CS305 Topic – Security

- Viruses, Worms, and Other Undesired Programs
- Hacking and Network Attacks
- Defensive Measures
- Laws and Penalties

Sources: Baase: A Gift of Fire *and* Quinn: Ethics for the Information Age

Undesired Programs

- Viruses
- Worms
- Trojan Horses
- Malware
- Adware
- Spyware

Computer Viruses

A piece of self-replicating code embedded within another program (host).

- It needs a host to spread – typically spread through email or downloaded programs
- Viruses almost always corrupt or modify files on a targeted computer.

First Computer Virus?

In the early 70s, the *Creeper* virus was detected on ARPANET (the predecessor of Internet) infecting the Tenex operating system.

- Creeper gained access through a modem and copied itself to the remote system where the following message was displayed:

  "`I'M THE CREEPER: CATCH ME IF YOU CAN`."
- The *Reaper* program, itself being a virus, was created to delete Creeper.
- The creators of both programs are unknown.

Some Notable Viruses

- *Brain (c. 1986)*
  - 1st virus to move from one PC to another
- *Michelangelo (c. 1991)*
  - Attacks only on March 6th
- *Melissa (c. 1999)*
  - Attached to email, infected 100K computers
- *Love Bug (c. 2000)*
  - Another email virus, deletes files and collects passwords

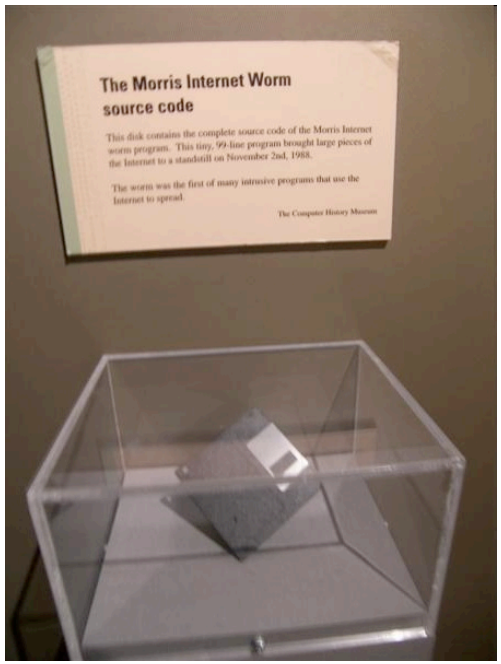
Computer Worms

A self-contained program that spreads through a network by exploiting security holes in networked computers.

- It does not need to attach itself to an existing program.
- Worms almost always cause harm to the network (e.g. at least consuming bandwidth)

The Morris Internet Worm (1988)

- First worm to affect thousands of computers
- Used a buffer overflow attack exploiting bugs in three Unix applications: ftp, sendmail, and fingerd
- Designed by a Cornell student, with a simple goal of seeing how many Internet computers he could infect with the worm
- Resulted in a conviction of the student



Disk containing the source code for the Morris Worm held at the Boston Museum of Science. Picture credit: Shannon Bullard, Go Card USA

Buffer-Overflow Attacks

A favorite exploit for hackers.

- Exploits a program that waits for user input (a string of characters) and stores the input in an allocated space
- Exploits a security hole in C and C++, that no array bounds checking is performed
- If the user input's size is bigger than the allocated space, it overflows and over-write other storage slots nearby

Two Forms: stack-based and heap-based

Stack-Based Overflow Attack

```
void processing_name (char *name) {
    char buf[NAME_LIMIT];
    strcpy(buf, name); // no bounds hecking
    ...
}
int main (int argc, char **argv) {
    processing_name(argv[1]);
}
```

- The overflow over-writes the *return address* slot in the stack frame
- When the called function returns, it will return to whatever address that is in the *return address* slot

Buffer-Overflow Attacks Fixes

- For language designers:
  - Require array bounds check (e.g. Java)
- For OS designers:
  - Disallow executable code on the stack or heap
- For programmers:
  - Fix specific programs that has vulnerability

