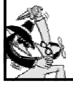
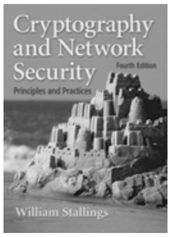
Computer & Network Security Lecture 1

- •Mechanics
- •Are we at risk?
- •Risk assessment
- •Viruses/malware



CNS 06

- Are you in the right class?
- Tom Dunigan dunigan@cs.utk.edu
  - –Office hours: by appointment or before/after class
  - –TA A. J. Wright ajw@utk.edu
- Meet here, each Tuesday 5:05 - 7:45
- Text
  - –errata



CNS Lecture 1 - 2

Class mechanics

Prerequisites
- C/make programming
- UNIX familiarity
- Web/email/CS account access
- Postscript/pdf viewer

Grading	CS494	CS594
• [Assignments:]	50%	40%
• [Midterm:]	20%	20%
• [Final Exam:]	30%	20% paper 20%

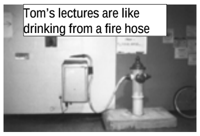
CNS Lecture 1 - 3

Objectives

book smarts & street smarts

- understand computing vulnerabilities
- understand tools and techniques for developing secure applications and practicing safe computing

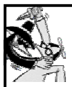
method: study
- risks and countermeasures
- common attacks
- cryptography principles
- applied cryptography



Tom's lectures are like drinking from a fire hose

method: do
- practice secure computing
- develop secure software
- think like a hacker

CNS Lecture 1 - 4



TO DO list ...

Attacks & Defenses
- Risk assessment
- Viruses
- Unix security
- authentication
- Network security
  Firewalls,vpn,IPsec,IDS
- Forensics

Cryptography
- •Random numbers
- •Hash functions
  MD5, SHA,RIPEMD
- •Classical + stego
- •Number theory
- •Symmetric key
  DES, Rijndael, RC5
- •Public key
  RSA, DSA, D-H,ECC

Applied crypto
- •SSH
- •PGP
- •S/Mime
- •SSL
- •Kerberos
- •IPsec
- •Crypto APIs
- •Coding securely

CNS Lecture 1 - 5

Plan of attack

Lectures

1. Risk, viruses
2. UNIX vulnerabilities
3. Authentication & hashing
4. Random #s classical crypto
5. Block ciphers DES, RC5
6. AES, stream ciphers RC4, LFSR
7. **MIDTERM** ☹
8. Public key crypto RSA, D-H
9. ECC, PKCS, ssh/pgp
10. PKI, SSL
11. Network vulnerabilities
12. Network defenses, IDS, firewalls
13. IPsec, VPN, Kerberos, secure OS
14. Secure coding, crypto APIs
15. review

The bottom up approach

Issues: technical, social, ethical, political, legal, mathematical

CNS Lecture 1 - 6

Building a crypto toolbox

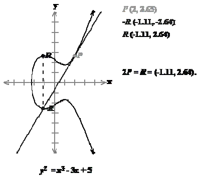
tools for building secure applications

- fast symmetric key encryption
- hash functions
- random numbers, prime testing
- public key crypto
- Big integer math libraries/methods
- algorithms for message authentication, key exchange, user authentication

We'll find all of these in the OpenSSL library
emphasis will be C
some Java examples

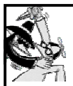
Mathematics of cryptography

- mod arithmetic, gcd, CRT (shift cipher, Hill, RSA, D-H, ECC)
- Polynomial arithmetic over GF(2^n) (LFSR, ECC, AES, CRC)
- Testing primes, irreducible polynomials, generators
- Random number generation (keys, IV, blinding, k for DSS)
- BIG integer arithmetic
- Nonlinear Boolean functions (Bent)
- Factoring and discrete logs
- Elliptic curves

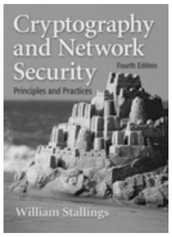


Security through mathematics

Class web resources



- class page
- policy
- resources
- lectures
  - Required reading
- assignments



Computer security

- Protecting assets
- Setting security goals
- Establishing security policy
- Identify threats
- Develop controls/countermeasures
- Have a disaster/recovery plan

Principle: path of least resistance

security

Objective: protect information

- integrity
- privacy
- availability
- PAIN (non-repudiation)

Provided by:

- having a plan (risk assessment, policy)
- educating users/programmers
- Secure applications and tools -- hashing, signing, encryption

security features ≠ secure features

threats

threats are real – interruption, interception, modification, fabrication

- dependence on info technology
- passive attacks
  - sniffing, wiretaps, TEMPEST
  - social engineering
  - dumpster diving
- active attacks (DoS, worms/viruses, exploits)
- attack tools easily available

Social Engineering – because there's no patch for human stupidity.

