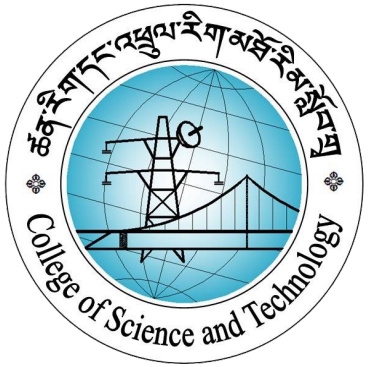


Bachelor of Engineering in Information Technology

ITM301 Professional Practices in IT

Unit V: Crime and Security

Mr. Yeshi Jamtsho
Lecturer

Overview

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

Undesired Programs

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

Computer Viruses

- **Computer Virus** is 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 **1971**, the ***Creeper*** virus was detected on ARPANET 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.
- Both programs created by Mr. Raymond Samuel Tomlinson,
  - American Computer Programmer
  - implemented the first email program on ARPANET system

Some Notable Virus

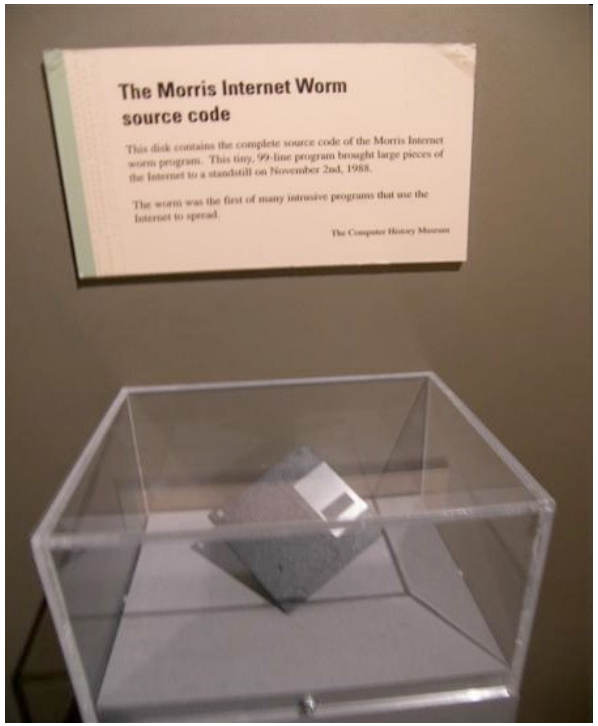
- *Brain (1986)*
  - 1st virus to move from one IBM PC to another
  - Spreaded through floppy disk
- *Michelangelo (1991)*
  - boot sector virus that infects the startup sectors of storage devices (floppy disk or master boot record (MBR) of a hard disk).
- *Melissa (1999)*
  - Attached to email, infected 100K computers
- *Love Bug (2000)*
  - Another email virus, deletes files and collects passwords

Computer worms

- **Computer worm** is 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 & 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

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

The Conflicker 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

Trojan Horses

- **Trojan Horses** is a malicious program which get downloaded and installed on the computer and be hidden within a host program. When the host 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 Virus 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 jargons

- ***Malware*** – A general term used by computer professionals to mean a variety of forms of intrusive/annoying software or program code.
- ***Adware*** – Any software which automatically plays/displays/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

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

Hacking and Networks

- *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”) *(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 computers on network**:
  - 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

- **DoS Attack** is 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 Websites 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*** *(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*** *(1984)*
  - An invitation-only hackers
  - 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:

1. **Read hacker newsletters** and **participate in chat** rooms undercover

2. Track a handle by **looking through newsgroup archives**

3. Set up "**honey pots**" (i.e. websites that attract hackers) to record and study

4. Use **computer forensics** to retrieve evidence from computers

Cybercrime in Bhutan

YOU MUST THROUGH THESE SITES

- https://www.rbp.gov.bt/cybercrime
- https://kuenselonline.com/index.php/news/cybercrime-liable-to-prosecution

Penalties for Hacking

- BICMA 2018

https://www.bicma.gov.bt/data/publications/act/BICM_Act_2018_English.pdf

- 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)

- US: 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

Security Vs Civil Liabilities

- 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 **Digital Millennium Copyright Act(**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)

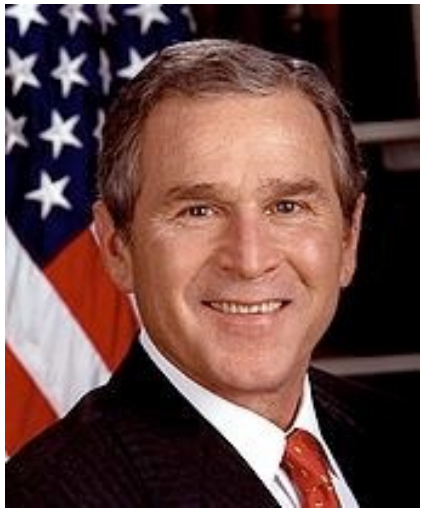
Cybercrime Treaty

- **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:	**50,456,002**	**50,999,897**
Popular vote		
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

- **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."

– by Bruce Schneier

Doscussion 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?

- University 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.

Thank you