Computer Security

Definition:

Computer Security is the ability of a system to protect information and system resources with respect to confidentiality and integrity.

Aspects of Security:

- Prevention: take measures that prevent your assets from being damaged
- Detection: take measures so that you can detect when, how, and by whom an asset has been damaged
- Reaction: take measures so that you can recover your assets or to recover from a damage to your assets

Analogy: Home Security

Analogy: Credit Card Security?

Computer Security - Goals

1. Confidentiality: Preventing, detecting or deterring the improper disclosure of information
2. Integrity: Preventing, detecting, or deterring the improper modification of data
3. Availability: Preventing, detecting, or deterring the unauthorized denial of service or data to legitimate users
4. Authenticity: Ensuring that users of data/resources are the persons they claim to be
5. Accountability: Able to trace breach of security back to responsible party

Confidentiality

- Prevent unauthorised disclosure of information
- Two aspects of confidentiality
  - Privacy: protection of personal data
    - e.g., personal medical records, student grade information
  - Secrecy: protection of data belonging to an organisation
    - e.g., Formula for a new drug, plans for the company for the next 5 years, Student Records

Integrity

- Detection (and correction) of intentional and accidental modifications of data in a computer system
- Various examples of modification
  - Corruption of hard drive
  - Changing course grades by breaking into university records
  - Transferring money from one account to another account fraudulently

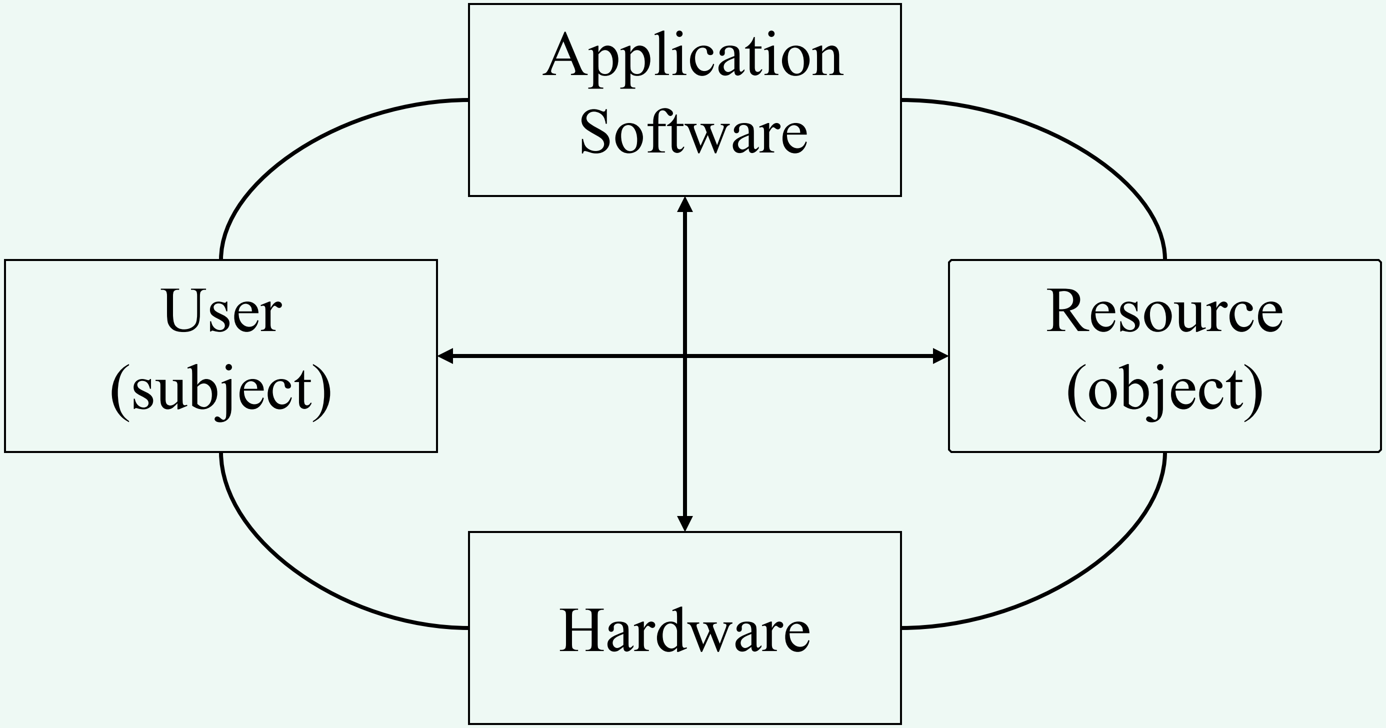
Availability

- The property that a product’s services are accessible when needed and without undue delay
- Denial of Service is the prevention of authorised access of resources or the delaying of time-critical operations
- Distributed Denial of Service occurs when multiple sources contribute to denial of service simultaneously

