’n Crunch cereal produced a 2600 Hz tone
- This could be used to reset trunk lines and control phone switches
- The NY Phreaking crew “Group Bell”, consisting of “Evan Doorbell”, “Ben Decibel”, and Neil R. Bell also active
- Captain Crunch’s Web site:
<http://www.webcrunchers.com/crunch/>
- Phreaker Mark Bernay (“The Midnight Skulker”) has an incredible archive of phreaker antics from the 1960s-1980s here:
<http://www.wideweb.com/phonetrips/>



1971: The Rise of the "Blue Box"

- **Esquire Magazine's 10/71 article called "Secrets of the Little Blue Box"**
 - Featured Joybubbles and Captain Crunch
 - Taught the world how to make a full-fledged hacking device to place free phone calls
 - Later, Steve Jobs (aka "Berkeley Blue") and particularly Steve Wozniak (aka "Oak Toebark") would sell these boxes as members of the Homebrew Computer Club
- **Article is online at:**

<http://www.webcrunchers.com/crunch/stories/esq-art.html>



“The Man” is Watching!! Errr...Listening!!



They'll never catch you!

Some people say it's easy to rip off the phone company. Use a phony credit card or someone else's number. Make all the long distance calls you want . . . free. They'll never catch you.

Don't you believe it.

There are some very sorry people who now know different. The fact is: toll fraud is a crime.

Charging calls to phony numbers is a Class A Misdemeanor. Up to one year in jail and a \$1000 fine.

Using an electronic device (i.e. "blue box") is a misdemeanor, too. For out-of-state calls, it's fraud by wire—a Federal offense. Up to five years in jail and a \$1000 fine.

If you're caught, you'll spend some time behind bars until you can raise bail.

If you're convicted, chances are you can kiss your scholarship and your college career good-bye. And your odds are lousy for getting into law school, medical school . . . ever becoming a teacher, or holding a civil service job. The list of deadends is endless.

The phone company is constantly checking for toll fraud. And they get full cooperation from the local authorities.

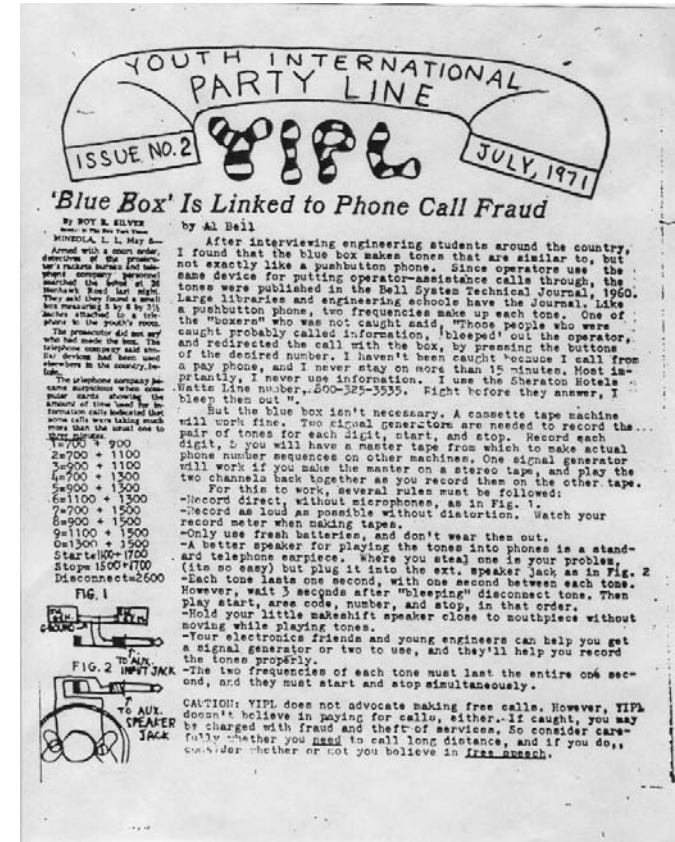
Toll fraud isn't worth it. Once you're caught, you're allowed just one more free call.

For HELP!


**ROCHESTER
TELEPHONE**

1971-1972: The Yippies

- Abbie Hoffman and Al Bell started the Youth International Party Line (YIPL) magazine dedicated to phreaking.
- The name was later changed to Technological Assistance Program (TAP)
- The Vietnam War's Federal surtax on phone service led to "civil disobedience" by phreaking



1972: The "Mute Box" / "Black Box"

- Ramparts magazine published an article in June 1972 entitled "Regulating the Phone Company In Your Home"
- Instructions on how to construct a "mute box" to receive free calls
- The magazine was seized by California police and PacBell officials



Regulating the Phone Company In Your Home

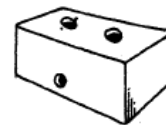
The wizardry of America's Phone Phreaks has received considerable

Quantity	Description
1	0.47 microfarad mylar capacitor at 200 volts
1	5600 ohm resistor one half watt
1	single pole single throw (spst) momentary push-button switch. (The most convenient form of this is a simple doorbell button; it is referred to as such in the following instructions and drawings.)
1	single pole single throw (spst) toggle switch
1	a small plastic utility box large enough to put all of the parts with plenty of room for wiring the parts together; about 1½" x 4" x 2" will do very well. About 20 feet of insulated wire.

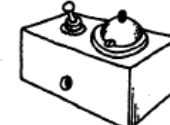
of this esoteric underground long lines, loops and the notorious "Blue Box." The free long distance phone build such a Blue Box, and

come into our hands makes any is in danger of being technically knowledgeable everyone. The document to can change the plug on

THE BOX



WITH HOLES
DRILLED

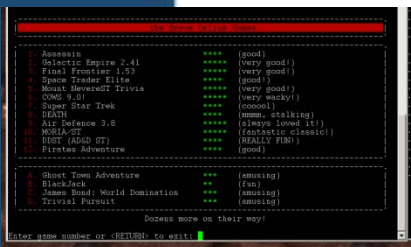


WITH SWITCHES
INSTALLED

Try to remember which part is which since it will help save time during construction. Try to get both switches with

1977-1980: BBS, Usenet & a virus

- The very first bulletin board systems (BBS) came online in 1977 and 1978.
- Names like “Sherwood Forest”, “Catch-22” and others
- The Source and CompuServe started in 1978
- Hackers readily flocked to the BBS realm, and many of the dial-in numbers were guarded closely
- Usenet BBS comes online and becomes the preferred discussion board for hackers
- On October 27, 1980, ARPAnet is shut down from the accidental release of a status message virus



