Security

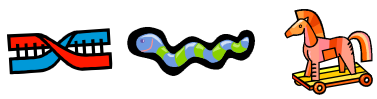
Attack and defense

Security

- Attacks
  - Malware
  - Spyware and phishing
  - Adware and spam
  - Abnormal behaviors
- Defenses
  - User management
    - Privilege control
  - Protections
    - Antivirus software
    - Auditing software
    - Firewall, spam filter
  - Encryption

Malware

- Infect programs/computers, erase data, slowdown performance…
- Types
  - Virus: attached to an existing program
  - Worm: a stand alone program
  - Trojan horse: disguised as valid files or programs



Spyware and phishing

- Spyware: collects information about users without their knowledge.
  - Keylogger: log the keys struck on a keyboard
  - Login sniffing: simulates the login process to get valid user name and password.
  - Network sniffing: intercept network messages
- Phishing: acquires information by masquerading as a trustworthy entity in an electronic communication

Adware and spam

- Adware: automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used.
- Spam: sends unsolicited bulk messages indiscriminately.
  - Email spam

Abnormal behaviors

- Dictionary attack: trying passwords derived from a list of words in a dictionary.
- Denial of service attack: overloading a computer (server) with messages to make a computer resource unavailable to its intended users.
- Spoofing attack: masquerading as a party other than one's self

User management

- To protect the computer's resource from access by unauthorized personnel.
  - User authentication process: Username, password, …
- Privilege control: To prevent malicious programs to execute dangerous instructions.
  - Nonprivilege mode: only "safe" instructions
  - Privilege mode: those instructions that can be only executed in the privilege mode are called privilege instructions.
  - Super user / administrator / root: a kind of user having higher privilege to control machines and operating system.

Protections

- **Antivirus software**: detecting and removing the presence of known viruses and other infections.
- **Auditing software**: detecting and preventing abnormal situations
- **Firewall:** filtering messages passing through computers.
  - Spam filter: firewall for email spam