

## Computer Security

Assoc. Prof. Pannipa  
Phaiboonnimit

Adapted for English Section by  
Kittipitch Kuptavanich  
and Prakarn Unachak

1

## Classification of Threats

- Computer Attack
  - Intend to damage files, computers and/or networks
- Computer Crimes
  - Use of computer or network technology in criminal activities
- [https://www.youtube.com/watch?v=AuYNXgO\\_f3Y](https://www.youtube.com/watch?v=AuYNXgO_f3Y)
- Source: code.org

Computer Ethics and Security

2

## Computer Attacks

- Malwares — Trojan, Worm, and Virus
- Denial of Service (DoS)

Computer Ethics and Security

3

## Malicious Software (Malware)

- Automated programs and/or actions that intend to cause damage to computers and network
- Self-replicating
  - Virus
  - Worm
- Non self-replicating
  - Trojan

Computer Ethics and Security

4

<http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html>

## Virus/Worm

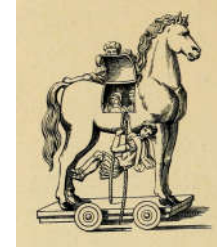
- Self-replicating
- Virus
  - Usually damage files
  - Can reside in important part of hard drive, such as boot sector
  - Can spread through e-mail attachment or USB drive
- Worm
  - Does not destroy files
  - Designed to copy and send itself through networks
  - Brings computers down by clogging memory

Computer Ethics and Security

5

## Trojan

- Trojan Horse
- Look like legitimate program
  - Trick user to install/ execute it
- Multiple possible actions
  - Annoying popup ads
  - Create backdoor and give access/control to the attacker
  - Damaging files/ systems
  - Hold computers/ files ransom



Computer Ethics and Security

6

## Denial of Service

- In computing, a **denial-of-service** attack (DoS attack) or **distributed denial-of-service** attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users.
- Generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.
- For DDoS, attackers usually have computers under their control (bot/zombies) repeatedly connect to the target, disrupting it.

Computer Ethics and Security

7

## Computer Crimes

- Unauthorized Access
- Cyber Stalking
- Fraud and Identity Theft
- Phishing, Scam and Hoax

Computer Ethics and Security

8

## Unauthorized Access

- Using computer systems with no authority to gain such access
- Other examples from the media
  - Employees steal time on company computers to do personal business
  - Intruders break into government Web sites and change information displayed
  - Thieves steal credit card numbers and buy merchandise

Computer Ethics and Security

9

## Hacking and Cracking

- Hackers
  - Someone who seeks and exploits weaknesses in a computer system or computer network.
  - Black Hat
    - Hack for criminal/malicious purpose
    - Blackmail / Data theft / Extortion
    - Damage systems for fun
  - White Hat
    - Hack for non-malicious reason (curiosity / security concern)
    - Test the systems, then alert authority / publish vulnerabilities
  - Grey Hat
    - Mix of Black and White

Computer Ethics and Security

10

[http://en.wikipedia.org/wiki/Hacker\\_\(computer\\_security\)](http://en.wikipedia.org/wiki/Hacker_(computer_security))

## Hacking and Cracking (2)

- Crackers
  - Break into computers with the intention of doing harm
- Hacktivists
  - Break into computer systems to promote political or ideological goals
- Script kiddies
  - Non-expert using tools made by others

Computer Ethics and Security

11

## Cyber Stalking

- Use of computer/network technologies to stalk or harass one or more persons
- Activities
  - Defamation
  - Gathering information
  - Identity theft
  - Monitoring (esp. on Social Network)
  - Threats

Computer Ethics and Security

12

<http://en.wikipedia.org/wiki/Cyberstalking>

## Identity Theft

- Pretending to be someone else, for malicious purpose
  - Criminal Identity Theft
    - Pretend to be someone else when arrested
  - Financial Identity Theft
    - Credit card, loans, etc
  - Identity cloning
    - Living as someone else
  - Medical Identity Theft
    - Using other's ID to obtain drug
  - Child Identity Theft
    - Using Child's ID
- Use information gather (partially) from the web

