Computer and Communications Security

COMP4631

Cunsheng Ding

cding@ust.hk

https://www.cse.ust.hk/faculty/cding/COMP4631/

Outline of this Lecture

- Brief introduction to COMP4631
- Physical security: an important step towards understanding computer security

Course Introduction

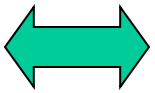
Course Structure

Core theory

encryption

authentication

digital signature



Practice

Unix security

Distributed system security

Network security

Web security

Course Structure & Grading

Lecture	Tutorial x

Grading:

Four assignments (28%), in-class quizzes (32%), final exam (40%)

In-Class Quizzes

- At the end of a lecture, 6 minutes are reserved for a quiz on the content of this lecture.
- Not every lecture is followed by a quiz (it depends on whether at the end of the lecture we have time left for it or not). Hence, the total number of quizzes is unknown.
- The marks of your best performed 12 quizzes will be counted towards your final grade. Hence, missing several quizzes will **not** be a problem.
- The purposes of the in-class quizzes are to activate your in-class learning and enhance your success in this course.
- **Please do not take this course** if you cannot come for most of the quizzes!

Main Topics

- Computer security: an introduction
- Conventional cryptosystems
- Public-key cryptosystems
- Key management
- Hash functions, authentication
- Digital signature, identification
- Access control
- Unix security
- Distributed system security
- Network security

Main Topics ctd.

- Email security
- Web security
- Firewalls
- Virtual private networks

Reference Books

- Behrouz A. Forouz, Cryptography and Network Security, McGraw Hill, 2008.
- D. Gollmann, Computer Security, John Wiley & Sons, 1999.
- W. Stallings and L. Brown, Computer Security: Principles and Practice, Pearson Education, 2008.

Learning Outcomes

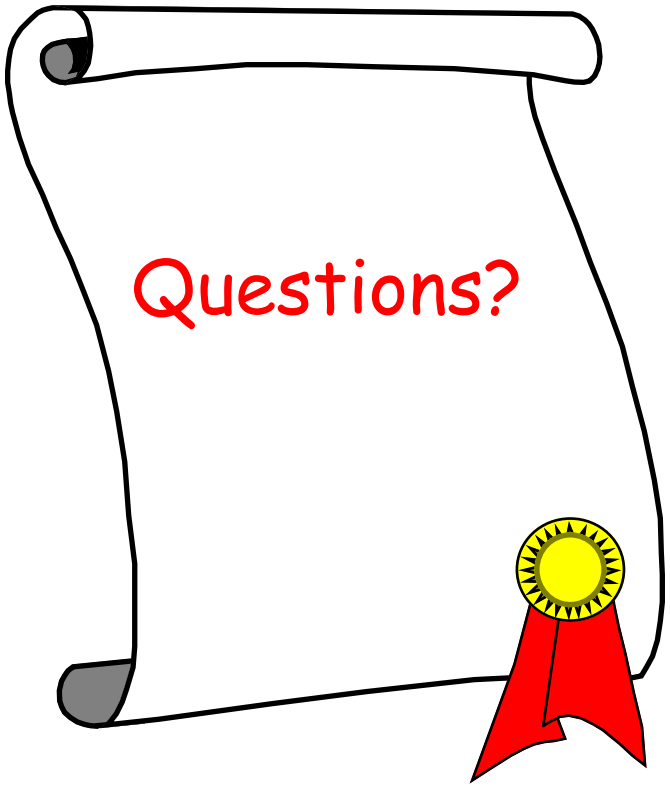
On completion of this course you will be able to:

1. evaluate potential vulnerabilities and attacks on computer and communication systems;
2. learn the basic security tools;
3. select and apply basic tools to build security systems; and
4. get familiar with real-world security systems.

Prerequisites:
Discrete mathematics

Important Information

Take this course only if you have time to visit lectures (due to in-class quizzes), and work out assignments.


Questions?

Physical Security:
The first step towards understanding computer security

Definition of Physical Security

- Physical security refers to the protection of building sites and equipment (and all **information** and **software** contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee).

Definition in Wikipedia

- **Physical security** describes measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media.
- It can be as simple as a locked door or as elaborate as multiple layers of "armed guardposts".