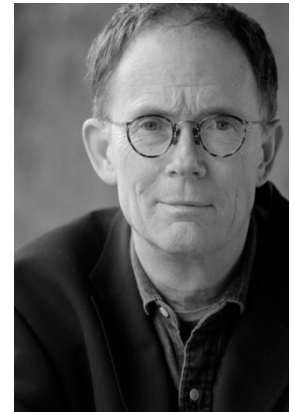
1981-1982: CCC and Mitnick

- **The Chaos Computer Club (CCC) formed in Germany in 1981**
 - Still active today with over 1500 members
 - Every year CCC hosts the Chaos Communications Congress in Europe
- **Kevin Mitnick steals computer manuals from a PacBell switching center in Los Angeles. He's 17, and gets probation.**



1982: More Mitnick, Gibson, and the 414 Gang

- Mitnick breaks into PacBell and TRW and allegedly destroys data
- William Gibson first uses the word “cyberspace”
- The “414 Gang”, Wisconsin phreakers/hackers named for their area code, break into 60 systems at the Sloan-Kettering Cancer Center and Los Alamos Lab systems in New Mexico.



William Gibson

Movie #1: TRON (1982)

- Kevin Flynn, a programmer and hacker, breaks into ENCOM mainframe and battles the Master Control Program (MCP) after being digitized
- Real hacking? NO
- Awesome story? YES



Shackleford Hacker Movie Rating: 4/10

1983: "Hackers at Play", Trojan Horses & Dark Dante

- "The 414's" get busted - all 6 are teenagers, and most are not charged with anything
- This gets lots of media attention, the pinnacle of which is the *Newsweek* cover story "Hackers at Play"
- Ken Thompson, inventor of UNIX, receives the Turing Award and describes the first-ever backdoor "Trojan Horse" in a compiler
- Kevin Poulsen, aka "Dark Dante" breaks into ARPAnet. Since he is only 17, he is not prosecuted.



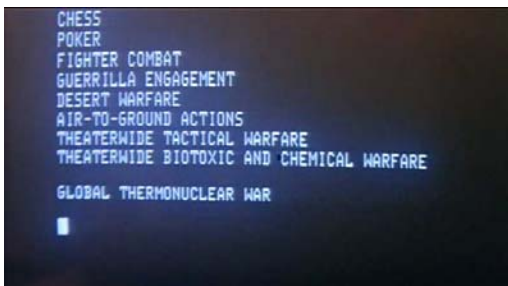
Kevin Poulsen



Ken Thompson

Movie #2: WarGames (1983)

- High-school student David Lightman dials for open modems
- He finds one with games, hacks in, and plays "Global Thermonuclear War"
- He is actually in a NATO supercomputer called WOPR that prepares to launch a real nuclear attack
- David teaches the computer that there's no way to win the game
- Everybody hugs.



Shackleford Hacker Movie Rating: 9/10

1984: The Legion of Doom (LoD)



Erik Bloodaxe

- No, not the enemies of the Superfriends. ☺
- Founded by Lex Luthor (real name unknown)
- Other members included:
 - Erik Bloodaxe (Chris Goggans)
 - The Mentor (Loyd Blankenship)
 - Phiber Optik (Mark Abene)
- Published LoD Technical Journals and furthered hacking knowledge in the underground community
- LoD ran several BBS that were highly coveted by hackers
- Phiber Optik and Erik Bloodaxe had a falling out & Phiber left the group



The Mentor



Phiber Optik

1984: *2600: The Hacker Quarterly*

- Eric Corley, aka Emmanuel Goldstein (taken from George Orwell's novel *1984*), founds 2600.
- Hacking tips and info on the underground hacking scene



Emmanuel Goldstein

More in '84: "The Cracker", Viruses, & Cult of the Dead Cow

- Bill Landreth, aka "The Cracker" is convicted after breaking into GTE and looking at NASA and DoD email
- Fred Cohen first uses the term "computer virus" in his dissertation
- The hacking crew Cult of the Dead Cow (cDc) is formed in Texas



1984: The “Hacker Ethic” * *

- Steven Levy coined this phrase in the book *“Hackers: Heroes of the Computer Revolution”*
- Levy’s principles include:
 - Access to computers — and anything which might teach you something about the way the world works — should be unlimited and total.
 - Always yield to the Hands-on Imperative!
 - All information should be free.
 - Mistrust authority — promote decentralization.
 - Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
 - You can create art and beauty on a computer.
 - Computers can change your life for the better.

****See: http://en.wikipedia.org/wiki/Hackers:_Heroes_of_the_Computer_Revolution**

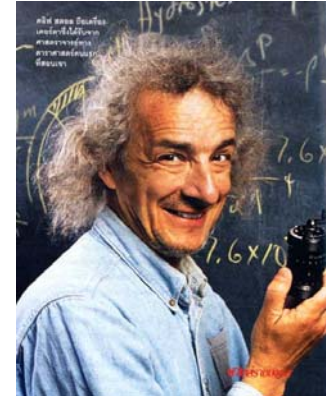
1985: Phrack

- Craig Neidorf, known as "Knight Lightning", and Randy Tischler (aka "Taran King") start publishing another hacker periodical called *Phrack*.
- Posted on BBS, it was all about the *philes* and who could get them.
- One excellent inclusion in the first issue was the phile "How to Make an Acetylene Bomb" by The Clashmaster ☺

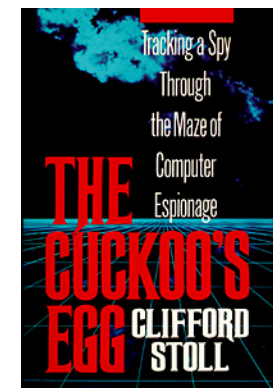


1986: Cliff Stoll's Adventures

- Cliff Stoll, an astronomer at Lawrence Berkeley National Laboratory, investigated a 75-cent accounting error
- Discovered a hacker called "Hunter" who had broken into his systems and was using it to hack into government and military networks.
- First published as "Stalking the Wily Hacker" in 1988
- Cliff published the full account in the New York Times bestseller *The Cuckoo's Egg* in 1989



Cliff Stoll



1986: The Law!



