Introduction to Computer Security

Cunsheng Ding
HKUST, Hong Kong, CHINA
cding@cs.ust.hk

Outline of this Lecture

- A brief introduction to computer security
- A theoretical framework of computer security
- References on computer security

A Brief Introduction of Computer Security

Agenda of this Part

- Sources of threats to computer security
- Computer security aspects
- Potential Solutions

Sources of Threats to Computer Security

- Attackers on a computer system may be “insiders“ or “outsiders“.
- Is outside threat more serious than inside threat?

Sources of Threats: Internal versus External

- Is outside threat more serious than inside threat?
  - While the threat from outsiders is indeed as great as generally believed, the malicious insider with approved access to the system is an even greater threat!
  - Why?

Sources of Threats to Computer Security

- Various surveys, with results of order (Why?)
  - human error
    - For example, system administrator and users compromised password incidentally.
  - disgruntled (discontented) employees
  - dishonest employees
  - outside access

Inside Threat to Computer Security (1)

- Unauthorized entry into any compartmented computer system.
- Unauthorized searching/browsing through classified computer libraries.
- Unauthorized modification, destruction, manipulation, or denial of access to information residing on a computer system.

Inside Threat to Computer Security (2)

- Storing or processing <u>classified</u> information on any system not explicitly approved for classified processing.
- Attempting to circumvent or defeat security or auditing systems, without prior authorization from the system administrator.
- Any other willful violation of rules for the secure operation of your computer network.

Outside Threat to Computer Security (1)

In addition to foreign intelligence services, your computer network is at risk from many other types of outsiders.

- Freelance information brokers.
- Foreign or domestic competitors.
- Military people from adversary nations who are developing the capability to use the Internet as a military weapon.

Outside Threat to Computer Security (2)

- Terrorist organizations for which organized hacking offers the potential for low cost, low risk, but high gain actions.
- Crime syndicates and drug cartels.
- Hobbyist hackers who penetrate your system for sport or to do malicious damage.
- Common thieves who specialize in stealing and reselling laptop computers.

Threats in Summary

Users
Terrorists

Hackers
Criminals

Issue Motivated Groups

Foreign Intelligence

||
||
||
\/

Destroy

Disrupt

Modify

Disclose

Computer Security Aspects

- Personnel (human aspect => identification + auth.)
- Physical (machines => access control to rooms)
- Managerial (administration => security education)

- Data security
- Networking security
- Software security
- Operating systems security
- Hardware security
- Communication security