Social engineering

misplaced trust

- impersonation
- scam
- email -- who really sent it, phishing
- email -- attachments (viruses)
- web -- rogue applets, plugins
- Download this fix for virusX

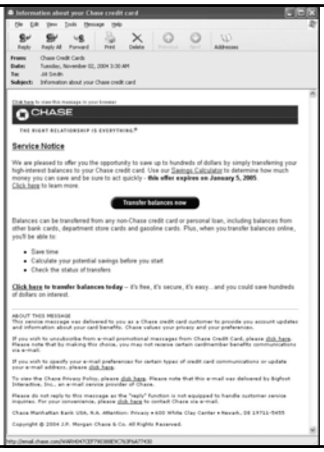
Be suspicious...

419 scam

"Nigerian uncle has died intestate. Need to transfer $8M to US with your assistance. You will get 10% of funds, need your bank info to initiate the transfer …."

[user] Hello?
[hacker] Hi, this is Bob from IT Security. We've had a security breach on the system and we need every user to verify their username and password.
[user] What do I need to do?
[hacker] Let's walk through a login, just to make sure everything is fine.
[user] OK
[hacker] OK, go ahead and login. What username are you coming in as?
[user] My username is "smith".
[hacker] Excellent. What password are you using?
[user] I am using the password "drowssap".
[hacker] Do you have a system prompt yet?
[user] Yes, I'm in.
[hacker] OK, there you are. I see you now. Everything is fine. We appreciate your cooperation.
[user] OK, goodnight.
[hacker] Thanks again, goodbye.

phishing


Information about your Chase credit card
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses

From: Chase Credit Cards
Date: Tuesday, November 02, 2004 3:30 AM
To: Jill Smith
Subject: Information about your Chase credit card

Click here to view this message in your browser

CHASE

THE RIGHT RELATIONSHIP IS EVERYTHING.®

Service Notice

We are pleased to offer you the opportunity to save up to hundreds of dollars by simply transferring your high-interest balances to your Chase credit card. Use our Savings Calculator to determine how much money you can save and be sure to act quickly - **this offer expires on January 5, 2005**. Click here to learn more.

Transfer balances now

Balances can be transferred from any non-Chase credit card or personal loan, including balances from other bank cards, department store cards and gasoline cards. Plus, when you transfer balances online, you'll be able to:

- Save time
- Calculate your potential savings before you start
- Check the status of transfers

Click here to transfer balances today -- it's free, it's secure, it's easy…and you could save hundreds of dollars on interest.

ABOUT THIS MESSAGE
This service message was delivered to you as a Chase credit card customer to provide you account updates and information about your card benefits. Chase values your privacy and your preferences.

If you wish to unsubscribe from e-mail promotional messages from Chase Credit Card, please click here. Please note that by making this choice, you may not receive certain cardmember benefits communications via e-mail.

If you wish to specify your e-mail preferences for certain types of credit card communications or update your e-mail address, please click here.

To view the Chase Privacy Policy, please click here. Please note that this e-mail was delivered by Bigfoot Interactive, Inc., an e-mail service provider of Chase.

Please do not reply to this message as the "reply" function is not equipped to handle customer service inquiries. For your convenience, please click here to contact Chase via e-mail.

Chase Manhattan Bank USA, N.A. Attention: Privacy • 600 White Clay Center • Newark, DE 19711-5455

Copyright © 2004 J.P. Morgan Chase & Co. All Rights Reserved.

http://email.chase.com/WARH047CEF790300E9C763F6A77430

Hoaxes and urban legends

- Good intention user forwarding warning
  - Good Times Virus
  - I may have sent you a virus, see if you have vb.exe ....
  - Poisoned chewing gum
  - Travelers having their kidneys stolen
  - 1954 home computer in Popular Mechanics

Scientists from the RAND Corporation have created this model to illustrate how a "home computer" could look like in the year 2004. However the needed technology will not be economically feasible for the average home. Also the scientists readily admit that the computer will require not yet invented technology to actually work, but 50 years from now scientific progress is expected to solve these problems. With teletype interface and the Fortran language, the computer will be easy to use.