- Based on legislation created in 1984, the Computer Fraud and Abuse Act was officially passed in 1986
- The law did not apply to juveniles, quite a shortcoming at the time
- The law made it a criminal offense to access computers and information in an unauthorized manner
- Causing damage or harm via unauthorized access is also cause for criminal charges

1. Knowingly accessing a computer without authorization in order to obtain national security data
2. Intentionally accessing a computer without authorization to obtain
 - * Information contained in a financial record of a financial institution, or contained in a file of a consumer reporting agency on a consumer.
 - * Information from any department or agency of the United States
 - * Information from any protected computer if the conduct involves an interstate or foreign communication
3. Intentionally accessing without authorization a government computer and affecting the use of the government's operation of the computer.
4. Knowingly accessing a computer with the intent to defraud and there by obtaining anything of value.
5. Knowingly causing the transmission of a program, information, code, or command that causes damage or intentionally accessing a computer without authorization, and as a result of such conduct, causes damage that results in:
 - * Loss to one or more persons during any one-year period aggregating at least \$5,000 in value.
 - * The modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals.
 - * Physical injury to any person.
 - * A threat to public health or safety.
 - * Damage affecting a government computer system
6. Knowingly and with the intent to defraud, trafficking in a password or similar information through which a computer may be accessed without authorization.

More reading: <http://www.usdoj.gov/criminal/cybercrime/ccmanual/01ccma.pdf>

1986: The Hacker Manifesto & NetSweep

- LoD's "The Mentor" is arrested, and shortly thereafter pens the most famous writing to characterize the hacker culture
- Published in Phrack magazine**

```
Yes, I am a criminal.  
My crime is that of curiosity.  
My crime is that of judging people by what they say and  
think, not what they look like.  
My crime is that of outsmarting you, something that you  
will never forgive me for.  
I am a hacker, and this is my manifesto.  
You may stop this individual, but you can't stop us all...  
after all, we're all alike.  
  
+++The Mentor+++
```

- Pete Shipley writes NetSweep, the first network security scanner

**<http://www.phrack.org/archives/7/P07-03>

1988: The Morris Worm

```
/* Strategy 0, look through
/etc/hosts.equiv, and /.rhost for
new hosts */
```

```
strat_0() /* 0x5da4 */ { FILE
*hosteq; char scanbuf[512]; char
fwd_buf[256]; char *fwd_host; char
getbuf[256]; struct passwd *pwent;
char local[20]; struct usr *user;
struct hst *host; /* 1048 */ int
check_other_cnt; /* 1052 */ static
struct usr *user_list = NULL;
hosteq =
fopen(XS("/etc/hosts.equiv"),
XS("r")); if (hosteq != NULL) { /*
292 */ while (fscanf(hosteq,
XS("%s.100s"), scanbuf)) { host =
h_name2host(scanbuf, 0); if (host
== 0) { host =
h_name2host(scanbuf, 1);
getaddr(host); } if (host->o48[0]
== 0) /* 158 */ continue; host->flag
|= 8; } fclose(hosteq); /* 280 */ }
hosteq = fopen(XS("/.rhosts"),
XS("r")); if (hosteq != NULL) { /*
516 */ while (fgets(getbuf,
sizeof(getbuf), hosteq)) { /* 344,504
*/ if (sscanf(getbuf, XS("%s"),
scanbuf) != 1) continue; host =
h_name2host(scanbuf, 0); while
(host == 0) { /* 436, 474 */ host =
h_name2host(scanbuf, 1);
getaddr(host); } if (host->o48[0]
== 0) continue; host->flag |= 8; }
fclose(hosteq); }
```

- Robert Tappan Morris, a Cornell grad student, launched the worm from MIT in November 1988
- Amazing first effort: it was multi-exploit!
 - Finger
 - Sendmail
 - Rsh/rexec
 - Passwords
- Throttled many UNIX systems
- Estimated to have crippled 10% of the Internet (6,000 systems)
- He was sentenced to 3 years probation, fines, and community service



Robert Tappan Morris

1988: Mitnick and Poulsen Updates

- **Kevin Mitnick is arrested after infiltrating DEC networks and supposedly causing damage and stealing data**
 - He is convicted the next year and serves a year in jail
- **Kevin Poulsen goes on the run after the FBI starts investigating him for phone tampering**
 - He rigged a radio show contest and won a Porsche while on the run
 - It's much easier to be the 102nd caller when you control the phone lines



1989-1990: Cliff Stoll Take 2 & MoD

- **Cliff's work in tracking the movements of the German hacker pay off**
 - Markus Hess is Stoll's hacker, and goes to trial in Germany
 - 3 other hackers are also implicated in an espionage scheme to sell OS source code to the KGB
- **After parting ways with LoD, Phiber Optik joins Masters of Deception with other New York hackers Acid Phreak, HAC, and Scorpion**
 - They soon become one of the most revered hacking groups ever known



C:\NYFO\920563\EXH19.TIF
TOP: SCORPION, THE WING, ACID PHREAK,
THE SEEKER, HAC
BOTTOM: CORRUPT, RED KNIGHT, LORD MICRO,
PHIBER OPTIK

1990-1992: EFF, Sundevil, and MoD

- The Electronic Frontier Foundation was founded in 1990 by Mitch Kapor, John Gilmore and John Perry Barlow
 - One goal was to help defend those accused of criminal hacking
- The US Secret Service and other law enforcement undertake Operation Sundevil, that targeted BBS, Phrack, and other hacker activity
- The US government uses wiretaps for the first time to arrest and indict five members of MoD for breaking into TRW, the NSA, and other systems



Also: In 1991, both PGP and the first version of Linux are released

1991: An Evening With Berferd

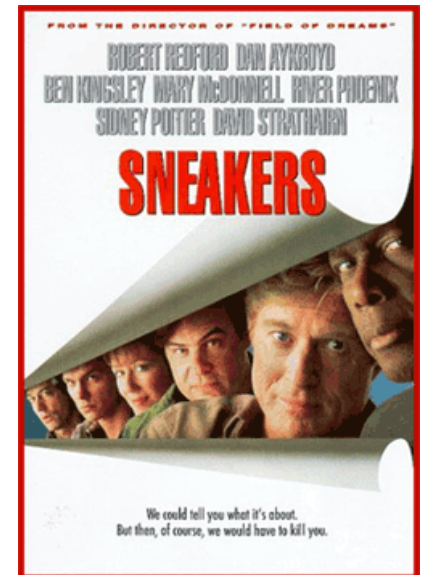
- Bill Cheswick, a well-known security guru begins tracking a hacker at AT&T Bell Labs
- He had set up a simple honeypot with fake services, logging, and a chroot jail
- “Berferd” kept logging in from systems at Stanford
- The hacks were coming from the Netherlands, and Weitse Venema ended up tracking “Berferd” down.