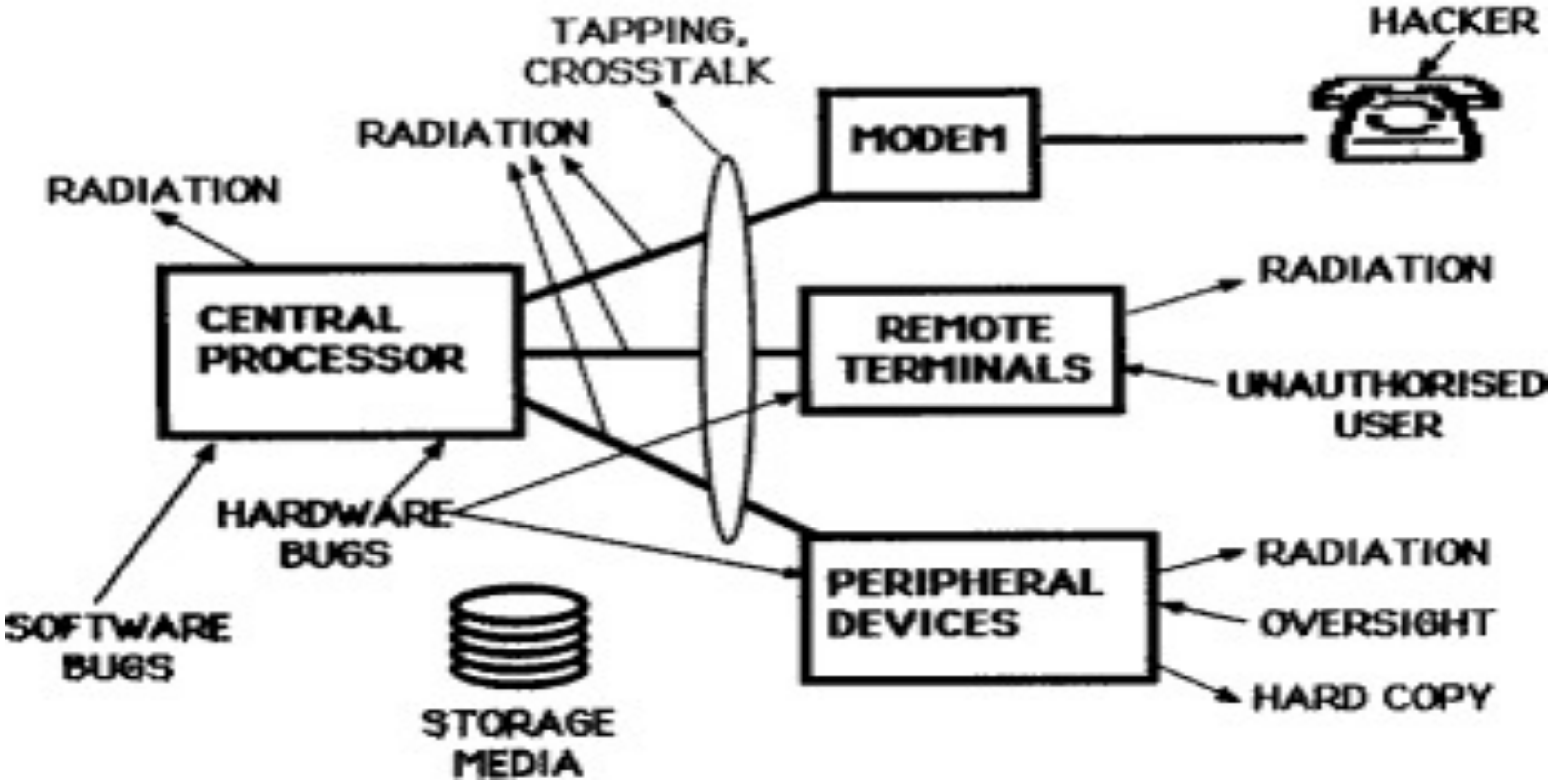
Potential Security Solutions

- Personnel - Access Tokens, Biometrics
- Physical - Integrated Access Control
- Managerial - Security Education
- Data Networking - Configuration control
- S/W & O/S - use "Trusted" systems
  - E.g., Use the logon screen provided by the OS
- H/W - h/w handshake (not covered in this course)

Assets in a Computer System

- Hardware
- Software
- Documentation
- Data
- Communications
- People

COMPUTER VULNERABILITIES



Countermeasures

A check or restraint is implemented to:

- Reduce threat (firewall)
- Reduce vulnerability (biometrics auth.)
- Reduce impact (backup data)
- Detect a hostile event (intrusion detect.)
- Recover from an event (software backup)

After giving a brief introduction to computer security, we now present:

A Theoretical Framework of Computer Security

Agenda of this Part

- Search for a definition of computer security
- Propose fundamental design principles for computer security

What is security?

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

Example 1 - Private Property

- Prevention: locks at doors, window bars, walls round the property.
- Detection: burglar alarms, closed circuit TV.
- Reaction: calling the police, replace stolen items, make an insurance claim.

Example 2 - eCommerce

- Prevention: use encryption when placing orders, rely on the merchant to perform checks on the caller.
- Detection: an unauthorized transaction on your credit card statement
- Reaction: complain, ask for a new card number, etc.

Prevention Aspects

- Confidentiality: preventing unauthorized disclosure of information
- Integrity: preventing unauthorized modification of information
- Availability: preventing unauthorized with-holding of information or resources

Confidentiality (Prevention)

- Prevent unauthorized disclosure of information (prevent unauthorized reading)
- Question: How to achieve confidentiality?
  - Encryption (cryptography)

Integrity (Prev. + Det.)

- No unauthorized and malicious alteration or destruction of data or software stored in computer.
- **Question**: How do we check data integrity?
  - Cryptography

Integrity (Prev. + Det.) ctd.