Point, click, attack

Sophisticated attack tools designed by troubled genius

- deep understanding of OS (source files)
- look for known vulnerabilities (overflows)
- lots of time
- adaptable, avoids countermeasures

- tools available on the net
- cookbook attacks
- your little brother could do it

alt.2600 faq

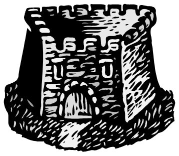
How do I reset a BIOS password?
How do I access the password file under Windows NT?
How do I crack Windows NT passwords?
How can I recover a lost Windows NT Administrator Password?
How does the Microsoft Windows 3.1 password encryption work?
How do I change to directories with strange characters in them?
What is this system?
What are some default accounts?
What is a computer virus?
What is a computer worm?
What is TEMPEST?
How do I remove copy protection?
How do I send fake mail?
How do I fake posts and control messages to Usenet

How can I find security vulnerabilities in source code?
What is an integer overflow?
What is a race condition?
What is a format string vulnerability?
What is a random number vulnerability?
What is an SQL Injection Attack / Vulnerability?
How can I securely erase data?
What is two factor authentication?
How do I crack VMS passwords?
What can be logged on a VMS system?
What privileges are available on a VMS system?
How do I crack Unix passwords?
How do I change a MAC address?
How do I recover the password for a Cisco router?
How do I decrypt Cisco passwords?

Microsoft's 10 immutable Laws of Security

Law #1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore
Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore
Law #3: If a bad guy has unrestricted physical access to your computer, [or data] it's not your computer anymore
Law #4: If you allow a bad guy to upload programs to your website, it's not your website any more
Law #5: Weak [or weakly protected] passwords trump strong security
Law #6: A computer is only as secure as the administrator is trustworthy [and is aware of threats and countermeasures]
Law #7: Encrypted data is only as secure as the decryption key
Law #8: An out of date virus scanner is only marginally better than no virus scanner at all
Law #9: Absolute anonymity isn't practical, in real life or on the Web
Law #10: Technology is not a panacea

countermeasures



prevention, detection, response

- education ←
- physical protection
- authentication
- authorization
- auditing (intrusion detection)
- encryption

Threats/countermeasures -- a never ending cycle ...
good job security!

The bad guy has it is easy, he only has to find one hole.

You have the hard job, you need to defend all the holes!

Security services

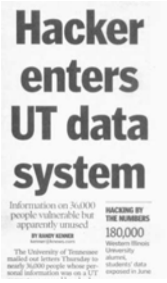
From the ISO definition:

- access control
- authentication
- privacy
- integrity
- non-repudiation

Cryptography
- hash functions (MD5, SHA)
- secret-key encryption (DES, Rijndael)
- public-key encryption (RSA, DSS)

provided through applications, protocols, mechanisms, and algorithms

Are we at risk?



Hacker enters UT data system

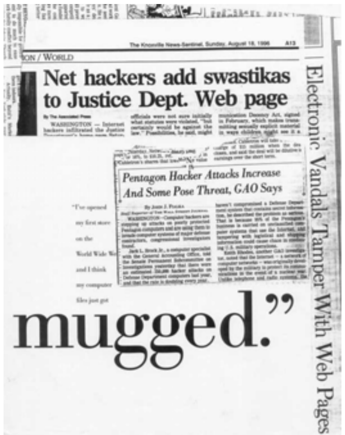
Information on 36,000 people vulnerable but apparently unused

HACKING BY THE NUMBERS

180,000

Western Illinois University alumni, students' data exposed in June

The University of Tennessee mailed out letters Thursday to nearly 36,000 people whose personal information was on a UT



The Knoxville News-Sentinel, Sunday, August 18, 1996 A13

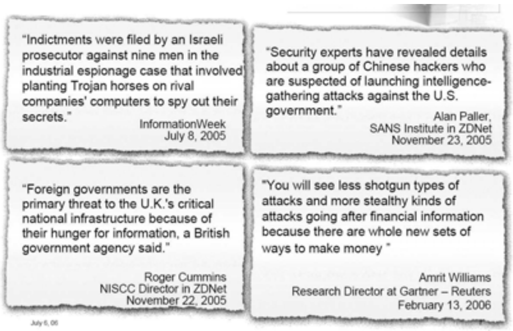
Net hackers add swastikas to Justice Dept. Web page

Pentagon Hacker Attacks Increase And Some Pose Threat, GAO Says

"I've opened my first store on the World Wide Web and I think my computer files just got mugged."

Electronic Vandals Tamper With Web Pages

Are we at risk?



