Chapter 1:
Introduction to Information Systems Security

Faculty of Computer Science & Engineering
HCMC University of Technology
2013

Outline

1. Basic concepts
2. Basic steps in Information Systems Security
3. Information System Components

Basic concepts

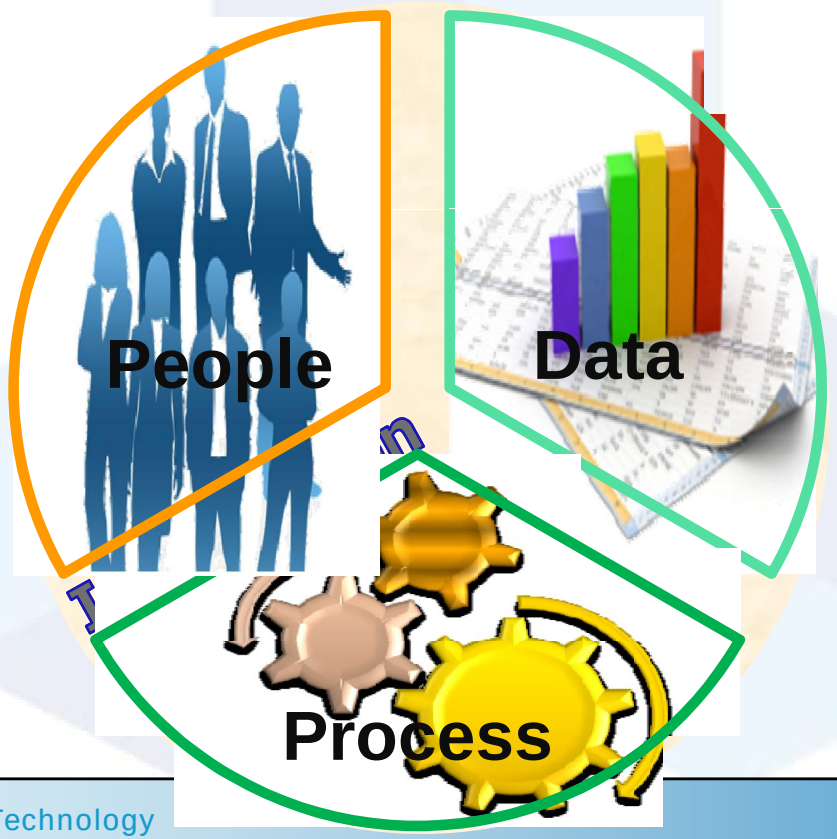
- Data and Information
- Information Systems
- Information System Security
- Requirements of Information System Security
- Goals of Information System Security

Data and Information

- ***Data*** are plain facts.
- When data are processed, organized, structured or presented in a given context so as to make them useful, they are called ***Information***.
- ***Data -> Information -> Knowledge***

Information System

- ***Information System*** refers to a system of **people**, **data** records and activities that **process** the data and information in an organization.



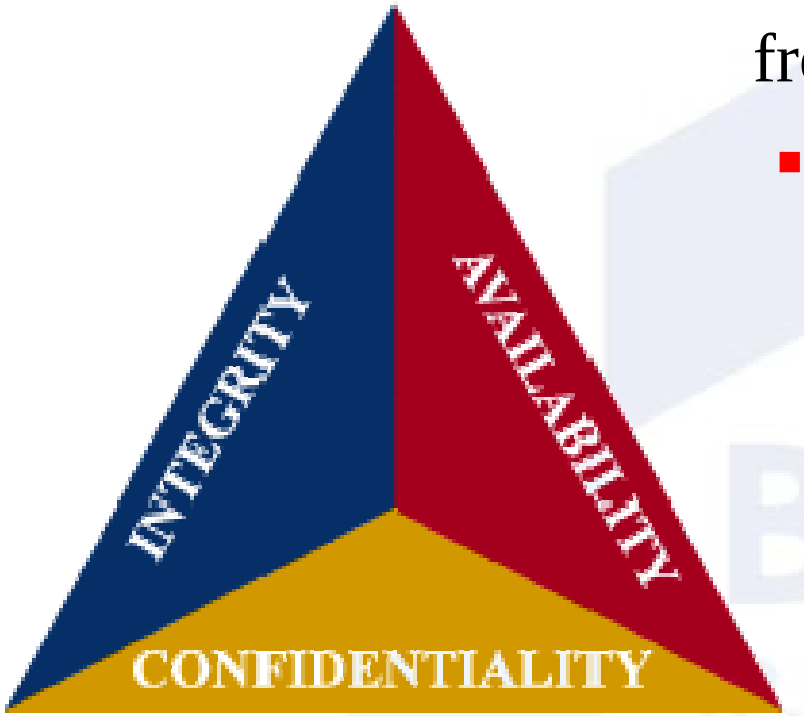
Information Security

- ***Information Security*** means protecting information and information systems from *unauthorized access, use, disclosure, disruption, modification or destruction..*

