Unit 1 - Hardware

Computer Security

What is *computer security*?

Measures that are taken to prevent computer systems from malicious attacks, theft, or accidents.

These include:

- Physical security: preventing theft of devices.
- Information security: preventing theft of private data.

Why would anyone *attack* a computer?

- Financial gain
- Vandalism
- Curiosity
- Proving superiority
- Revenge

Viruses

- **What is a virus?**
  - A virus is essentially a program that attaches itself to another program or file, enabling it to spread from computer to computer.
- **What does a virus do?**
  - The effects of a virus vary depending on its design.
  - Remember: Someone *made* that virus! It's effects are intentional.
- **How do I get a virus?**
  - Most viruses are attached to an executable file (.exe).
  - A VIRUS WILL NOT RUN ON YOUR COMPUTER UNLESS THE INFECTED FILE IS EXECUTED!
  - Generally, viruses do not spread without human interaction.

Worms

- **What is a worm?**
  - A worm is similar to a virus except that it can travel from computer-to-computer *without* human interaction.
- **How does the worm travel?**
  - It takes advantage of existing pathways of travel.
  - Common route: The worm is programmed to look for the computer user's address book and send copies of itself to everyone.
- **Why are worms so dangerous?**
  - People are careless – they see an email from a friend and despite how strange it appears, they open the attachment.

Famous Worms: Morris Worm

- **Big Idea:**
  - Used bugs in email programs built into operating systems to execute undesired code.
  - Spread from computer to computer, but did nothing else.

- **Why was it so dangerous?**
  - It re-infected the same computers over and over. This bogged down the computers and made them unusable.

- **Estimated Damages:** $10,000,000 USD

- **Famous Quote:**

  "There may be a virus loose on the internet."

  - Andy Sudduth of Harvard, 34 minutes after midnight, Nov. 3, 1988

Famous Worms: ILOVEYOU

- **Big Idea:**
  - Propagated as an email attachment in Outlook (email program) and mailed itself to all the users on the users' mailing list.
  - Changed the extensions of many files to .VBS and over wrote some others.
  - Also was known to steal passwords and credit card information.

- **Why was it so dangerous?**
  - One of the earliest worms to use email lists to propagate.

- **Estimated Damages:** $5.5 to 10 billion USD

- **Famous Quote:**

  "There may be a virus loose on the internet."

  - Andy Sudduth of Harvard, 34 minutes after midnight, Nov. 3, 1988

Famous Worms: Mydoom

- **Big Idea:**
  - Attacked Windows computers only.
  - Looked like a "Email not sent" failure message. Asked to resend by clicking on the attachment.
  - Once opened, it installed a copy of the worm on the host computer. Once installed, sends mail to address book contacts and also copied itself to shared folders of Peer-to-Peer networks.
  - It also opened a backdoor on the compromised PC to allow access to the hacker at anytime.
- **Why was it so dangerous?**
  - Spread quickly, left computers open ALL of the time.
- **Estimated Damages:** Over $22 billion USD
- **Interesting Fact:** Author not known!

Trojan Horse

- A Trojan horse is a virus that disguises itself as something you'd want (e.g. a free anti-virus software).

- Once opened, the Trojan horse typically opens a *backdoor* on the computer and alerts the controller of the access opportunity.

- Controller can connect to the infected computer and do some *really nasty stuff.*

Spyware

- Not really a virus.
- Spyware tracks your Internet movements (browser history, etc.) and sends targeted advertisements to you.
- This is often done through Internet *cookies* -- small files that websites put on your PC to store information about you and your browsing preferences.
- Malicious spyware will relay this information back to its owner. Some of this information could be private or financial data.

Malware

- *Malware* is a term used to refer to all of the discussed security threats.

- Malware comes from a number of sources:
  - Infected files
  - Infected programs
  - Exploits (using bugs in programs that haven't been fixed yet)

Exploits

- An exploit is a bug in a piece of software that a person can use to their advantage.

- Only a very small percent of the population knows about the exploit and therefore it remains unfixed by the software's creators until the knowledge is public.

- Many websites exist that are dedicated to notifying the public about exploits. This does two things:
  - Allows hackers to use the exploit to their advantage.
  - Forces the software creators to move quickly to release a fix.

- Windows often requires patch fixes for exploits.