"Indictments were filed by an Israeli prosecutor against nine men in the industrial espionage case that involved planting Trojan horses on rival companies' computers to spy out their secrets."
InformationWeek
July 8, 2005

"Security experts have revealed details about a group of Chinese hackers who are suspected of launching intelligence-gathering attacks against the U.S. government."
Alan Paller,
SANS Institute in ZDNet
November 23, 2005

"Foreign governments are the primary threat to the U.K.'s critical national infrastructure because of their hunger for information, a British government agency said."
Roger Cummins
NISCC Director in ZDNet
November 22, 2005

"You will see less shotgun types of attacks and more stealthy kinds of attacks going after financial information because there are whole new sets of ways to make money"
Amrit Williams
Research Director at Gartner – Reuters
February 13, 2006

July 6, 06

Are critical resources at risk?

Assets controlled by computers

air defense
command and control
banking
power grid
phone system
traffic signals
corporate email
refinery
SCADA systems
medical records
personnel records

nuclear weapons systems
Taco Bell
electronic funds transfer
air traffic control
elevators
trains
grades
stock exchange
TV/radio
police records
payroll

HE'S GONE: Jerry Garcia Dead at 53
TIME
CYBER WAR
The U.S. rushes to turn computers into tomorrow's weapons of destruction. But how vulnerable is the home front?

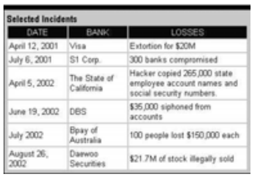
- Information warfare/cyber terrorism -- fact or fiction?

Under cyber attack?

- After America accidentally bombed the Chinese embassy in Belgrade in 1999, Chinese hackers launched hundreds of attacks on U.S. Web sites and infiltrated at least four government Internet sites.
- War protesters and hackers are assaulting .gov and .mil Websites "in digital retaliation" for the war in Iraq in record numbers, according to the security firm mi2G Ltd. of London.
- One such hacker, interviewed by e-mail for this article, warned that Western governments and businesses should brace themselves for 'suicide cyber attacks' in the event of a war against Iraq. He defined a 'suicide cyber attack' as one in which the hacker sets out to cause maximum damage unhindered by any regard for being detected and caught. The hacker who issued this stark warning belongs to a group calling itself the Iron Guards which has in the past attacked Israeli government and business sites as part of the Arab-Israeli cyberwar.
- Computer hackers broke into 26 government Internet sites on three continents in "one of the largest, most systematic defacements of worldwide government servers on the Web," according to an online security organization.

Cyber attacks/extortion on financial institutions

- Russian police have broken up a hacker ring that extorted money from British bookmakers, inflicting millions in losses on their Web sites in a series of attacks that attracted the British government's attention, officials said Wednesday.
- According to computer security expert Dr Neil Barrett, the credit card trading centre of the world is St Petersburg in Russia. It is the site of a number of secret internet marketplaces where card details are offered in bulk, typically costing $1 a card, sold in batches of 500 through to 5,000.
- 80% unreported



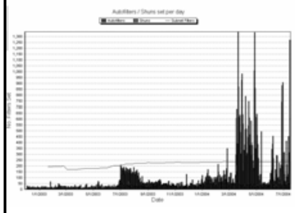
Selected Incidents

DATE	BANK	LOSSES
April 12, 2001	Visa	Extortion for $20M
July 6, 2001	S1 Corp.	300 banks compromised
April 5, 2002	The State of California	Hacker copied 265,000 state employee account names and social security numbers.
June 19, 2002	DBS	$35,000 siphoned from accounts
July 2002	Bpay of Australia	100 people lost $150,000 each
August 26, 2002	Daewoo Securities	$21.7M of stock illegally sold

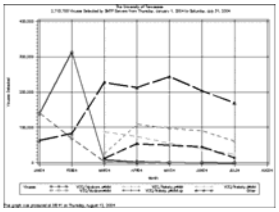
Hacking the infrastructure

- LOS ANGELES, California (CNN) -- As Californians suffered under rolling blackouts last month, computer hackers were trying to breach the computer system at the California Independent System Operator (Cal-ISO), which oversees most of state's power transmission grid
- Nationwide rolling blackouts could have a devastating impact on the economy, but experts also fear that the stress being placed on the nation's power grid could make it more susceptible to disruptions from hackers.
- After flunking three congressional audits, the Federal Aviation Administration says air traffic control systems are finally safe from hack attack
- Attacks on core Internet routers and DNS servers
- '97 employee alters software in Taco Bell cash register

Recent local activity



Nasty hosts and subnet



Nasty emails

In the news …

- Hacker gains access to personal data (SS# etc) of 36,000 students and staff at University of Tennessee
- Cyber scams prey on Katrina victims
- Congress introduces anti-spyware legislation
- Google search can provide access to many "security webcams"
- Hacker gets 3 years for botnet attack using 10,000 PCs
- 'Two Cal State Northridge students have been accused of hacking into a professor's computer, giving grades to nearly 300 students.
- Plus the usual viruses and buffer overflows ….