Bill Cheswick

Movie #3: Sneakers (1992)

- Marty & Cosmo are hackers in the 1960's.
- Cosmo is arrested
- Marty leads a tiger team 30 years later to retrieve a secret "black box" designed by a mathematician, thinking he's working for the NSA
- He ends up handing over the box to Cosmo, who is now *bad*
- Shenanigans ensue to retrieve the box, which can bypass major cryptosystems
- Marty gets the box back
- Everybody hugs.



Shackleford Hacker Movie Rating: 8/10

1993: DefCon!




- Started by Jeff Moss (aka “Dark Tangent”), the Las Vegas gathering was supposed to be a farewell party to “Platinum Net” BBS (since the Web was now online)
- The name? “DEF” is #3 on the phone
 - David Lightman also chooses to nuke Las Vegas in the movie WarGames
- Still going strong in 2008



<http://www.defcon.org/html/links/dc-faq/dc-faq.html>

An Aside on DefCon: All in Good Fun

JUL-03-2001 03:03 702 796 3354 P.01



ALEXIS PARK
RESORT & SPA • LAS VEGAS

July 1, 2001
ATTN: Department Heads

Rules for Alexis Park staff during DEFCON Event:

Before and during the event:

- Disable and conceal all motorized carts (golf and bicycle).
- Secure and maintain closure of all fitness and salon areas.
- Wear all keys and access cards on a lanyard around your neck.
- Any request for room access must be approved by two managers.
- Harass NO guest, report any incidents to a manager on duty.
- If you are not scheduled to work, you may not attend the event.

Things to report:

- Drugs and/or weapons of any kind.
- Deceased or dismembered guests.
- Farm animals.
- Missing payphones or ATM machine.
- Additional payphones or ATM machines.
- Unauthorized connections to outdoor PBX telephones and cable TV system.
- Dislocated room doors, windows, stairs, walls.
- Fire.

Acceptable during this event ONLY:

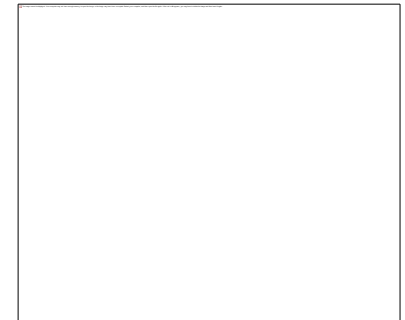
- Any guests not sleeping in a room.
- Fountains and pools functioning with foreign dyes or bubbles.
- Underage possession of alcohol and/or smoking.
- Debauchery and/or libation.

Thank you,
Alexis Park Management

1993: Bugtraq

- Bugtraq was founded by Scott Chasin to announce computer vulnerabilities
- This marked the early days of the full disclosure movement
- The list was not moderated at first, but moderation began in 1995
- Aleph One was the first moderator
- Taken over by SecurityFocus in 1999
 - SF was bought by Symantec, which many in the community did not like
 - The Full Disclosure list began shortly thereafter

Bug Traq



Elias Levy ("Aleph One")

1994: The Famed Mitnick Attack

- Kevin Mitnick breaks into Tsutomu Shimomura's personal network on Christmas Day
- Cool attack! IP Spoofing, trust exploitation, sequence number guessing...
 - ...but he gets busted.
Tsutomu is, like, um, smart and stuff, and decides to track Kevin down.
- Tsutomu, with the FBI, locates Kevin and they arrest him next year. Doh!
- The book "Takedown" chronicles this effort
- It is generally accepted that many others besides Kevin had infiltrated Tsutomu's systems, as well.

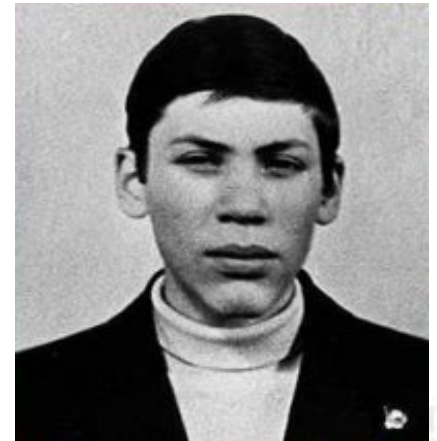


Tsutomu Shimomura

1994: CitiBank

- Russian hacker Vladimir Levin hacks into Citibank's cash management system
- He steals \$10 million!
- Citibank manages to recover all but \$400k
- Vlad is arrested in 1995, sentenced to 3 years in prison and \$240k in fines

The Citibank logo, featuring a red arc above the word "citibank" in a blue, sans-serif font.



Vladimir Levin

1995: Mitnick goes to jail, Black Baron goes to jail, and...SATAN?

- Kevin Mitnick is arrested in February on a number of charges, primarily stealing 20,000 credit card numbers
- Christopher Pile, aka "Black Baron" is the first person to go to jail for writing the *SMEG.Pathogen* and *SMEG.Queeg* viruses, as well as the *SMEG* polymorphic engine.
- Dan Farmer and Wietse Venema write the first well-known network vulnerability scanner, SATAN (Security Analysis Tool for Auditing Networks)



Movie #4: The Net (1995)

- Angela Bennet is a software beta tester who is given a disk with a curious program
- While in Mexico on vacation, she is accosted for the disk and escapes
- While re-entering the country, she learns her identity has been altered (she is now a prostitute with drug offenses).
- Bad people want the program - Angela must get evidence to exonerate herself
- She does.
- Bad guys die.
- No hugs this time.

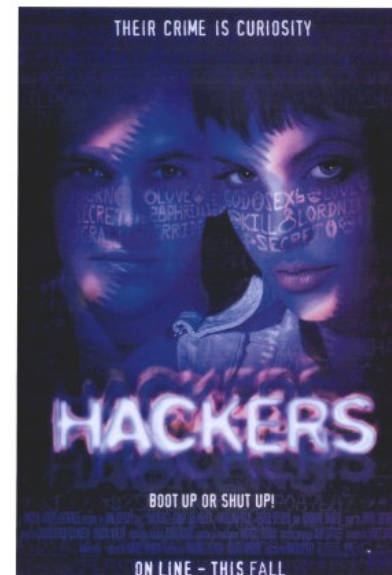


Shackleford Hacker Movie Rating: 2/10

Movie #5: Hackers (1995)

Hack the Gibson!