Armed Guard Post

Security System

- Security model
  - No wood, no walls, only three guards.
  - Can be placed anywhere
- Security policies
  - The duties of each guard
  - Centralized or decentralized
  - How often should they move?
- How to implement the policies?

Armed Guardpost

Physical Security: Example

- Your house
- A cash room in a bank

Elements of Physical Security

The field of security engineering has identified three elements to physical security:

- Obstacles, to frustrate trivial attackers and delay serious ones. (Prevention)
- Alarms, security lighting, security guard patrols or closed-circuit television cameras, to make it likely that attacks will be noticed. (Detection)
- Security response, to repel, catch or frustrate attackers when an attack is detected. (Response)

In a well-designed system, these features must complement each other.

A computer security system has also three steps.

Design of Physical Security

There are three layers of physical security:

- Environmental design (prevention step)
- Mechanical and electronic access control (prevention step)
- Intrusion detection (detection step)

Environmental Design

- The initial layer of security for a campus, building, office, or physical space.
- It is used to deter threats.
- Examples: warning, fences, metal barriers, vehicle height-restrictors, site lighting.

Mechanical & Electronic Access Control

- The second layer of physical security
- Examples:
  - Doors with locks
  - Doors with security guards
- Access control policy is implemented. Only authorized people are allowed.

Intrusion Detection

- The third layer is intrusion detection systems or alarms.
- Intrusion detection monitors for attacks.
- It is less a preventative measure and more of a response measure.

Violating Physical Access Control

- **Masquerading**: A person disguised as an authorized user. This can be done using a forged ID or pretending to be a repair man.
- **Piggy-backing**: A person who enters the security perimeter by following an authorized user.

Violating Physical Access Control

- **Lock-picking**: Any lock can be picked. Or better, go through dropped ceilings or removing the hinges from door.
- http://www.wikihow.com/Pick-a-Lock-Using-a-Paperclip
- The Complete Guide to Lock Picking
  - https://repo.zenk-security.com/Lockpicking/The%20Complete%20Guide%20To%20Lockpicking%20-%20Eddie%20the%20Wire%20-%20Loompanics.pdf

Violating Physical Access Control

- **Visual/auditory access**:

- **Example:** Russians spied on Americans by installing a telephone near a code-room. They got the secret key by hearing **electric balls** on typewriters.

A Case Study of Physical Security

A Real-World Example

- Problem: Suppose you are the President of a country called The New Empire. You have ordered the killing of many innocent people in the world and have thus got many enemies. You would build a house as both your working office and residential place, which provides you as much security as possible.
- Given a fixed amount of money for doing this, how would you build a secure house?

Some Design Requirements

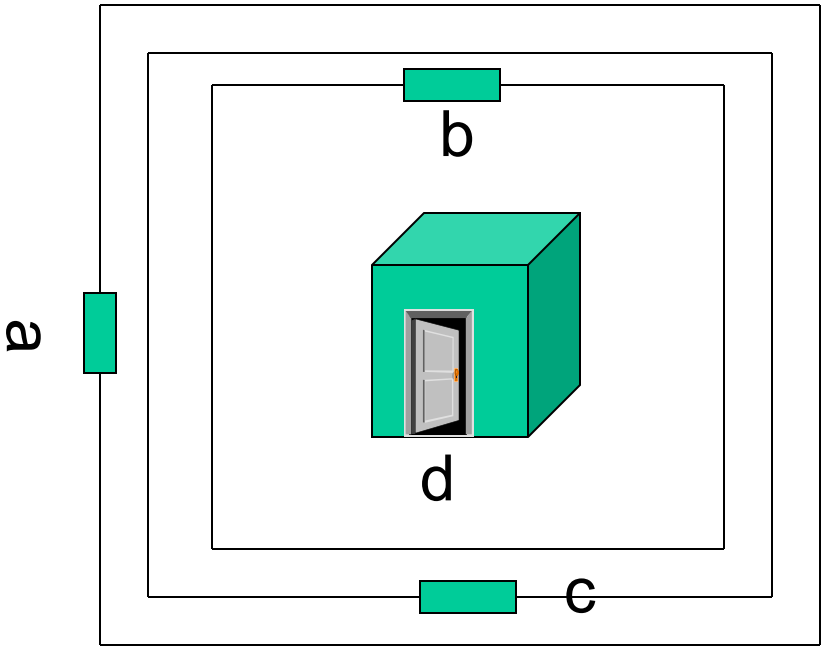
- The house should have at least one entrance door which is controlled by a (physical or electronic) lock or guard.
- It should have at least one window for getting sunlight.
- It should accommodate you (the President) and your spouse.
- It should provide a "certain level" of security.