The attackers

- amateur
- insider (greed, disgruntled)
- kids
- hackers
- criminals
- spies
- sociopath (terrorist/vandal)

Why?

- money
- retribution
- sport
- political/military
- pathological

easy to do, hard to catch,
harder to prosecute

victimless crime? just a prank?

Ancient history

" A long time ago in a galaxy far, far way ...“

- 1900 BC first written cryptography
- 500 BC Hebrew substitution cipher
- 50 BC Caesar cipher
- 1844 telegraph (easily “tapped”, civil war)
- 1876 telephone invented
- 1878 first report of teenagers kicked off phone system for pranks
- 1900 radio/wireless (easy intercept)
- 1917 one-time pad
- 1923 Enigma machine
- 1948 Captain Midnight decoder ring (Ovaltine)
- 1950’s/60’s single user then batch computing

Recent history

- ’64 teletype/acoustic coupler (remote users!)
- ’67 DEC10 timesharing
- ’69 ARPANET (email)
- ’70 DEC 11 / UNIX
- ’71 Captain Crunch -- 2600
- ’74 DES
- ’75 crypt for passwd
- ’76 public key crypto / Ethernet
- ’77 Apple II / uucp/USENET
- ’79 VAX / BSD UNIX (free)
- ’80 DECnet / MFEnet / SNA / CSnet / BITNET / MS DOS
- ’81 Mitnick (17) steals Pac Bell manuals
- ’84 ORNL on Internet (ARPAnet/MILNET) 9.6
- ’85 Sun workstations (sniffers)
- ’86 first virus/ LBL cuckoo’s egg
- ’88 Morris worm (hit ORNL)
- ’91 PGP
- ’93 Mosaic/www point/click/attack
- ’94 ORNL/MSR breakin
- ’94 Linux (free) / rootkit
- ’95 Mitnick attack SDSC / SATAN / SSL
- ’98 smurf attack
- ’00 ILOVEYOU, DDOS, Rijndael

First virus? ☺

happenings

1999

- 512-bit number factored (7 mos, 292 computers/11 sites)
- EFF cracks DES key in 22 hours
- Shamir describes TWINKLE (crack 512-bit RSA in days)
- AES selects 5 finalists (Mars, RC6, Rijindael, Serpent, Twofish)
- Pentium III with hardware RNG (and serial no.)
- script kiddies plaster graffiti on web sites
- Melissa Word macro virus (80-400M)
- PaPa Excel macro virus
- DVD cracked
- version of GSM cracked (cell phone)
- CERT warns of distributed DoS attacks
- Serbian hackers threatened NATO info sites
- two Chinese hackers sentenced to death

the new millenia

- I LOVE YOU virus
- Distributed Denial of Service/botnets
- credit cards stolen (hack and SQL)
- AES selects Rijndael cipher
- Australian net vigilantes (kiddie porn)
- US debates offensive methods
- cyber warfare (pakistan/india, china/taiwan)
- crypto export relaxed ? (myth)
- Broadband/dsl/wireless proliferation
- Al Qaeda using internet ?
- Blaster worm
- Spyware, phishing
- 2004, 50 new malwares/day
- To date: 100,000 identified malwares

Trends

- More (vulnerable) things connected to the net

DOCTOR FUN
4 June 2003
W3
0wN
uR
fR1dg3!
3133T
SNAX0rZ
Copyright © 2003 David Farley, d-farley@ibiblio.org
http://ibiblio.org/Dave/drfun.html
This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.

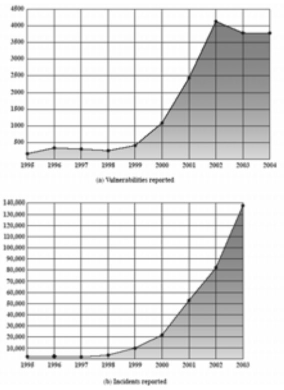
The brave new world of IPv6

trends

- People and enterprises are more security-aware
- More tools for detecting/preventing malicious software

- But
  - –More security-challenged boxes online 7x24 (DSL, cable modems)
  - –More wireless nets (802.11, cellular, bluetooth/PDAs, RFID)
  - –Faster machines/connections
  - –More sophisticated malicious software
  - –More dependence on “the Net”

CERT statistics



(a) Vulnerabilities reported

(b) Incidents reported

Risk assessment

- identify assets and value
- determine vulnerabilities
- estimate probabilities
- estimate losses
- identify controls and their cost
- estimate savings

determine an acceptable risk

Personal safety

Lock your doors? Mutliple locks?