- Dade hacks
- Dade moves to New York and meets a hot chick and other hackers
- Joey hacks into a system and gets a file he shouldn't have
- Evil security weenie "The Plague" frames the crew so that his "DaVinci Virus" won't be discovered
- Hacker army comes to the rescue
- Dade goes on to wed Angelina Jolie in real life, so he's the big winner. 😊



Shackleford Hacker Movie Rating: 7/10

1996: Smashing the Stack

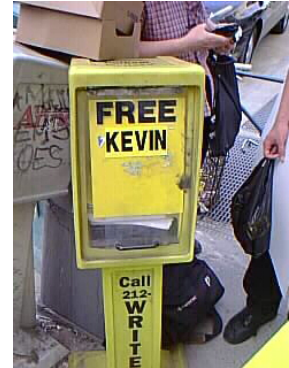
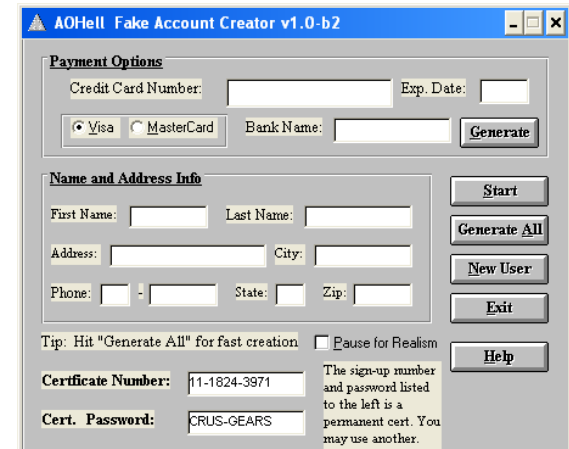
- The still-relevant paper by Aleph One called “Smashing the Stack for Fun and Profit” is published in Phrack Magazine #49
- Describes the fundamentals of buffer overflows

``smash the stack`` [C programming] n. On many C implementations it is possible to corrupt the execution stack by writing past the end of an array declared auto in a routine. Code that does this is said to smash the stack, and can cause return from the routine to jump to a random address. This can produce some of the most insidious data-dependent bugs known to mankind. Variants include trash the stack, scribble the stack, mangle the stack; the term mung the stack is not used, as this is never done intentionally. See spam; see also alias bug, fandango on core, memory leak, precedence lossage, overrun screw.

Check it out here: <http://www.phrack.org/issues.html?issue=49&id=14#article>

1996-1997: Free Kevin! And More...

- The hacker underground rallies to free Kevin Mitnick, who actually stays imprisoned for 4+ years
- The InterNIC domain registry operated by Network Solutions is hacked by rival AlterNIC - queries to Internic are routed to AlterNIC instead.
- AOHell becomes popular, allowing script kiddiez to hack AOL with no skillz.

AOHell Fake Account Creator v1.0-b2

Payment Options

Credit Card Number: Exp. Date:

☒ Visa ☐ MasterCard Bank Name: **Generate**

Name and Address Info

First Name: Last Name:

Address: City:

Phone: - State: Zip:

Start
Generate All
New User
Exit
Help

Tip: Hit "Generate All" for fast creation ☐ Pause for Realism

Certificate Number: 11-1824-3971

Cert. Password: CRUS-GEARS

The sign-up number and password listed to the left is a permanent cert. You may use another.

1998: Solar Sunrise

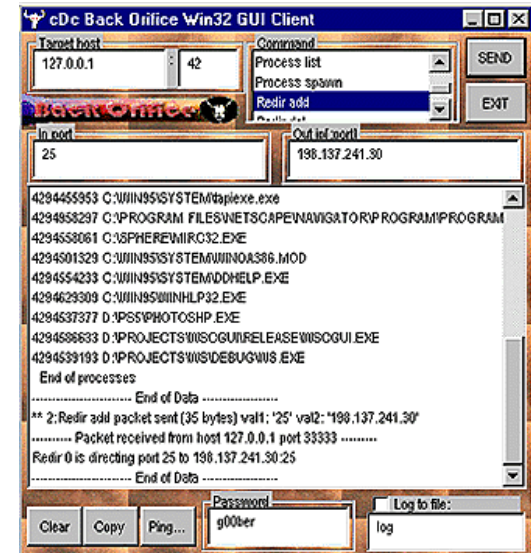
- Houston, we have a problem
- In February, DoD systems and networks were systematically attacked, as were those at MIT
- US was preparing for possible military action against Iraq
- Attacks seemed to come from Israel, France, Germany, etc.
- Two California high school students were apprehended
- Their mentor was The Analyzer, an Israeli named Ehud Tenebaum



The Analyzer

1998: Back Orifice

- cDc releases BO at DefCon this year
- BO is an incredibly full-featured Trojan horse and remote control program written by Sir Dystic
- BO server includes:
 - System/file control
 - Process/network control
 - Packet & Application Redirection
 - Sniffers
 - Plugins



1998: CIH, NYT, L0pht, and a death sentence!

- The CIH (aka Chernobyl) virus corrupts the BIOS on systems, proving viruses can indeed be destructive
- The New York Times Web site is defaced by the group “Hacking for Girlies” to protest Kevin Mitnick’s imprisonment and the book “Takedown”
- The L0pht group testifies before Congress that it could disable the Internet in 30 minutes
- Hao Jinglong and Hao Jingwen (twin brothers) are sentenced to death by a court in China for breaking into a bank computer network and stealing 720,000 yuan (\$87,000)



The L0pht boys, from left: Silicosis, Brian Oblivion, John Tan, Mudge, Kingpin (standing), Space Rogue (front), Weld Pond and Dildog.

1999: The Legions of the Underground (LoD) Hullabaloo

- In December 1998, someone from the LoD declares cyberwar on Iraq and China
- The stated intent is to draw attention to human rights abuses in these countries
- The majority of the group comes out to disavow this, with claims of mistaken identities and so on
- Phrack, 2600, cDc, L0pht, and CCC members all speak out against this

We - the undersigned - strongly oppose any attempt to use the power of hacking to threaten or destroy the information infrastructure of a country, for any reason. Declaring "war" against a country is the most irresponsible thing a hacker group could do. This has nothing to do with hacktivism or hacker ethics and is nothing a hacker could be proud of.

Frank Rieger of the CCC said, "Many hacker groups don't have a problem with Web hacks that raise public awareness about human rights violations. But we are very sensitive to people damaging networks and critical systems in repressive regimes or anywhere else. The police and intelligence communities regard hacking as seditious. It is quite possible now that hackers - not only in totalitarian states - could be jailed or executed as 'cyberterrorists' for the slightest infraction of the law."