Possible Attacks

- Biological attacks from the air (you have to breath).
- Missile attacks from the air.
- Break-in from the entrance door (there must be at least one door).
- Tunnel attacks.
- Fire break.
- Attacks from your spouse and security guards.
- Can you find out all possible attacks?

Security Model

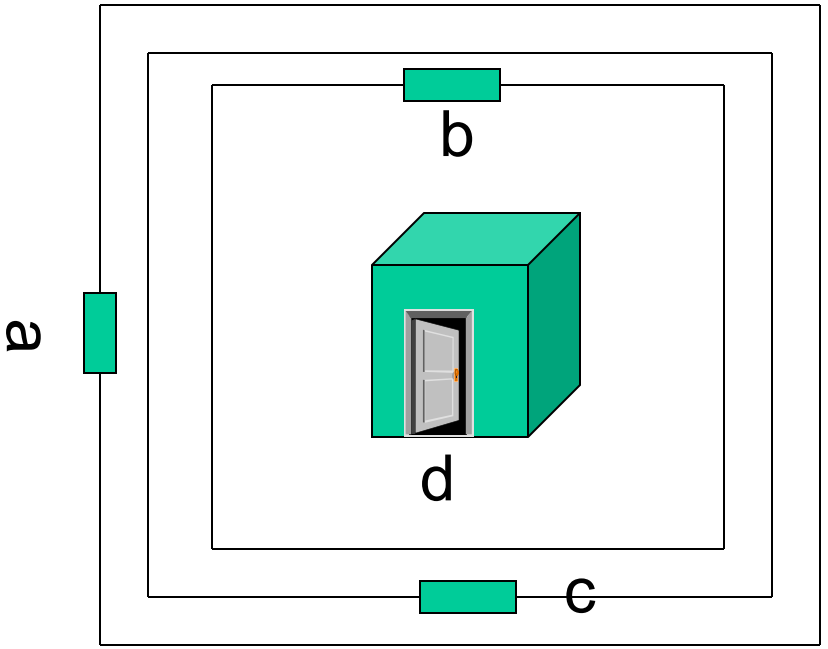
- Chinese Wall Model (other models too, e.g. the guard post model)
- Human-machine approach (security guards + locks)
- Security policy: access control



The First Design Decision:

what is the focus of security controls?

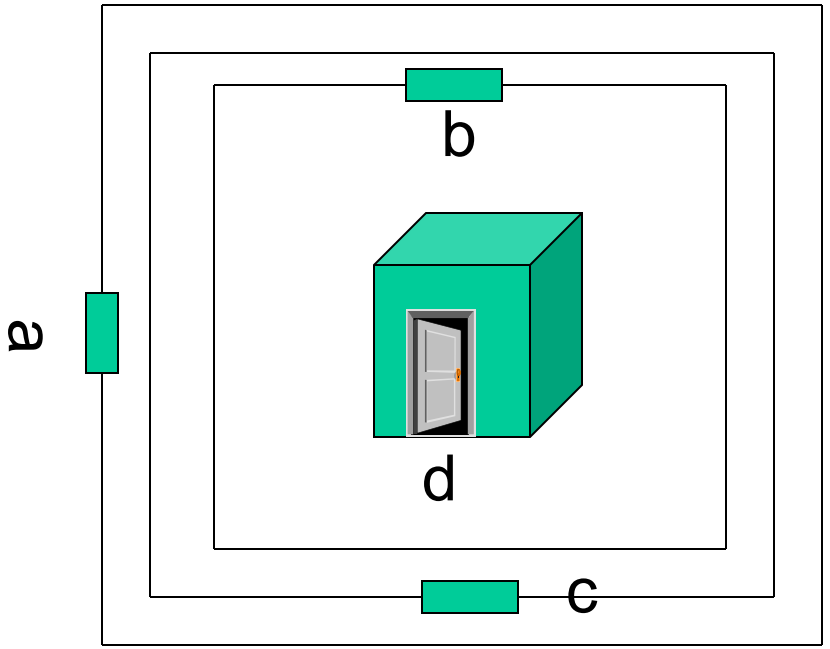
- Access control on the doors, assuming that
  - all the walls are tall enough;
  - all the walls are very strong;
  - all doors are very strong.