Bars on windows?

Alarm system?

Electric fence?

Guards?

Safe room? Fallout shelter?

Seat belt?

Walk at night?

Concealed weapon?

Buy “extended warranty”

Buy insurance/deductible?

Think like a bad guy …

Cost of losses

- priceless -- trade secrets
- don’t know when digital info is "stolen"
- dollar value of assets
- plus cost to replace/fix, time
- loss of "face" or confidence
- liability

controls

- bomb shelter
- insurance (actuarial tables)
- sprinkler system
- UPS
- redundancy
- backups
- alternate site
- 7x24 maintenance
- vaults
- encryption
- access/audit logs
- policy/procedures

Principle: Defense in depth

Door/windows locks

Surveillance cameras

Door/window alarms

Background checks

Guards

Safe

Insurance

Review: probabilities/costs change, new assets/threats

Industrial strength

- formal policy/procedures
- automated analysis tools
- threat models
- forms and sign-off
- who is responsible
- contingency plans
- configuration mgt.
- audit and drills
- user training
- incident response teams
- periodic review
- punishment

Risk assessment useful?

problems
- not precise -- OK, it’s a planning tool
- file and forget -- review
- unscientific -- no based on statistics

benefits
- improve awareness
- identifies assets, vulnerabilities, controls
- basis for decisions
- justification for budget ($)

Enterprise security planning

how an organization addresses security

- policy -- security goals →
- current state
- requirements to meet goals
  - –Hardware/software
  - –Education/training
  - –Audits and testing
- who is responsible
  - –Incident response plan and team
- schedule for implementation
- schedule for review

based on risk assessment

Security Policy

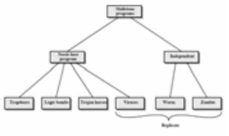
security goals -- integrity, availability, privacy

•who can access what and how
 -no cleartext logins or POP
 -patched OS
•mechanisms (fences, authentication, audit, encryption, smart card, firewall, antivirus)
 -password policy
 -unix config guidelines
 -patches
 -access points, authorization
 -ssh/kerberos ssl
 -UT netreg (patches, anti-virus)
•Policing and punishment -- scans

security is hard -- physical, OS, applications, network, programmers, users

Security is a process – not something you buy

Malicious programs



- trap doors
  - War Games
  - sendmail
- logic bombs
  - 'blowup' if you're fired
- trojan horse
  - "social engineering"
- worm
  - Self-propagating
  - Blaster, Sasser, Slammer
- zombie/bot
  - Internet host used to launch attacks
- virus
  - Infects other programs

Cause?

•Bad design

•Improper configuration

•Bad implementation – overflows

•Intentional/insider

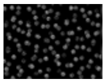
•stupid

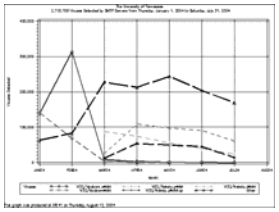
Morris worm '88

- Entry via network (sendmail debug option, or fingerd stack overflow … details later)
- Executed simple commands to download rest of worm
- Collected potential target hosts from /etc/hosts .rhosts .forward
- tried cracking /etc/passwd
- Attempt to rlogin or use sendmail/fingerd to attack targets
- Probably hit 10% of Internet hosts in 1988

viruses

- Anatomy
  - Parasitic – attached to an executable
  - Memory-resident – in the OS
  - Boot-sector
  - Stealth – avoid detection
  - Polymorphic – dynamic signature
- Threat
  - Damage/nuisance
  - Loss of information/privacy
  - replication
- propagation
- detection
- Prevention
  - Email scanners, download check, OS activity monitor
- Recovery
  - Removal, registry restore

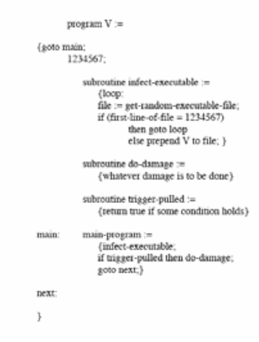




Virus phases

- Dormant phase
  - Activated by event or time or when infected program is executed
- Propagation phase
  - Replicate
  - "infection" by disk/CD, email attachments, trojan horses, downloads/plugins
- Execution phase
  - Nuisance messages
  - Delete files
  - Delayed/triggered execution