See: <http://www.cultdeadcow.com/news/statement19990107.php>



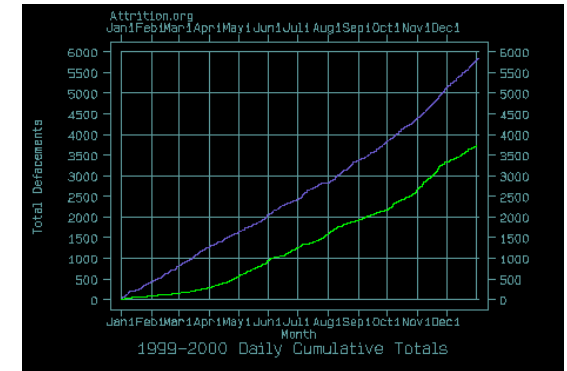
- **David L. Smith releases the Melissa virus, which wreaks havoc all over the place**
 - Originally released on the alt.sex newsgroup
- **The virus infects files and sends mass emails**
- **Smith is arrested, convicted, sentenced to 20 months in jail and \$5k in fines**
- **Peter Shipley invents automated wardriving* ***



Earliest citation courtesy Carole Fennelly: <http://www.wordspy.com/words/wardriving.asp>

1999: Attrition.org

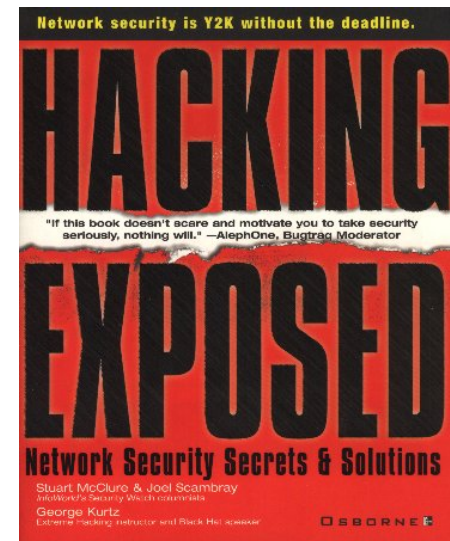
- The site chronicles hacks, Web site defacements in particular
- The site is a “hobby site”, a volunteer effort by a group that includes Jericho, Lyger, Cancer Omega, and others
- The site currently has a Data Loss archive available as well



Year	Total
1995	5
1996	20
1997	39
1998	245
1999	3746
2000	5822
2001	5315
Grand Total	15203

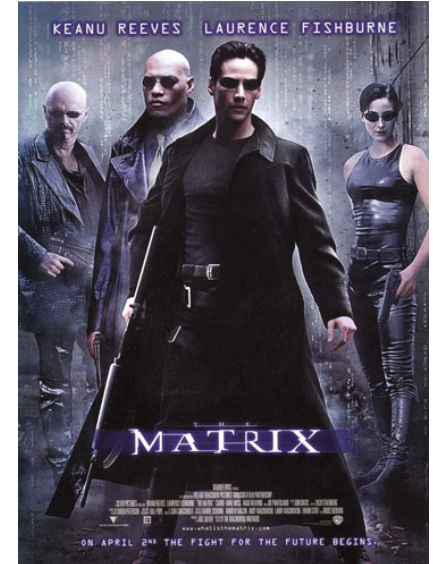
1999: "Hacking Exposed"

- In 1999, the first edition of "Hacking Exposed" was released
 - Authored by folks at Foundstone - Stuart McClure, Joel Scambray, and George Kurtz
- This was pretty frightening for a lot of people
- This book was also well-written and organized, much more so than any others prior to it.



Movie #6: The Matrix (1999)

- Whoa.
- Neo is a programmer by day, hacker at night
- He is contacted by Morpheus, a well-known hacker
- He meets up with Trinity, Morpheus, and their crew
- Our world is an illusion - we're all organic batteries
- Neo is The One, he'll save us all - he fights back against the agents and WINS.
- Whoa.



Shackleford Hacker Movie Rating: 8/10

2000: DDoS, Microsoft is hacked, and ILOVEYOU

- Some of the most high-profile Web sites in the world are attacked by a DDoS (Amazon, Yahoo, and eBay to name a few)
- Microsoft admits that source code for new and upcoming products have been stolen in a successful hack on their network
- The ILOVEYOU virus is the most rapid propagation of malware the world has ever seen (est. 45 million users in one day)

– Also deletes files and changes Registry settings

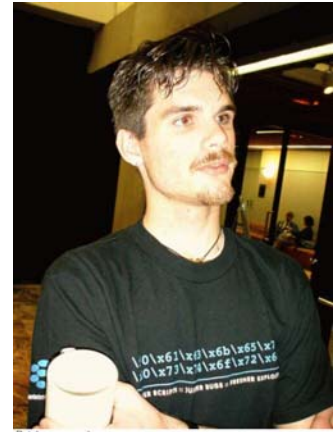
Date	Subject
05/05/2000	conference
05/05/2000	Re: applicat
05/05/2000	ILOVEYOU
05/05/2000	ILOVEYOU



Un e-mail con el virus ILOVEYOU en todo su esplendor.

2000: RFP and RFPolicy

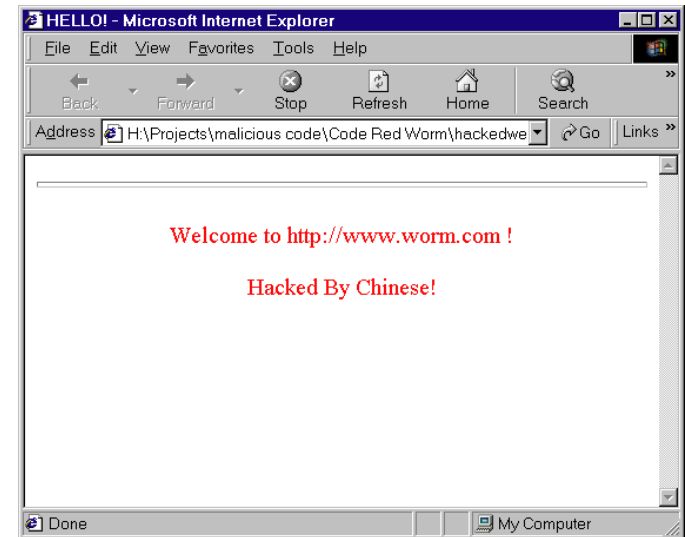
- Rain Forest Puppy (RFP) is a well-known hacker who found a number of significant vulnerabilities and wrote the Whisker library and tool for assessing Web app vulnerabilities
- In June 2000, RFP released a suggested protocol for vendors and security researchers to work together
- RFPolicy defines:
 - The involved parties
 - How long after contact is made before an issue is disclosed
 - How each party should ideally behave
- Found at: <http://www.wiretrip.net/rfp/policy.html>