- Software integrity is crucial for computer security.
- Integrity is a prerequisite for many other security services.
- Operating systems security has a lot to do with integrity.

Availability (Prevention)

- Availability: The property of being accessible and usable upon demand by an authorized entity
  - Email service
- Denial of Service: The prevention of authorized access of resources or the delaying of time-critical operations
  - DoS attacks on an email server
- *Availability may be the most important aspect of computer security, but there are few methods.*

Accountability (Detection)

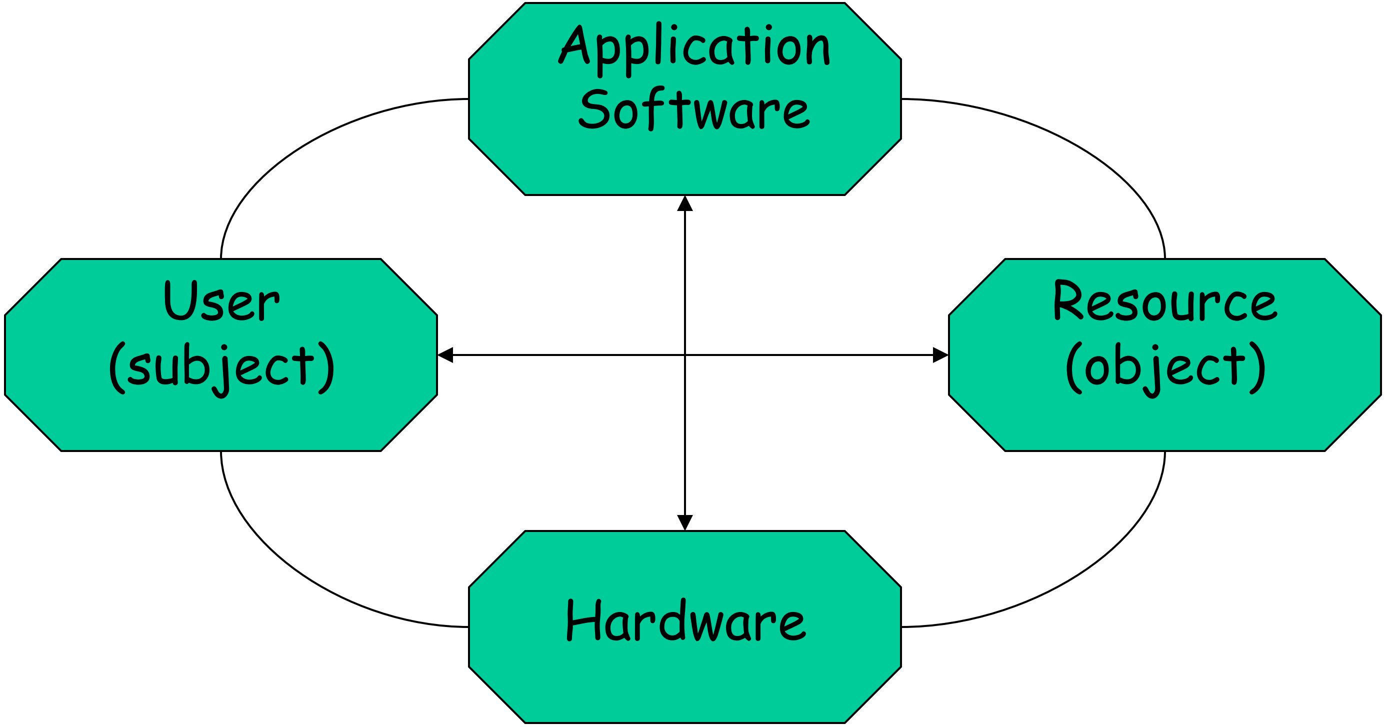
- Accountability: audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party. E.g., “su” command in Unix
- Users are identified and authenticated to have a basis for access control decisions.
  - ID + Password: Students and professors have different access rights
- The security system keeps an audit log (audit trail) of security relevant events to detect and investigate intrusions.