Infected program



```
        program V :=

{goto main;
        1234567;

            subroutine infect-executable :=
                {loop:
                file := get-random-executable-file;
                if (first-line-of-file = 1234567)
                        then goto loop
                        else prepend V to file; }

            subroutine do-damage :=
                {whatever damage is to be done}

            subroutine trigger-pulled :=
                {return true if some condition holds}

main:       main-program :=
                {infect-executable;
                if trigger-pulled then do-damage;
                goto next;}

next:

}
```

viruses

boot sector
- replace code in boot sector
- goes into RAM, alter I/O routines
- infects hard disk other floppies

program
- append virus code to end of file
- change first instruction to jump to virus code
- virus code makes itself resident
- resume execution of original application
- scans disk and infects other executables or worse

macro
- platform independent
- document contains macros (VBasic) (extends functions) (WORD or EXCEL)
- Command macro – e.g., executed each time uses clicks FILE SAVE
  or automatically executed when WORD starts – copy itself to other docs
- spread by email (Melissa, ILOVEYOU)

UNIX viruses?

UNIX script
- attached to end of a script you've downloaded
- search all scripts in the current directory
- if #virus# not there, attach script to end of target

download threats
- postscript
- Java applets, ActiveX
- MIME-encoded mail
- Plugins
- spyware
- root and shareware (tar, shar)

threats

- anything a program can do
- display a message on a certain date
- slow performance, alter display
- backdoor (backorifice, netbus), remote command window access
- Zombie – lay dormant awaiting command to attack/spam
- keyboard/net sniffer (collect passwords, SSN, credit card #s)
- alter files, crash system
- erase files .....

- Cost: disk cleanup, lost time ($55 billion/yr 2003)

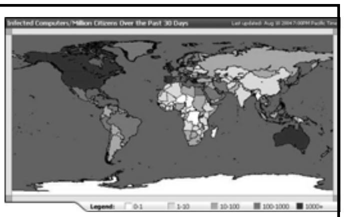
Popular viruses

- Stoned boot sector
- Michelangelo boot sector
- Pakistani Brain boot sector, marks area of disk as bad
- Jerusalem .COM and .EXE, memory resident, scrambles disk data
- Lehigh command processor, destroys data on hard disk
- Friday the 13th
- Melissa –virus and worm (emails itself to first 50 in your address book)
- ILOVEYOU
- Concept – first WORD macro virus
- ExploreZip -- worm
  - emails itself to people who have sent you email
  - Copies itself onto local microsoft net startup files
- Good Times – NOT (hoax)

See symantec or mcafee

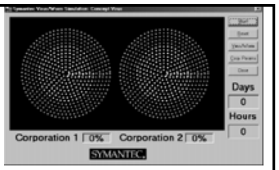
Virus construction kits
- •Virus Creation Lab
- •many Mutation Engines
- •Metasploit
- •more ……

propagation


Infected Computers/Million Citizens Over the Past 30 Days
Last updated: Aug 10 2004 7:00PM Pacific Time
Legend:
0-1
1-10
10-100
100-1000
1000+

- disk from home
- shared file system
- download (ftp/plugin)
- email (attachments)
  - Propagates through address books, archive email
  - See Symantec simulator →
- vendor (CD, updates, compiler!)
- Virus propagation require a person

Symantec simulator



- Virus/worms
  - Concept – first macro virus (email)
  - Melissa – virus and worm (email address book)
  - exploreZip – worm, spreads on reboot, email address book and recent senders, modifies startup script on shared files
- Two enterprises
  - Corporation 2 has ALL CORPORATION maillist
  - Parameters: email rate, external/internal, workgroup, ALL corp. list, % shared drives, reboots/day, # recipients, % attachments

Worm propagation

Code Red
- .ida vulnerability in Microsoft IIS servers (buffer overflow)
- Launched 99 threads and generated random IP addresses to attack
- Thread 100 defaced web server

Code Red II -- faster propagation
- 3/8 choose random address in local class B
- ½ from local class A
- 1/8 random from whole internet

Nimda
- 5 propagation techniques
  - IIS vulnerability probes
  - Bulk email from address lists
  - Copying to open network shares
  - Exploit code added to server page
  - Scan for Code Red II backdoors

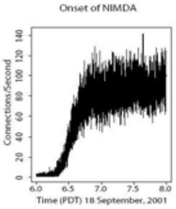
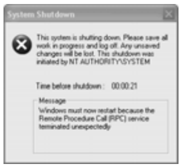


Figure 5: HTTP connections per second seen at the Lawrence Berkeley National Laboratory, rising due to the onset of Nimda, September 18.