The Second Design Decision:

where to place security controls?

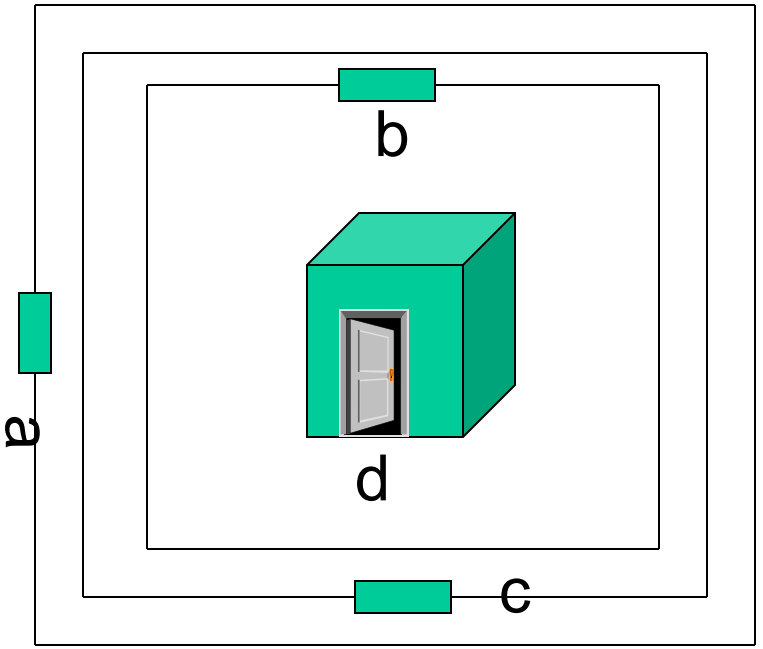
- The doors:
  - The man approach: guards only
  - The machine approach: locks only
  - man-machine approach: a combination
- Which approach is better?



The Second Design Decision:

where to place security controls?

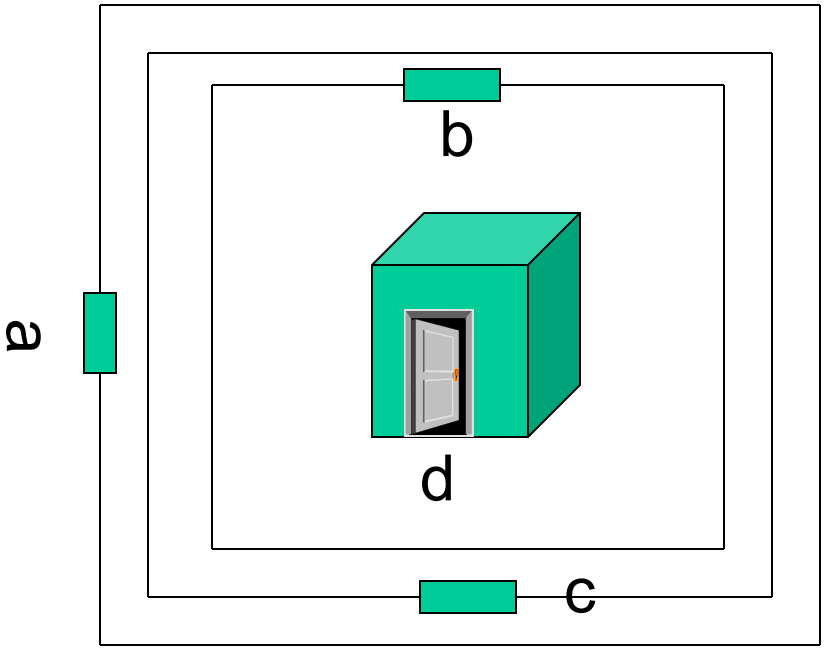
- The man approach
  - It is possible for one single person to use her/his beauty or detrimental gas to settle all the guards.
  - Possible to bribe all.
  - If one lock is used, this may not be possible.