[http://en.wikipedia.org/wiki/Identity\\_theft](http://en.wikipedia.org/wiki/Identity_theft)

## Software Piracy

- Legal activities
  - Making one backup copy for personal use
  - Sharing free software (shareware or public domain software)
- Illegal activities
  - Making copies of purchased software for others
  - Offering stolen proprietary software (warez peddling)

## Other Computer Crimes

Type of Crime	Description	Recent Examples
Carding	Stealing credit card information for one's own use or to sell	A carder code-named Smak sells a CD with 100,000 credit card numbers to undercover law enforcement agents.
Cloning	Using scanners to steal wireless transmitter codes for cell phones, then duplicating the phone for illegal use	The practice was so prevalent in New York City in the mid-1990s that the mayor, police commissioner, and a city council member were victims.
Data diddling	Changing electronic data before or after it is entered on computers	A payroll clerk in a large company credits overtime hours to her own account, allowing her to steal hundreds of thousands of dollars from the company and her fellow employees.
Dumpster diving	Scouring wastebaskets and dumpsters for credit card receipts and other information, then using the information illegally or selling it	A young man in California impersonated telephone employees to gain access to equipment. He was so successful that he started his own telephone service before he was caught.
Phishing or spoofing	Attempting to trick financial account and credit card holders into giving away their authorization information, usually by posting false Web sites that duplicate legitimate sites	Many account holders at eBay, the popular auction Web site, were duped by a false Web site into giving up account numbers.

## Other Computer Crimes (2)

Type of Crime	Description	Recent Examples
Phreaking	Breaking into telephone systems to make free long-distance calls or for other purposes	Kevin Mitnick, who served prison time in California under computer crime statutes, allegedly impersonated telephone employees to get free telephone service.
Piggybacking or shoulder-surfing	Looking over a person's shoulder while he or she is using an automated teller machine, cell phone, or other device in order to steal access information	At the Port Authority Terminal in New York City, computer fraud officers have often arrested people using binoculars to filch codes from telephone calling cards.
Salami slicing	Stealing small amounts of money from a large number of financial accounts	A bank employee transfers one penny from the balance of thousands of accounts every day and puts the money in an account she has set up for herself. She accumulates hundreds of thousands of dollars before being discovered.
Social engineering or masquerading	Misrepresenting yourself in order to steal equipment or to trick others into revealing sensitive information	A person telephones a company employee and says he is working at home and needs certain information. He is lying but has enough genuine information to trick the employee into revealing network passwords. He then cracks the network and downloads proprietary information.
Vishing	Also known as voice phishing: instead of asking users to visit a Web site, asking users to call a fake telephone number and "confirm" their account information	An e-mail asks the recipient to call a phone number to confirm his credit card information. The fake phone number has been set up using VoIP technology, and the caller transfers his information to a scammer located somewhere around the globe, who is then able to run charges on the credit card.

## Example: Cryptowall

- Malware that uses encryption:  
<https://www.youtube.com/watch?v=ZghMPWGXexs>  
Source: code.org
- Usually disguised as harmless attachments on e-mails, tricking you to open them.
- Once activated, the cryptowall encrypts files on your computers (and sometime those in the same network)
- A random note if left on your computer, detailing how to pay the ransom to get your files decrypted.

Computer Ethics and Security

17

<https://blogs.sophos.com/2015/03/03/anatomy-of-a-ransomware-attack-cryptolocker-cryptowall-and-how-to-stay-safe-infographic/>

## Hoax

- Deliberately fabricated falsehood made to masquerade as truth.
- Distinguishable from:
  - Errors in observation or judgment
  - Rumors
  - Urban legends
  - Pseudoscience
  - April Fools' Day events that are passed along in good faith by believers or as jokes.
- Above is official definition, can also mean just unsubstantiated rumor spreading around the web.