Microsoft blaster worm

- Exploited a buffer overflow in RPC (port 135)
- Installed msblast.exe in system folder
  - Modify registry so msblast.exe runs at boot and start msblast.exe
  - Prevent downloading a patch (SYN flood of windowsupodate.com)
  - Reboot the machine every 60 seconds
  - Look for other IP addresses ("nearby" or random) running port 135
  - '03, first 5 days, 3 million tech support calls
  - Survey 882 companies
    - Average cost $474k, max $4.2M
    - Entered via laptops, VPNs, then routers



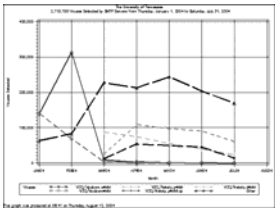
This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by NT AUTHORITY\SYSTEM

Time before shutdown : 00:00:21

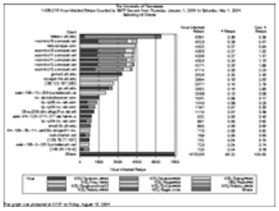
Message
Windows must now restart because the Remote Procedure Call (RPC) service terminated unexpectedly

Virus activity at UT

volume



who



symptoms

When YOU detect the malware☹

- file changes: length, date/time
- slower system operation
- reduced memory or disk space
- bad sectors
- unusual messages/displays
- failed program execution
- Blue screen of death

A fatal exception 0E has occurred at 0157:BF7FF831. The current application will be terminated.

* Press any key to terminate the current application.

* Press CTRL+ALT+DEL to restart your computer.

You will lose any unsaved information in all applications.

Press any key to continue

Detection – anti-virus software

- signature scan (batch)
  - Locate
  - Identify which virus
  - Remove (anti-virus software may help, or web site instructions, registry)
- Checksums – see that files have changed (tripwire)
- email checkers (active)
  - Virus signature
  - Executable attachments
- self-checking/integrity checking on load (not foolproof)
- Memory resident abnormal operation detection (detect new ones)
  - Block "abnormal behavior" – format disk, change registry, network apps, executable modifications
- emulators (IBM's digital immune system)
- commercial/shareware anti-virus software (updates)
- caution downloading software (shareware, Java), attachments

Recovery

- anti-virus often can remove virus, or see instructions at Symantec/McAfee, otherwise restore from backups

See symantec example

MSRT – Microsoft malware removal

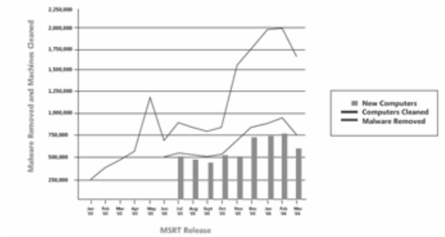
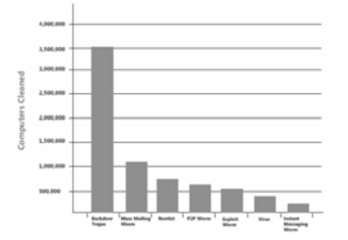


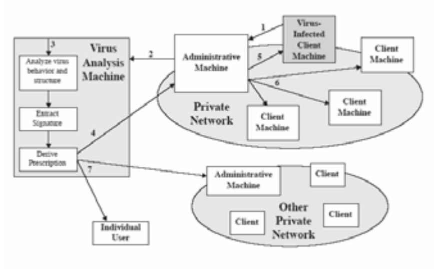
Figure 3. Malware Removed and Computers Cleaned Per MSRT Release

- 6 million computers cleaned
- Top malware: trojan horse (62%)
  - Used for bots (spam, spyware, DoS attack)

Malware Microsoft



Digital immune system



Don't need "signature" data base

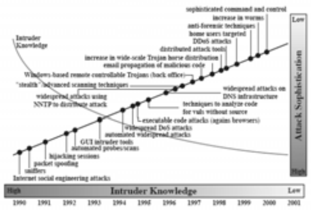
This is basically what Symantec/McAfee do at headquarters each day

Trends: combo attack – virus/worm/spam/DoS, sell botnet

zero-day exploit: vulnerability discovered on launch day

Trends

- Combo attacks – virus/worm/spam/DoS
- Sell botnet’s for spam – attack for profit $$
- Zero-day exploit: vulnerability discovered on launch day
- Attacks more sophisticated, less skill required (point/click/attack)



Source: CERT

Figure 1.2 Trends in Attack Sophistication and Intruder Knowledge

Your mission

- Protect cyber space
- Pass this course

Next time …

UNIX attacks, using PGP

Get your CS account!

Do assignment 1 and begin assignment 2