The main conclusion

- There is no single definition of security
- When reading a document, be careful not to confuse your own notion of security with that used in the document.
- Our definition: computer security deals with the prevention and detection of unauthorized actions by users of a computer system.

Principles of Computer Security

The Dimensions of Computer Security



1st Fundamental Design Decision

What is the focus of security controls?

- **Integrity follows a given set of rules on**

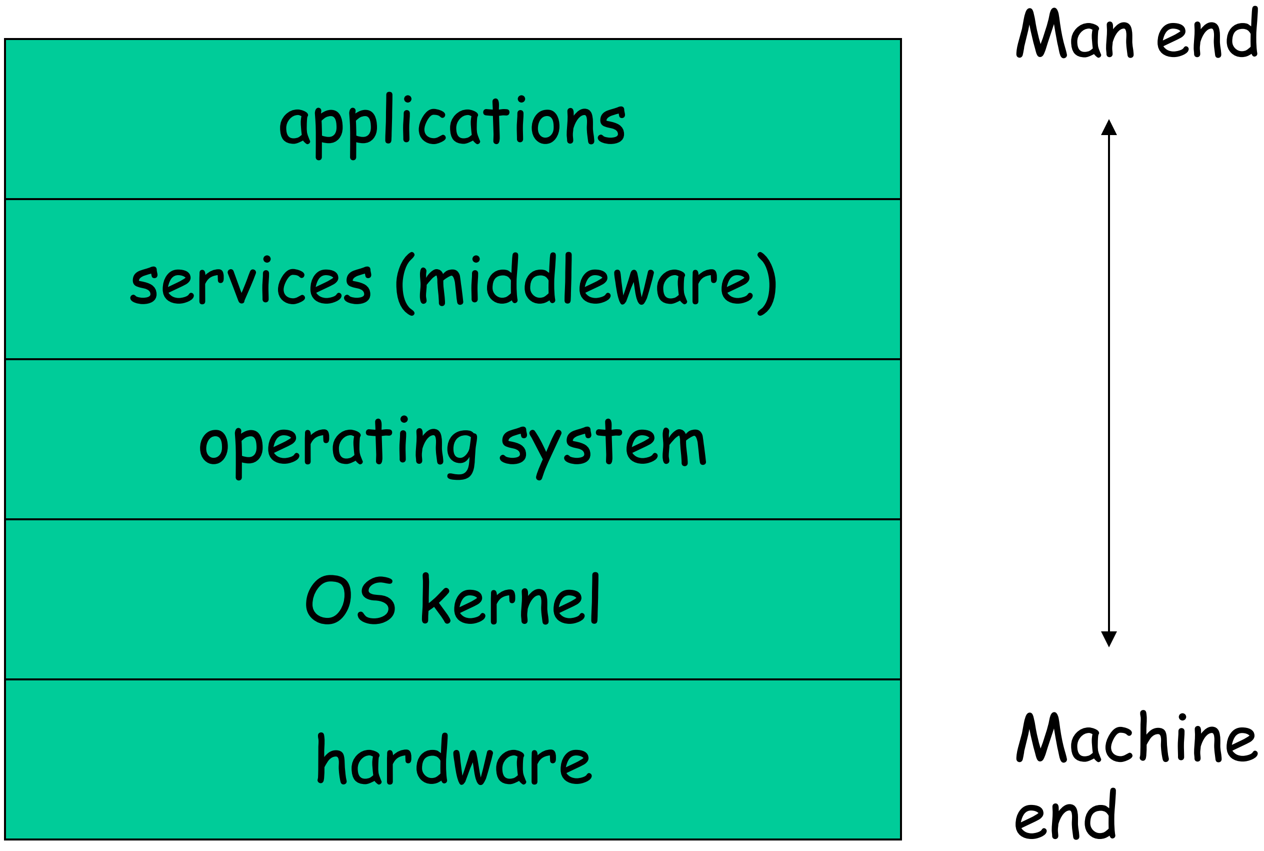
  1) the format and content of data items

  - 2) the operations that may be performed on a data item
  - 3) the users who are allowed to access a data item (authorized access)

- **Security controls can focus on**
  - 1) data
  - 2) operations
  - 3) users

2nd Fundamental Design Decision

Where to place security controls?