The Second Design Decision:

where to place security controls?

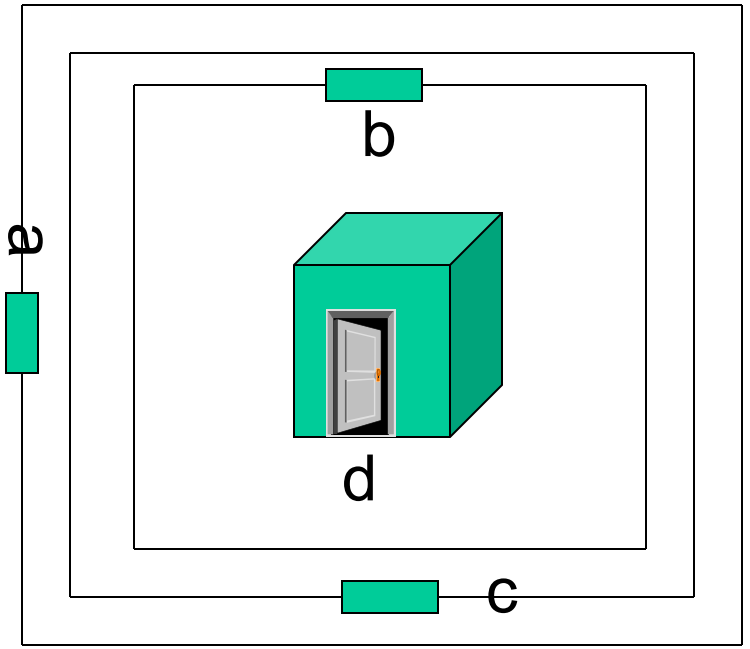
- The machine approach
  - What happens if you have a heart attack?
  - In case of fire and you cannot find the key to door D, what will happen?



The Second Design Decision:

where to place security controls?

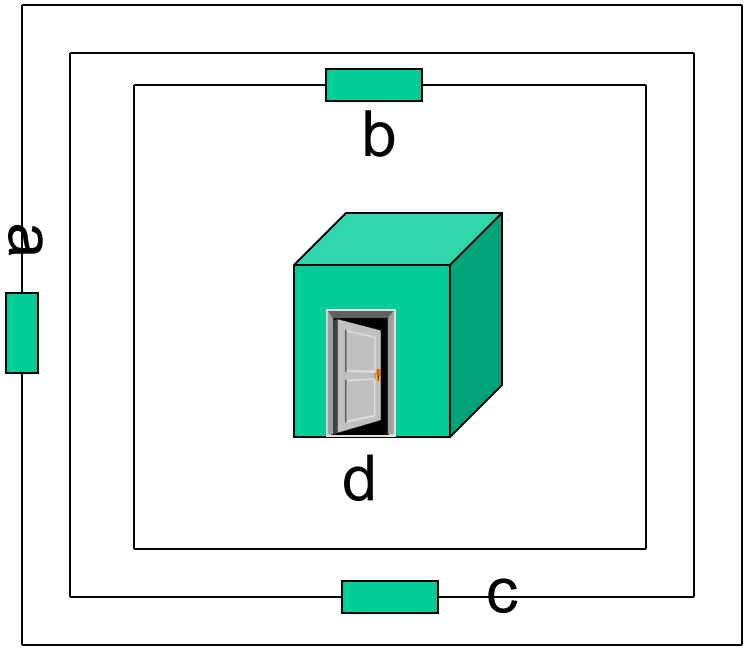
- Conclusion:
  - Man-machine approach is better!
- Questions:
  - How many locks and how many guards?
  - Which doors are controlled by locks and guards?
  - Male or female?



The Third Design Decision: simplicity and assurance (1)

- Access control policy:
  - For each door define who has access right.
  - The access control on door D is crutial (why).