Some Other Notable Worms

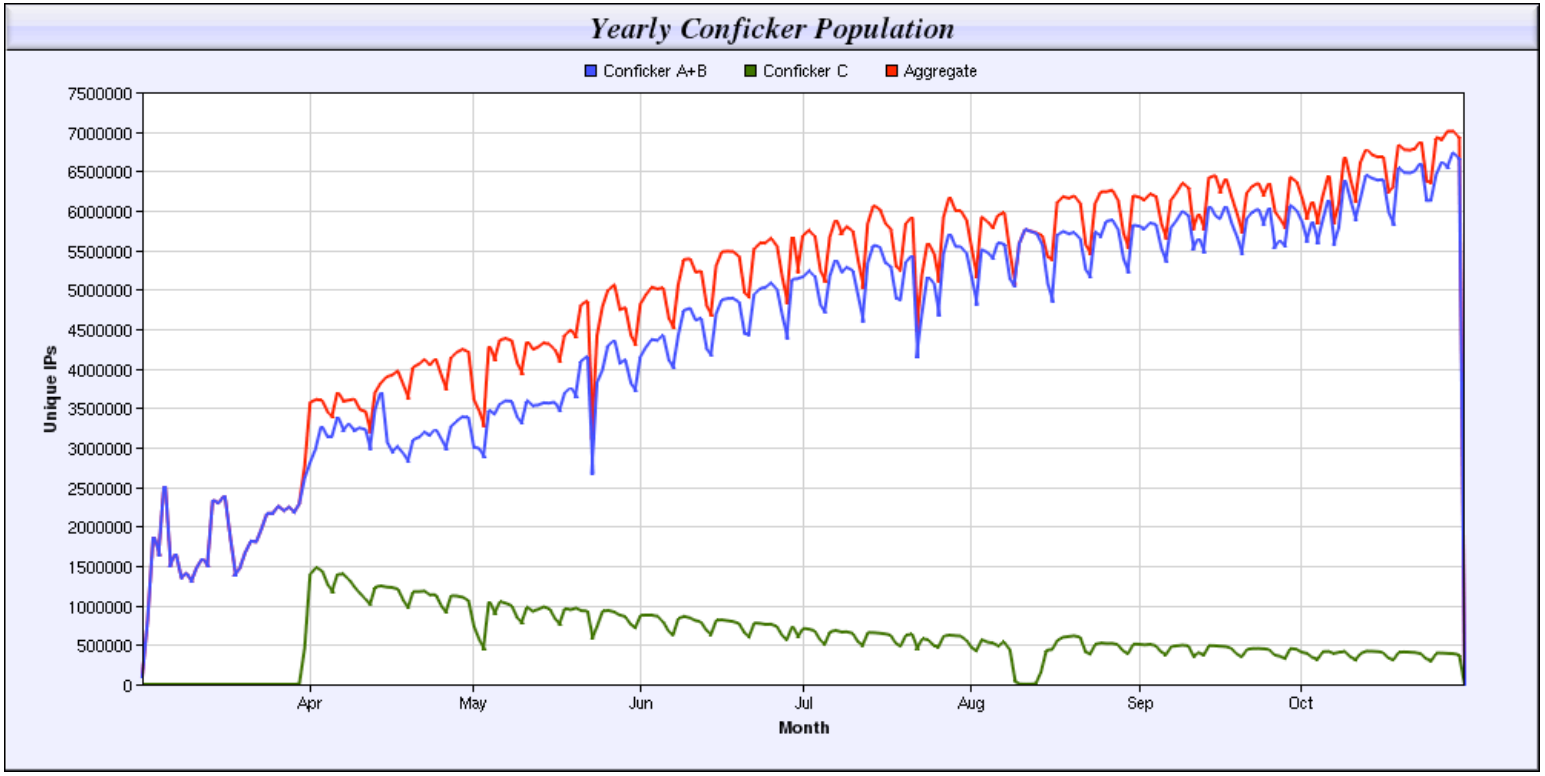
- *WANK (c. 1989)*
  - "Worms Against Nuclear Killers"
- *Code Red (c. 2001)*
  - Originated from China, spread to more than 359,000 hosts in less than 14 hours
- *Sapphire (Slammer) (c.2003)*
  - Fastest-spreading worm in history, number of infected hosts doubled every 8.5 seconds
- *Sasser (c. 2004)*
  - Infected 18 million computers, though effects were relative benign; created by a German teenager

