Computer and Network Security

- **Virus:**
  - Self replicating code embedded within another program: the host.
  - Populate via e-mail attachments
    - Read e-mail address and sends itself to others.
  - Can be benign or malicious.
    - Simply copies itself and sends its self on.
    - Can overwrite system files, destroy files, etc.

- **Worms**
  - Self contained programs.
  - Spreads through a computer network exploiting security holes.
Trojan Horses
- A program with a benign capability that conceals another, sinister purpose.
- Opening an Internet connection allowing outsiders to again control/access.
- Key-logging and sending information to someone: get passwords.
- Simply scan your computer looking for passwords.
- Destroying files.
- Launch Denial of Service attacks.

Bot networks
- A program that responds to commands sent by a command-and-control program elsewhere.
- Has legit and illegal uses:
  - Internet Relay Client bots (IRC).
  - SPAM senders.
  - Denial of Service attacks.
Protection

- Authentication based computer access.
  - Only works if users use strong passwords: dictionary attack.

- Firewalls
  - Filter trusted packets.
  - Limit resources exposed to the Internet.

- Keep software up to date.

- Use SPAM filters for e-mail.

- Use anti-virus software.
Phreaks and Hackers

- Hackers: positive and negative meaning.
  - Originally there to explorer and learn systems and improve them.
  - Original hackers did it not to commit fraud or for personal profit.

- Freaking:
  - Manipulate the telephone system.
  - Get out of paying for calls.
  - Steal/Guess long distance access codes.
Denial of Service attacks

- Intentional action designed to prevent legitimate users from making use of a computer service.
- Goal is to disrupt services.
- Usually for some financial gain.
- Popular attack is SYN flood attacking.
  - Typically a single user: spoofing IP address.
- Other intents: Fill all available computer disk space.
  - e-mail bombing.
  - Worms that generate a large number of errors: servers log all the errors.
  - Gain access to a machine and copy large amounts of files to the computer.
- Distributed Denial of Service
  - Use bot-nets to do SYN type attacks.
Penalties

- There are severe penalties for hacking.

- Activities deemed hacking:
  - Transmitting that causes computer damage.
  - Accessing without authority any computer on the Internet.
  - Transmitting classified government information.
  - Committing computer fraud.
  - Committing computer extortion.

- Maximum penalty: 20 years in jail $250,000 fine.