applications

services (middleware)

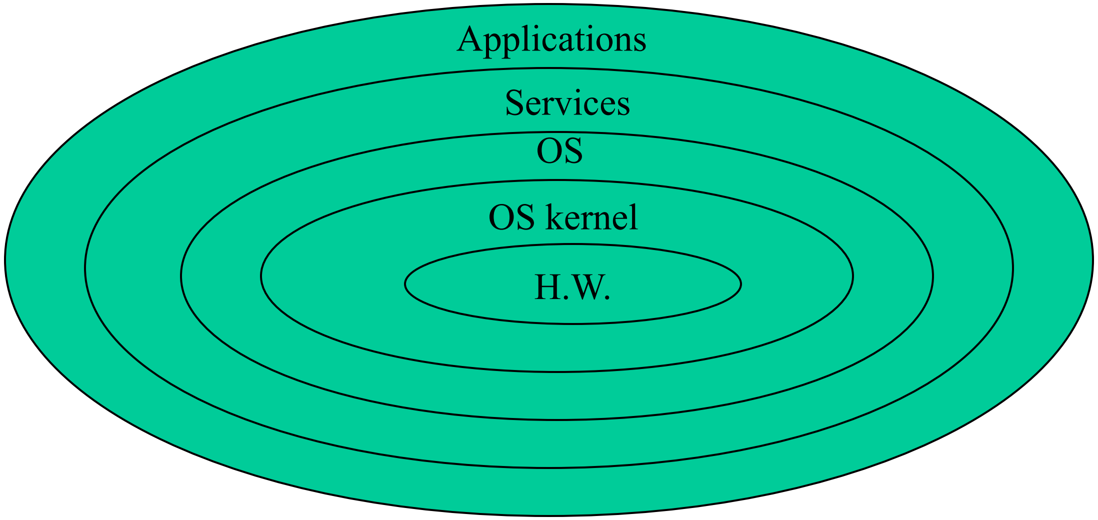
operating system

OS kernel

hardware

The Man-Machine Scale

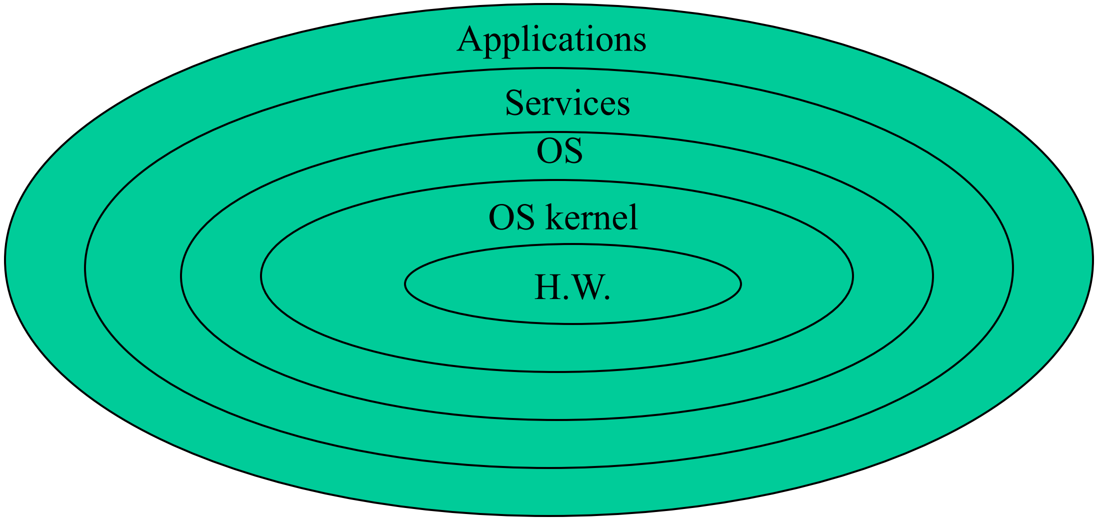
- Security mechanisms can be visualized as concentric protection rings, with hardware mechanisms in the **center** and application mechanisms at the **outside.**