The Conficker Worm

- First detected in Nov. 2008
- Estimated 8-15 million computers infected
- Takes no immediate actions on infected computers, but tries to contact the master (in a smart way)
- Microsoft is offering $250K reward for capturing the creator

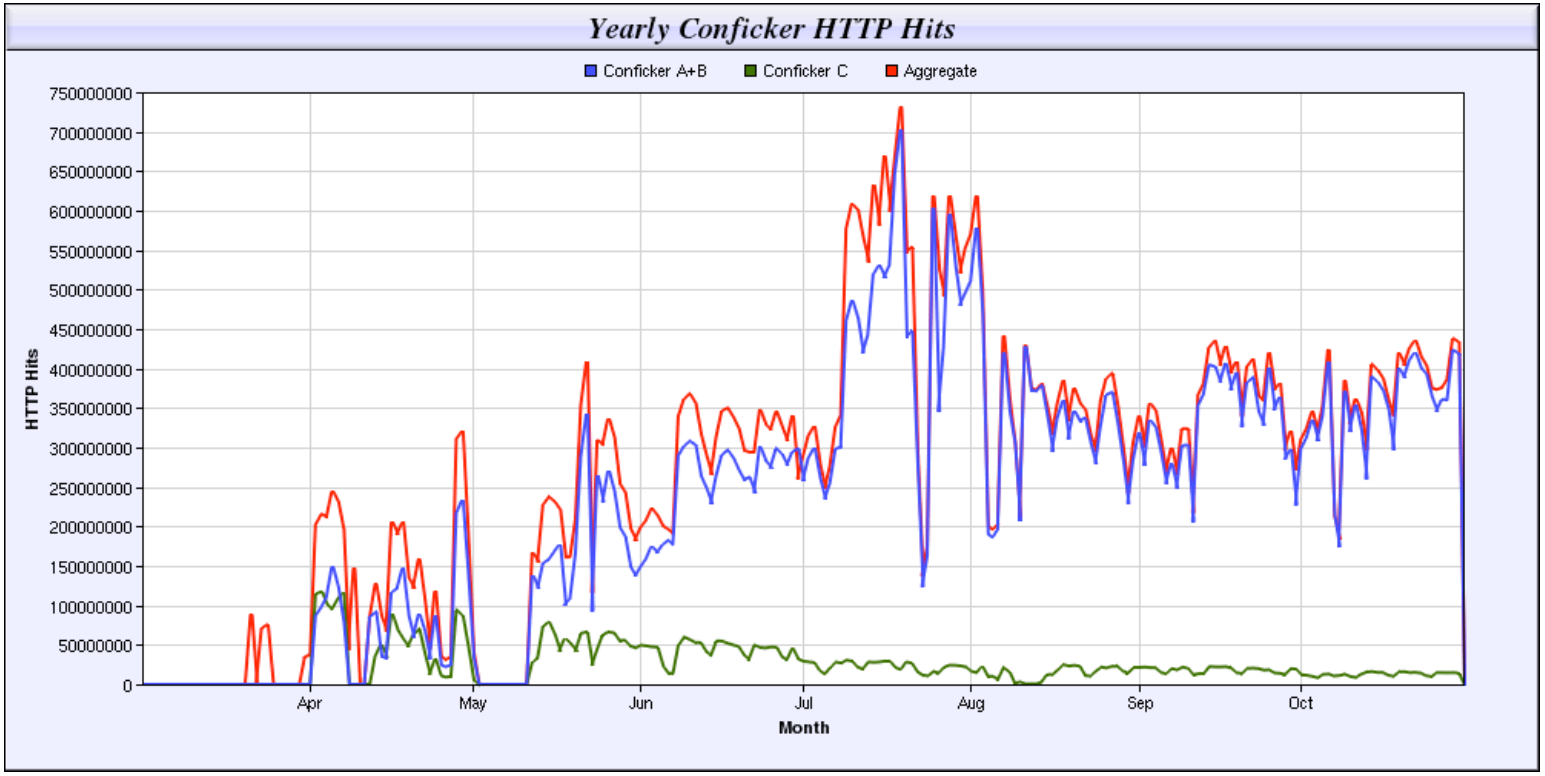
The Conficker Worm (cont.)

Daily tracking by the Conficker Working Group:



The Conficker Worm (cont.)