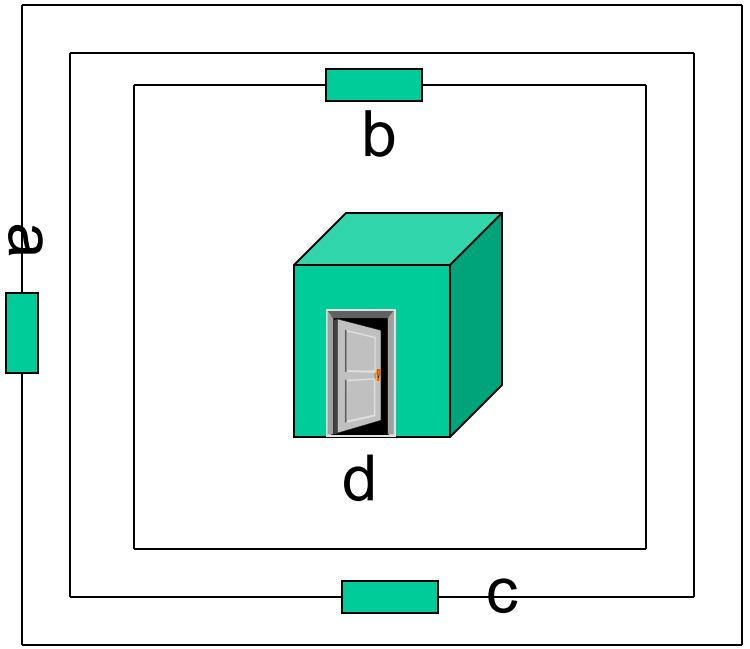
  - Guard at A is not allowed to access other doors. Guard at D is not allowed to cross A without the permission of the President.



The Third Design Decision:

Simplicity and assurance (2)

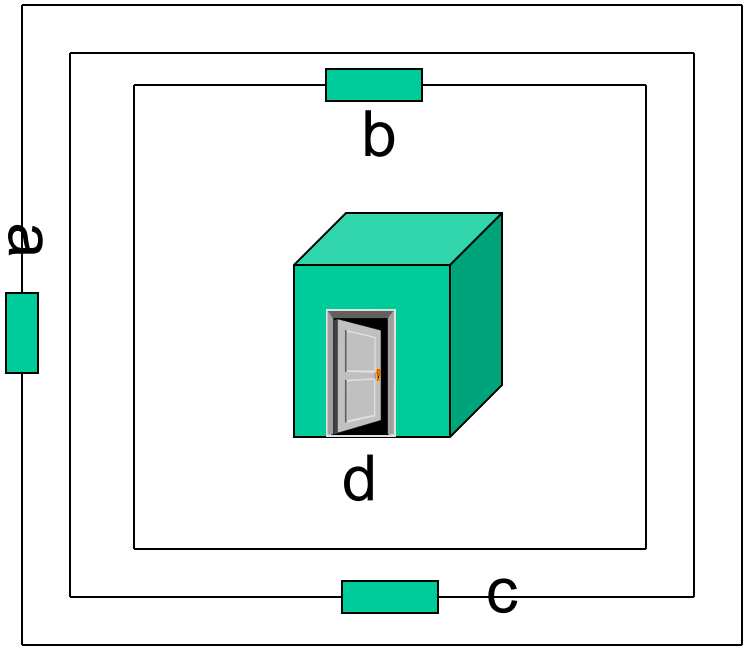
- Complicated access control policy makes it less efficient.
- Simple policy does not give enough security assurance.
- Solution: compromise



The Fourth Design Decision:

centralized or distributed?

- How to coordinate the access controls of all doors?
- In case of doubt, which guard makes the final decision?



Security Evaluation

- Remark: Once you have finished designing your house, you must evaluate whether your system meets all the security requirements.
- Question: Is it easy to prove or disprove that a security requirement is met?

Absolute Secure System?

- Question A: Is there any absolute secure system in the world?
- Question B: Could you enumerate all possible attacks on the system?
- Concluding remark: It is extremely hard to design a secure system!

Physical Security

- Physical security helps
  - not only understand computer security;
  - but also strengthen computer security.
- Physical security is combined with information security in many real-world applications.

Importance of Physical Security

- Physical security is a vital part of any security plan and is fundamental to all security efforts.
- Without it, information security, software security, user access security and network security are considered more difficult, if not possible, to initiate.

More on Physical Security

- **http://www.cpni.gov.uk/advice/Physical-security/**
- **http://physicalsecurity.com/**
- **https://nces.ed.gov/pubs98/safetech/chapter5.asp**