Accountability

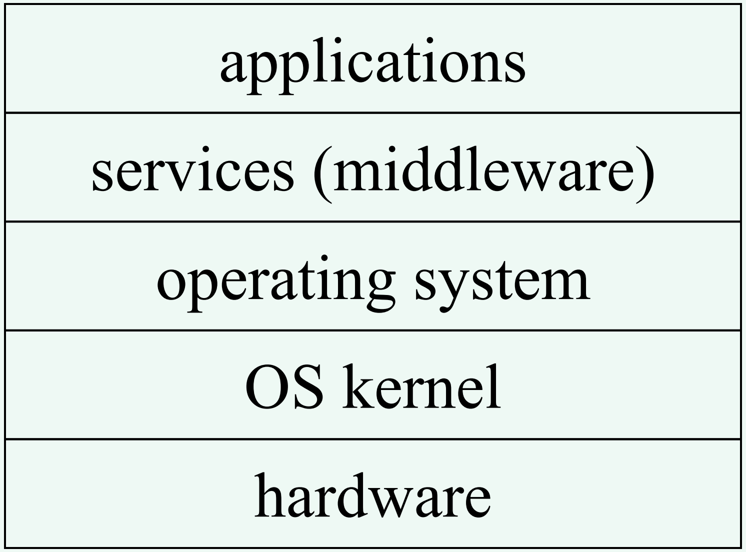
- Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party
- Users are identified and authenticated to have a basis for access control decisions.
- The security system keeps an audit log (audit trail) of security relevant events to detect and investigate intrusions.

Principles of Computer Security - I



- Where to focus security controls?
  - Data: Format and content of data
  - Operations: Operations allowed on data
  - Users: Access control of data based on user

Principles of Computer Security - II



applications

services (middleware)

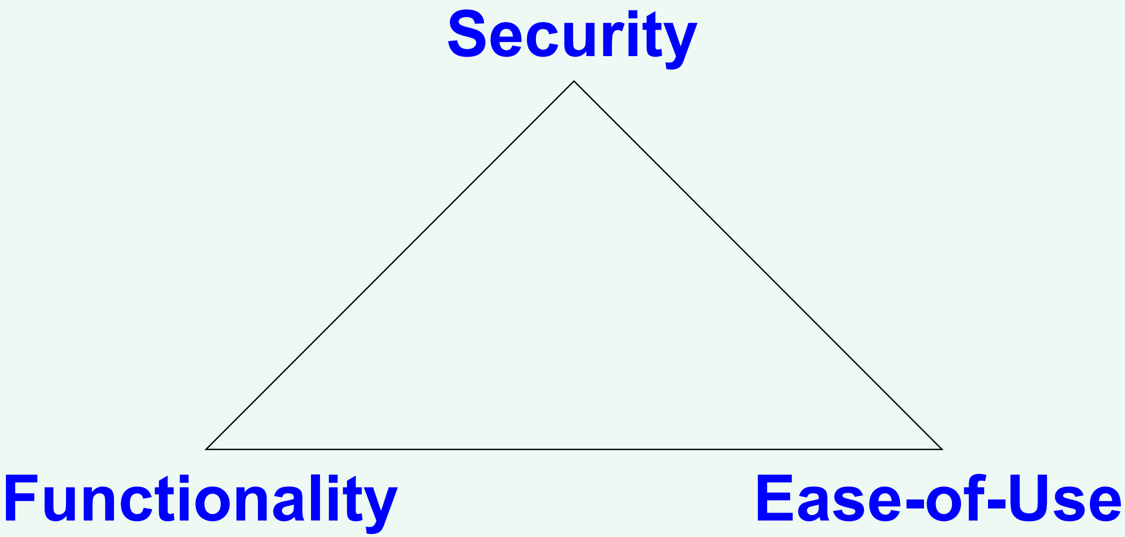
operating system

OS kernel

hardware

- Where to place security controls?
  - Lower layers offer more generic control
  - Higher layers allow most functionality and ease of use