Daily tracking by the Conficker Working Group:



Trojan Horses

A malicious program hidden within a benign host program. When the benign program executes, the hidden program does, too.

Examples of Malicious Tasks:

- Opening internet access to attackers
- Logging keystrokes and sending to attackers
- Destroying files
- Turning the PC into a proxy server for illegal activities

Trojan Horse Examples

- *Waterfalls.scr* – A free waterfall screen saver
  - When running, it unloads hidden programs and scripts
- *SubSeven* – A remote access program
  - Provides an easy-to-use GUI
  - Consists of a client program running on the attacker's computer, and a server program running on the victim's computer
  - Capable of capturing screen images, recording keystrokes, read/write files, and more

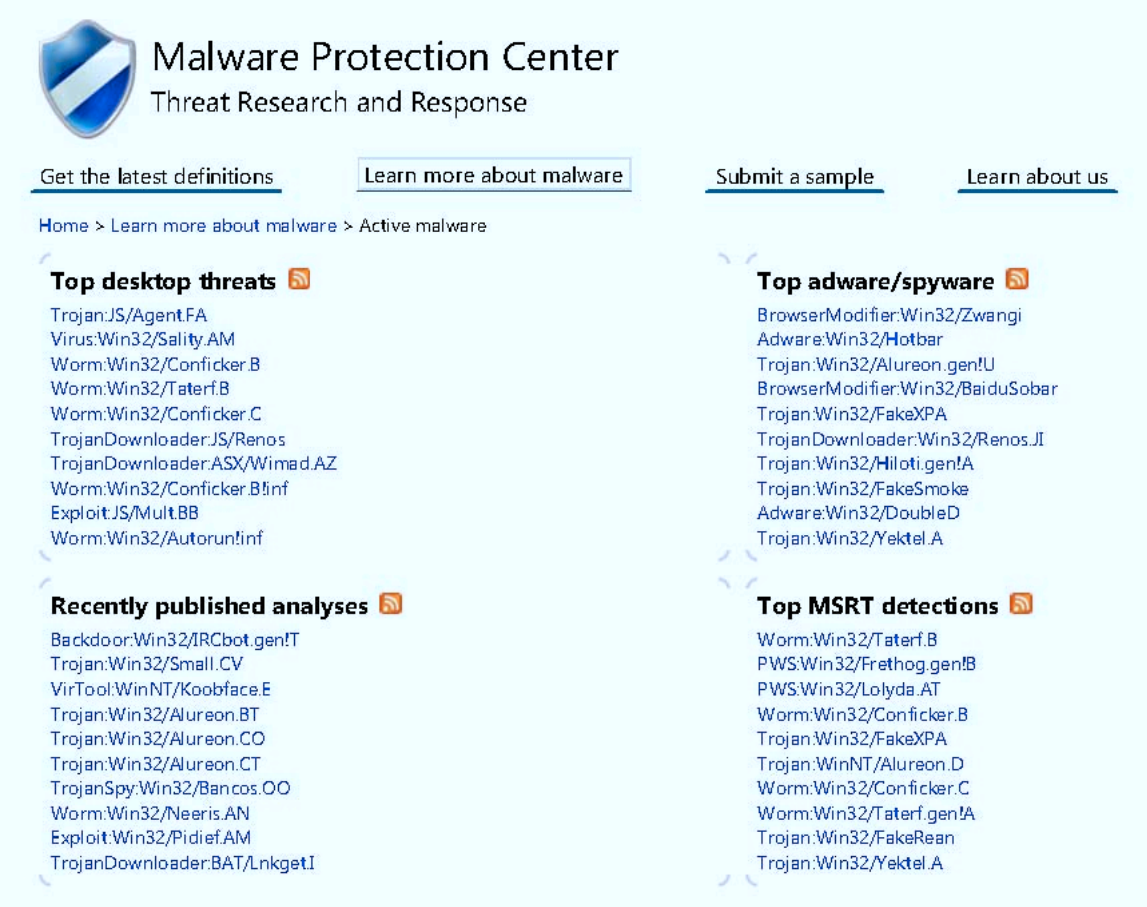
Related Jargon

- *Malware* – A general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.
- *Adware* – Any software which automatically plays, displays, or downloads advertisements to a computer after it is installed or while it is being used.
- *Spyware* – Any software that secretly monitors the user's behavior, such as Internet surfing habits, and collects various types of personal information. It can also interfere with user control of the computer in other ways, such as installing additional software, and redirecting Web browser activity.