RFP

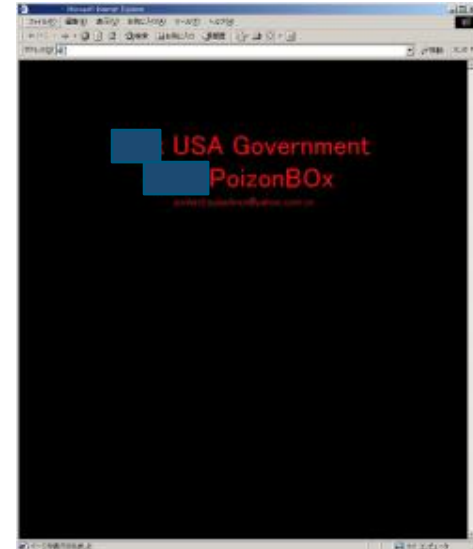
2001: Malware-o-rama

- **Code Red in July**
 - Major analysis done by eEye Digital Security
 - Exploited IIS Web server vulnerabilities
 - Defaced Web sites
- **Code Red II in August**
- **Nimda in September**
 - Email infection
 - Open shares infection
 - IIS ../ vulnerabilities
 - Compromised site browsing



2001: Microsoft & DNS, Sadmind, & Nikto

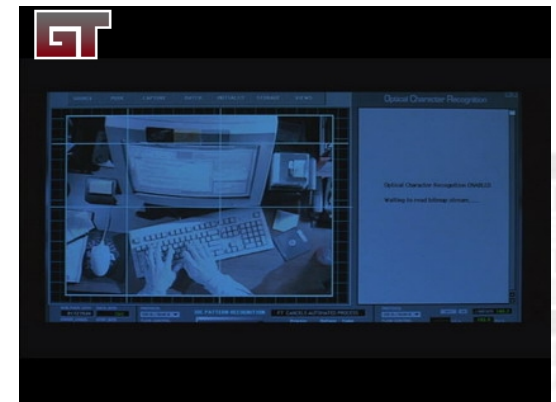
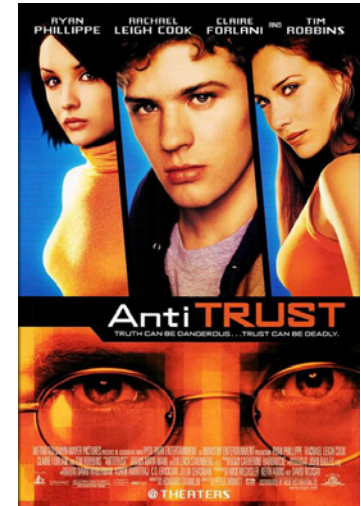
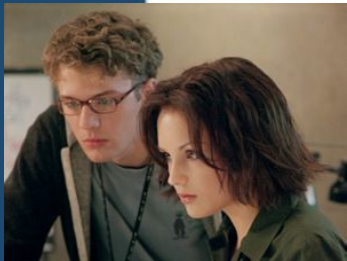
- Microsoft's DNS servers are hammered with DoS attacks which effectively shuts down their sites.
- Even more disturbing: The first true multi-platform worm is seen in the wild
 - Sadmind can infect Sun Solaris and Microsoft IIS
 - Believed to be political retaliation for the "US Spy Plane Incident" **
- Sullo released Nikto, a web application security scanner in December
 - Leveraging libWhisker, this quickly became an industry standard



**See <http://attrition.org/security/commentary/cn-us-war.html>

Movie #7: Antitrust (2001)

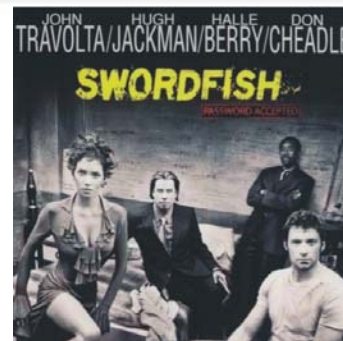
- A direct revolt against the Microsoft animated paper clip.
- OK, not really.
- Milo the programming whiz takes a job with BMFSC (Big ... Software Co.)
- Milo discovers that Winston, evil CEO of NURV, is ummm...evil?
- Wahoo! It's a race to save/destroy the day!
- Somehow Ryan Phillippe gets multiple hot chicks to pay attention to him
- Massive cheese factor



Shackleford Hacker Movie Rating: 2/10

Movie #8: Swordfish (2001)

- Dang that Hugh Jackman is sexy.
- Stanley Jobson used to hack
- He got caught, his life is messed up
- Hot chick and super-persuasive goatee dude offer lots o' \$\$ to hack into the government and steal a slush fund
- The money will fund an underground anti-terrorist movement
- Stanley gets the \$\$, John Travolta gets the \$\$ AND the girl



Shackleford Hacker Movie Rating: 3/10

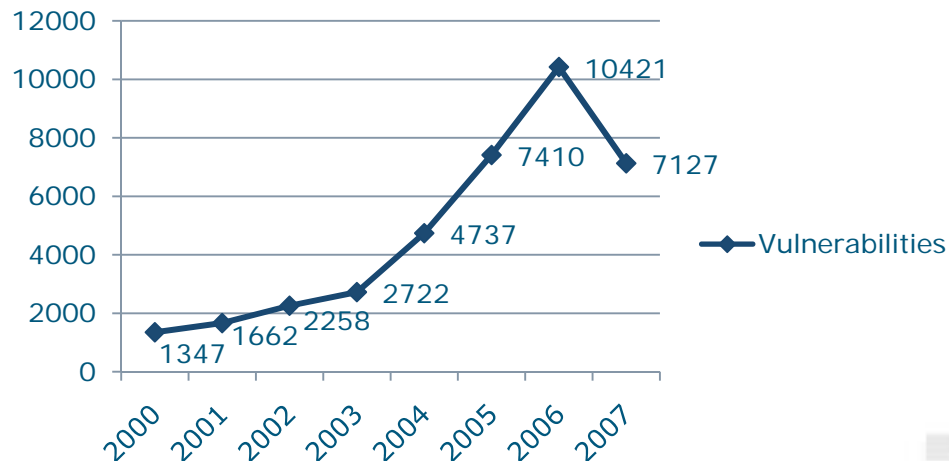
Major events in 2002-2004

- Microsoft announces its Trustworthy Computing Initiative. A little late, but OK.
- The first really BIG attack on the 13 root DNS servers occurs (2002)
- OpenSSH gets Trojaned. Ugh.
- Microsoft announced a \$5 million reward fund for help in tracking down hackers targeting MS software.
- SQL Slammer wreaked havoc.
- Witty Worm targets ISS software