Principles of Computer Security - III



Security

Functionality

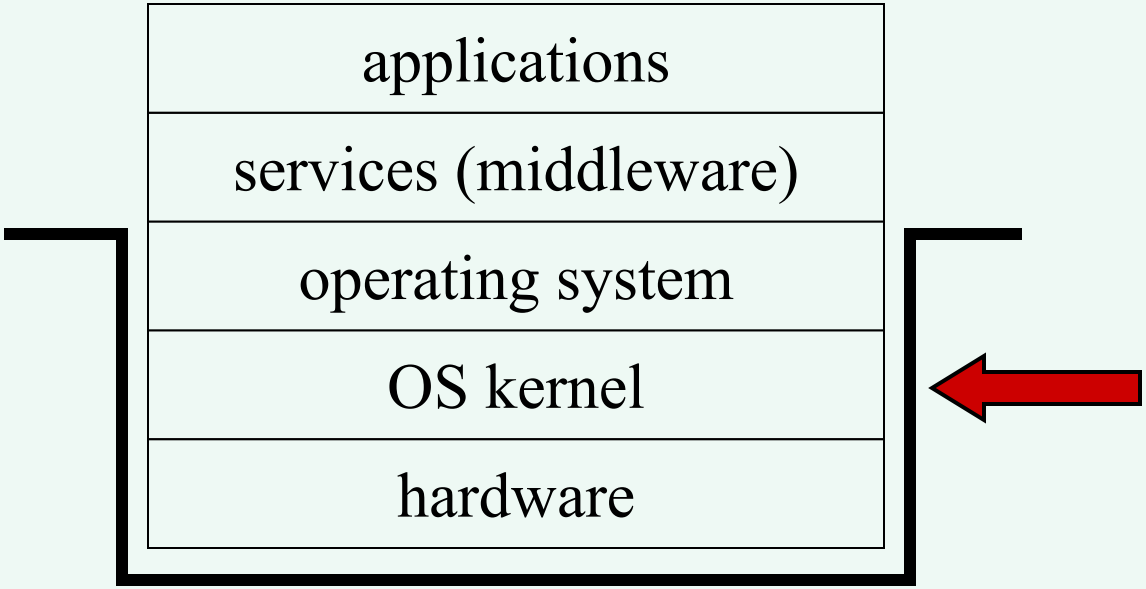
Ease-of-Use

- Security, functionality and ease-of-use linked together ?
  - Increasing Security hampers functionality & ease-of-use
  - Most secure computer is the one not plugged in and buried in 30 cu. ft. of concrete!

Principles of Computer Security - IV

- Centralized or Decentralized Security Control?
  - A central security authority provides much better control but may act as a bottleneck for productivity
  - A decentralized security control provides ability to fine tune security control for applications making system easy to use

Principles of Computer Security - V



applications

services (middleware)

operating system

OS kernel

hardware

Hackers attack at level below security perimeter

- How do you stop an attacker from getting access to a layer below your protection mechanism?
- Every protection mechanism defines a security perimeter (boundary). Attackers try to bypass protection mechanisms.

Principles of Computer Security – V cont'd.

- Tools to bypass protection mechanisms
  - Recovery Tools: These can read the hard disks byte-to-byte without acquiescing to high level security checks
  - Unix Devices: Unix treats physical memory devices like files, so, if improper access controls are defined a hacker can read disks
  - Backups: Backups are made to recover data in a computer crash. If not stored properly data can be read from the backup media

Security Policy

- A definition of information security with a clear statement of management's intentions
- An explanation of specific security requirements including:
  - Compliance with legislative and contractual requirements
  - Security education, virus prevention and detection, and business continuity planning
  - A definition of general and specific roles and responsibilities for the various aspects of information security program in business
  - an explanation of the requirement and process for reporting suspected security incidents, and
  - the process, including roles and responsibilities, for maintaining the policy document.

Source: IBM Consulting

Security Policy – Medical Records

- Medical records pose particular security problems. Assume that your medical records can be accessed on-line. On the one hand, this information is sensitive and should be protected from disclosure. On the other hand, in an emergency it is highly desirable that whoever treats you has access to your records. How would you draft your security policy and use prevention, detection and recovery to secure your records?