Defensive Measures

- Authentication mechanism
  - Only authorized person can take certain actions
- Firewalls
  - Monitoring and filtering packets to/from Internet
- Software updates
  - Patching security holes
- Antivirus software
  - Routinely scanning hard drives for hidden viruses/worms
- Personal vigilance
  - Don’t click on email attachment if you don’t know the sender

Microsoft Malware Protection Center



Malware Protection Center

Threat Research and Response

Get the latest definitions | Learn more about malware | Submit a sample | Learn about us

Home > Learn more about malware > Active malware

Top desktop threats

Trojan:JS/Agent.FA
Virus:Win32/Sality.AM
Worm:Win32/Conficker.B
Worm:Win32/Taterf.B
Worm:Win32/Conficker.C
TrojanDownloader:JS/Renos
TrojanDownloader:ASX/Wimad.AZ
Worm:Win32/Conficker.B!inf
Exploit:JS/Mult.BB
Worm:Win32/Autorun!inf

Top adware/spyware

BrowserModifier:Win32/Zwangi
Adware:Win32/Hotbar
Trojan:Win32/Alureon.gen!U
BrowserModifier:Win32/BaiduSobar
Trojan:Win32/FakeXPA
TrojanDownloader:Win32/Renos.JI
Trojan:Win32/Hiloti.gen!A
Trojan:Win32/FakeSmoke
Adware:Win32/DoubleD
Trojan:Win32/Yektel.A

Recently published analyses

Backdoor:Win32/IRCbot.gen!T
Trojan:Win32/Small.CV
VirTool:WinNT/Koobface.E
Trojan:Win32/Alureon.BT
Trojan:Win32/Alureon.CO
Trojan:Win32/Alureon.CT
TrojanSpy:Win32/Bancos.OO
Worm:Win32/Neeris.AN
Exploit:Win32/Pidief.AM
TrojanDownloader:BAT/Lnkget.I

Top MSRT detections

Worm:Win32/Taterf.B
PWS:Win32/Frethog.gen!B
PWS:Win32/Lolyda.AT
Worm:Win32/Conficker.B
Trojan:Win32/FakeXPA
Trojan:WinNT/Alureon.D
Worm:Win32/Conficker.C
Worm:Win32/Taterf.gen!A
Trojan:Win32/FakeRean
Trojan:Win32/Yektel.A

Hacking and Network Attacks

Phone Phreaking — where hacking got started:

- Early 70s, AT&T started to use automatic switching equipments
  - Dialing was controlled by different *tones*
  - No security check
- Hackers built the little “blue box”, which could emit different tones, and enable them to make free long-distance calls
  - John Draper (“Captain Crunch”) *(c. 1970)*

Computer Hacking

- “Hacking” is used to be a positive term:
  - A "hacker" was a creative programmer who wrote clever code to make computers do things that have not being done before
  - A "hack" was an especially clever piece of code
- Hacking helped to start the PC industry
  - The Homebrew Computer Club (which includes the “ultimate hacker” Steve Wosniak)

Computer Hacking (cont.)

- Now “hacking” means gaining illegal or unauthorized access to a file or computer:
  - To transmit a virus or worm
  - To steal information
  - To intercept email or other data transmission
- Good vs. Bad Hackers:
  - *“Black Hat”* vs. *“White Hat”*
  - Some people suggest that bad hackers should be called *“Crackers”*

DoS: Denial-of-Service Attack

An intentional action designed to prevent legitimate users from making use of a computer service.