The Onion model of protection mechanisms

The Man-Machine Scale

- Security mechanisms towards the **center** tend to be more **generic** while security mechanisms at the **outside** are more likely to address individual user requirements



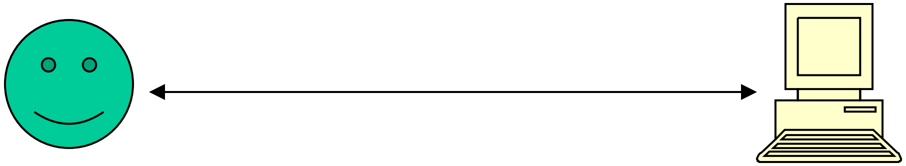
The Man-Machine Scale

- Combining our first two design decisions, we refer to a man-machine scale for security mechanisms.

The Man-Machine Scale

specific
complex
focus on users

generic
simple
focus on data



man
oriented

machine
oriented

3rd Fundamental Design Decision

complexity vs assurance

- Frequently, the location of a security mechanism on the man-machine scale is related to its complexity.
  - If it is put at the application layer, then it is usually more complex (it can provide a higher level of security).
  - If it is put in the center, it is simpler and generic, but may not provide a higher level of security.
- You find simple generic mechanisms, while applications often clamor for feature-rich security functions.
  - "IPSec" can provide security for many types of data, including email data, and is thus generic. But "PGP" can provide the "sender nonrepudiation" security service.
- The fundamental dilemma: simple generic mechanisms may not match specific security requirements. [Shirt design problem]

3rd Fundamental Design Decision complexity vs assurance

- There is an obvious trade-off between *complexity* and *assurance.*
  - Usually, a very secure system must be complex enough.
- *Simplicity and high assurance do not match easily.*
  - A simple security mechanism may not provide the required security level and security features.
  - A complex security mechanism may not be secure if it is not well designed.

4th Fundamental Design Decision

centralized or decentralized controls?

- Within the domain of a security policy, the same controls should be enforced.
  - E.g., within the HKUST domain of Windows machines, the same controls should be done.
- If a *single entity* is in charge of security, then it is easy to achieve uniformity, but this central entity may become a performance bottleneck.
- *A distributed solution* may be more efficient but you must take added care to guarantee that different components enforce a consistent policy.

4th Fundamental Design Decision

centralized or decentralized controls?

Question:

- Should the tasks of defining and enforcing security be given to a central entity or should they be left to individual components in a system?

Answer:

- It depends on what you want.

Security Evaluation

- Security evaluation checks whether a product delivers a promised security service. We must state

  1) the function of the security system

   2) the required degree of assurance (trust) in its security

- To achieve a high degree of assurance, the security system must be examined **exhaustively** and in close detail.

Books on Computer Security

- C.P. Pfleeger: Security in Computing, Prentice-Hall, 1997
- E. Amoroso: Fundamentals of Computer Security Technology, Prentice-Hall, 1994
- Ernst & Young: Logical Access Control, McGraw-Hill, 1993
- M. Gasser: Building a Secure Computer System. Van Nostrand Reinhold, 1988
- D. Gollmann: Computer Security, Wiley & Sons, 1999

Appendix

Blocking access to the layer below

- Every protection mechanism defines a security perimeter (boundary).
- Attackers may **bypass** protection mechanisms at some layer.
- How do you stop an attacker from getting access to a layer below your protection mechanism?
- **Example**: You just arrived at a hotel with 900 security guards who stand around it. One may carry out a tunnel attack which bypass the protection.

The Layer Below - Example

- <u>Unix</u> treats I/O <u>devices</u> and physical memory devices like files.
- If access permissions are defined badly, e.g. if read access is given to a disk containing read protected files, then an attacker can read the disk contents and reconstruct the files.

The Layer Below - example

- Object reuse: in a single processor system, when a new process becomes active, it gets access to memory positions used by the previous process.
- You have to avoid storage residues, i.e. data left behind in the memory area allocated to the new process.

The Layer Below - Example

- **Backup**: whoever has access to a backup tape has access to all the data on it.
- Logical access control is of no help and backup tapes must be locked away safely to protect the data.