2004: OSVDB

- The Open Source Vulnerability Database opened to the public in March 2004
- From the “About” page**:
“The goal of the project is to provide accurate, detailed, current, and unbiased technical information on security vulnerabilities”

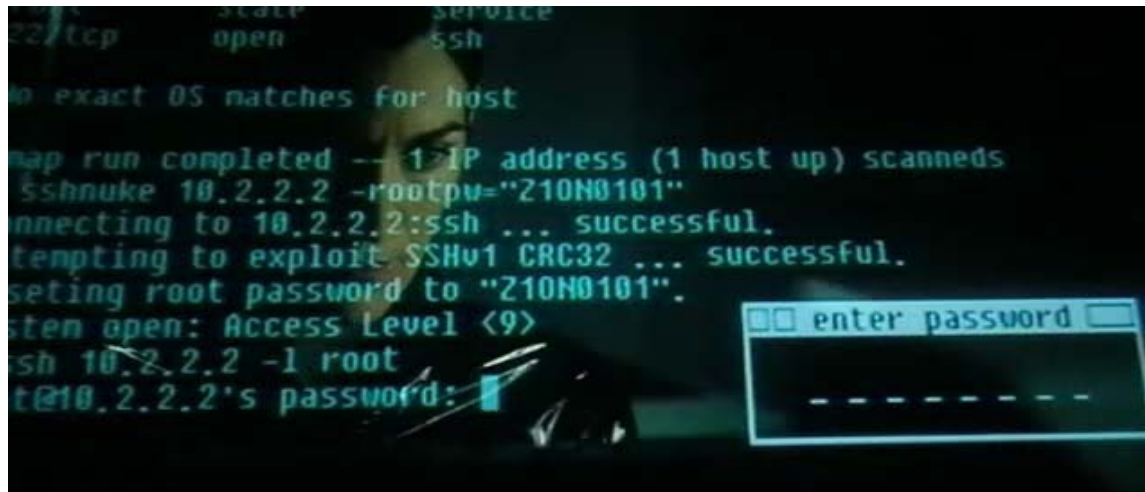
Vulnerabilities per Year



**<http://osvdb.org/about>

Movie #9: The Matrix Reloaded (2003)

- We all know this wasn't as good as the first one. We won't even mention the third one.
- 250,000 Sentinels are drilling to Zion.
- Neo must find the Keymaker to reach the Source to talk to the Architect to figure out how to save Zion to fulfill the prophecy to...
- Yeah, it got a little hokey toward the end.
- But that Nmap move by Trinity to set up sshnuke? Priceless.



Shackleford Hacker Movie Rating: 9/10

Another “Matrix Reloaded” Shot

```

* Welcome to CityPower Grid Rerouting *
Authorized Users only!
New users MUST notify Sys/Ops.

login:

# nmap -v -sS -O 10.2.2.2
# sshnuke 10.2.2.2 -rootpw="210N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Resetting root password to "210N0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password:
RRF CONTROL> disable grid nodes 21 - 48
  
```

Major events in 2005-Present

- ChoicePoint introduces us to the concept of large-scale personal data loss. And fraud.
- Titan Rain is the name given by the US government for a series of incidents reportedly by Chinese hackers
- Estonia is largely taken offline by a disgruntled group of Russian hackers.
- The Storm Worm incorporates Trojans, social engineering, botnets, and this nasty little thing called *server-side polymorphism*.
- MySpace gets hacked. A lot.

2006: The Story of Todd Shriber

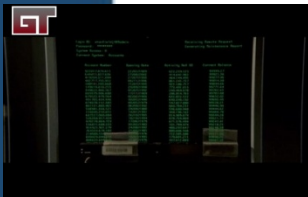
- Todd contacts folks at attrition.org to hire a hacker
- He needs to change a few college grades
- Jericho and Lyger lead Todd to believe they're game, which they're not
- Todd falls for it - he is not a bright bulb
- The squirrels didn't give it away, Todd?
- Oh, and Todd turns out to be a congressional aide. Duh!



Read the whole thing here: <http://www.attrition.org/postal/z/033/0871.html>
Get the news story here: <http://www.networkworld.com/community/?q=node/9999>

Movie #10: Firewall (2006)

- Jack Stanfield runs security at a bank
- He knows what's UP - he can "blackhole" intruders with a quick "rule to the IPS" (looks kinda like a Cisco ACL to me)
- His family is kidnapped
- The evildoers want Jack to break into the bank and get \$\$\$.
- Jack foils the plan
- Everybody hugs.
- This movie SUCKED - the iPod action is hilarious



Shackleford Hacker Movie Rating: 1/10

Trends & Things On the Way

- More Web app attacks
- More data theft incidents
- More multi-faceted malware, particularly bots
- More criminal activity - there's gold in them thar hills!
- More electronic warfare incidents - some we'll hear about, many we won't

Hacking Goes Mainstream

- Hacking is no longer just an underground activity
- There's money in security, and hacking is no different
 - Ethical hackers-for-hire
 - Penetration testing
- **Many of the best-known hackers are somewhat mainstream now:**
 - Kevin Mitnick owns Mitnick Security Consulting, LLC
 - Kevin Poulsen writes for WIRED
 - Marc Maiffrett founded eEye and now consults
 - Etc.

A Final Thought

- Think about who is really pushing the envelope in technology
- Hackers are hackers are hackers, and without them, we wouldn't have ½ the technologies we have now
- The motives have changed - people are in it for the money.
- Criminals work together and share info! That's a major reason they are ahead.
- You can make a difference - remember the integrity and camaraderie of the early hackers
- And no, just going to your local ISSA meeting does NOT cut it. 😊

Need a kick in the nether-region? Read: <http://www.nmrc.org/pub/report/sn-dc-2003.html>