- *Goal of attack:* Disrupt a server's ability to respond to its clients
- About 4,000 Web sites attacked each week

Political Hacking (Hacktivism)

- Use of hacking to promote a political cause
- Disagreement about whether it is a form of civil disobedience and how (whether) it should be punished
- Some use the appearance of hacktivism to hide other criminal activities

Examples:

- Defacing government websites

Some Notable Hacking Cases

- *The 414s (c. 1982)*
  - A group of teenage hackers from Milwaukee
  - Broke into dozens of high-profile computer systems
  - Newsweek article: “Beware: Hackers at play”
- *Legion of Doom (c. 1984)*
  - An invitation-only hackers BBS
  - Published “The Legion of Doom Technical Journal”, teaching people how to hack
  - Some members, e.g. Robert Riggs, were convicted later

Catching Hackers

Law enforcement agents

- Read hacker newsletters and participate in chat rooms undercover
- Track a handle by looking through newsgroup archives
- Set up “honey pots” (i.e. websites that attract hackers) to record and study
- Use computer forensics to retrieve evidence from computers

Penalties for Hacking

- Computer Fraud and Abuse Act (1986)
  - Covers government computers, financial and medical systems, and activities that involve computers in more than one state, including computers connected to the Internet
- USA Patriot Act expanded the definition of loss
- Sentencing depends on intent and damage done
  - Maximum 20 years in prison + $250,000 fine
  - Most young hackers receive probation, community service, and/or fines

Operation Sundevil (1990)

A nation-wide US Secret Service crackdown on "illegal computer hacking activities".

- Targeted at credit card thieves and telephone abusers
- Conducted raids in 16 cities

The *Steve Jackson Games* Case –

Three years later, a federal court awarded damages and attorneys' fees to the game company, ruling that the raid had been careless, illegal, and completely unjustified.

Security vs. Civil Liberties

- Search and Seizure of Computers:
  - Requires a warrant; However, court rulings inconclusive about whether information found on computers (but not covered by a warrant) is considered in “plain view”
- Are Automated Search Programs Legal?
  - Can monitor constantly and less likely to miss suspicious activity
- Where should a Trial be Held?
  - The FBI usually files in the state where the crime was discovered and the investigation began

Whose Laws Rule the Web?

- Someone whose actions are legal in their own country may face prosecution in another country where their actions are illegal
- Even if something is illegal in both countries, the laws and associated penalties may vary
- Corporations that do business in multiple countries must comply with the laws of all the countries involved
- Freedom of speech suffers if businesses follow laws of the most restrictive countries

Notable Cases

- A Russian citizen was arrested for violating the DMCA when he visited the U.S. to present a paper at a conference; his software was not illegal in Russia
- An executive of a British online gambling site was arrested as he transferred planes in Dallas (online sports betting is not illegal in Britain)

Cybercrime Treaty

- International agreement to foster international cooperation among law enforcement agencies of different countries in fighting copyright violations, pornography, fraud, hacking and other online fraud
- Treaty sets common standards or ways to resolve international cases

Electronic Voting

2000 Presidential Election (Gore v. Bush)

Florida, 500 votes out of 2,000,000.

Manual system, voters punch out holes

Problem: Hole not fully punched

(hanging chads)

Problem: Ballor design was ambiguous

Electronic Voting

U.S. Total:		
Popular vote	**50,456,002**	**50,999,897**
Percentage	**47.9%**	**48.4%**
Florida:		
Popular vote	**2,912,790**	**2,912,253**
Percentage	**50.005%**	**49.995%**

Electronic Voting

Ideas:

Electronic voting machines

Prints out a marked ballot

Online: Go to website to cast vote

Electronic Voting

Benefits:

Makes voting easier

Votes can be counted quickly

Elections will cost less

No ambiguity about outcome

Eliminates ballot-box tampering

Can check ballot to make sure it's OK

Can enable complex votes (e.g., numbers)

Electronic Voting

Problems:

Gives advantage to wealthy computer owners

Privacy of voter may be compromised

Opportunities for vote selling

What about DoS attacks on election day?

Viruses: What if personal computers are infected?

Fake servers: Vote is changed and forwarded to the real election server.

Electronic Voting

"A secure Internet voting system is theoretically possible, but it would be the first secure networked application ever created in computing history."

– Bruce Schneier

Discussion Questions

- *Debate:* "Hackers do a public service by finding and publicizing computer security weakness."

- *Debate:* "Those who create nondestructive viruses and worms for patching security holes are doing the computer industry a favor."

Discussion Questions

- Do you think hiring former hackers to enhance security is a good idea or a bad idea? Why?

- U of Calgary offered a senior CS course "Computer Viruses and Malware," in which students learned how to write viruses, worms, and trojan horses, along with how to block them. Debate whether the university was wrong to offer the course.