Computer Ethics and Security

18

## How to Stay Safe Online

Computer Ethics and Security

19

## How to Stay Safe Online

1. Take cautions before clicking any link
2. Take **EXTRA** cautions before sharing any personal information
3. Set privacy setting on social network properly
  - Location
  - Personal post/information
4. Install (trustworthy) security programs
  - Antivirus
  - Antispyware
  - Backup
  - Firewall

Computer Ethics and Security

20

## How to Stay Safe Online (2)

5. Practice Password Discipline
  - Change password often
  - Use different passwords for different sites
  - Use strong password
6. Logout from Facebook/Google/etc. after you're done using public computer
7. Set password for lockout screen for your PC/Phone/Tablet

Computer Ethics and Security

21

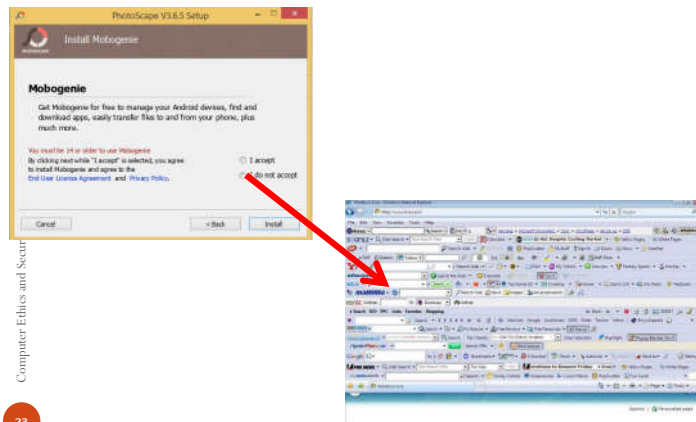
## Securing Your System

- As long as you have a computer and connect it to a network, you are vulnerable
  - Lock your computer when you are away
    - And set password to lockout screen
  - Disconnect your computer from the Internet when not being used.
  - Evaluate your security settings
    - Security Patches
    - Safeguarding your data
      - Anti-virus, password and encryptions, backups, separate user accounts

Computer Ethics and Security

22

## Be Careful of What You Click



Computer Ethics and Security

23

## Password Security

- Change password often
- Use different password for different sites
  - In case one got hacked
- Use strong password
  - Hard to guess, even if the attacker know your personal information
  - (Should not be so hard that you can't remember it)
  - Avoid: 123456, password, admin, pet's name
- Secret Question
  - Option to recover your account
  - Should you use correct answer?

Computer Ethics and Security

24

## Other Security Measure

- Biometrics
  - Use human characteristic and traits
  - Example: fingerprint, voice, face
  - Might not be practical
- Two-factor Authentication
  - Two components
    - Password + smart phone
    - Password + fingerprint

Computer Ethics and Security

25

## Backup

- A backup, or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event.
- Backups have two distinct purposes.
  - recover data after its loss
  - recover data from an earlier time
- Backup conditions
  - Periodically
  - Every change

Computer Ethics and Security

26

## Encryption/ Firewall

- Encryption
  - In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it
  - An authorized party, however, is able to decode the messages using a **decryption** algorithm.
- Firewall System
  - Firewalls impose restrictions on incoming and outgoing packets to and from private networks.
  - Only authorized traffic is allowed to pass through it.

Computer Ethics and Security

27

## Spam, Cookies and Spyware

- Spam
  - Unsolicited e-mail promoting products or services
  - Little protection available
- Cookies
  - Text file storing Web browsing activity
  - Help a website “remember” you
  - Can opt for cookies not to be stored
  - Web sites might not function properly without cookies
- Spyware
  - Software used for data collection without the users’ knowledge
  - Unlikely this activity will become illegal anytime soon

Computer Ethics and Security

28

## Top Free Antivirus (2013)

- Avast Free Antivirus
- Panda Cloud Antivirus Free
- ZoneAlarm Free Antivirus + Firewall
- Avira Free Antivirus
- Bitdefender Antivirus Free Edition



## Top Antispyware (2013)

- McAfee Virus Scan and Anti Spyware (not free)
- Navarre Webroot Spy Sweeper (not free)
- Lavasoft's Ad-Aware SE, Personal Edition
- Microsoft Windows Defender
- Spybot Search & Destroy