Requirements of Information System Security

CIA Triad

Requirements of Information System Security (2)

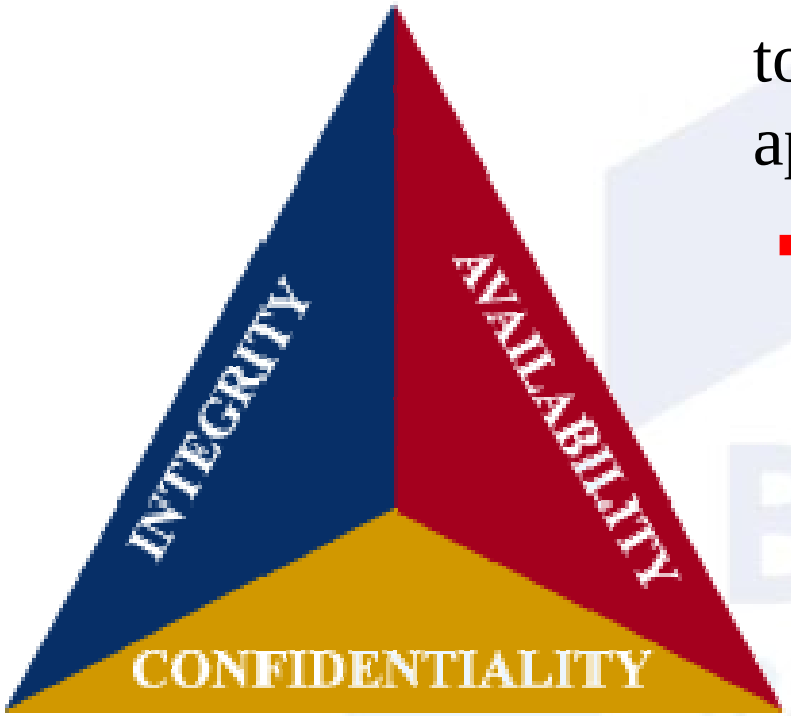


- ***Confidentiality***: Protection of data from unauthorized disclosure.
  - Example: In a bank system, preventing a client from finding out the information of another client, such as balance.

Requirements of Information System Security (3)

- ***Integrity***: Only authorized users should be allowed to modify data.
  - Example: In a bank system, preventing a client from changing his or her balance.

Requirements of Information System Security (4)

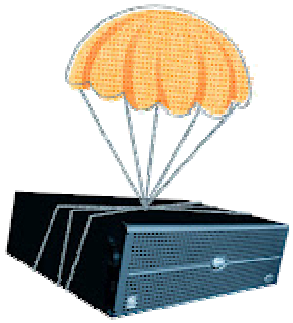


- ***Availability***: Making data available to the authorized users and application programs
  - Example: In a bank system, ensuring that the invoices are printed on time as required by law.

Additional Requirement

- ***Non-repudiation***: The ability to prevent the effective denial of an act.
  - Example: In a bank system, providing proof of the origin and delivery of transactions from a client.

Purposes of Information System Security



- ***Prevention***
  - Prevent attackers from violating security policies
- ***Detection***
  - Detect attackers' violation of security policy
- ***Recovery***
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

Outline

1. Basic concepts
2. Basic steps in Information Systems Security
3. Information System Components

Basic steps in Information Systems Security

- Identify threats
  - What could break your database system?
- Define a security policy
  - What the security system is expected to do?
- Choose security mechanism
  - How the security system should achieve the security goal?

Identify threats

Identify threats | Define a security policy | Choose security mechanism

- Events that bring violations to database are called threats.
- Grouped into categories:
  - Improper release of information
  - Improper modification of data
  - Denial of service
  - Denial of action

Some common threats

- Errors and Omissions
- Fraud and Theft
- Malicious Hackers
- Malicious Code
- Denial-of-Service Attacks
- Social Engineering

Errors and Omissions

- It is difficult to protect the system from the users who need to use it every day to destroy data **accidentally**.
- Errors and omissions attack the integrity component of the CIA triad
- The number-one threat to the system.
- Solutions:
  - Training
  - Security concept “least privilege”
  - Adequate and frequent backups of the information on the systems

Fraud and Theft

- The users are not accidentally destroying data but are **maliciously** destroying the information.
- The internal attacks is very dangerous.
- Solutions
  - Well-defined policies → gather evidence to find attackers (server, log files..)
  - Computer forensics

Malicious Hackers

- There are several groups of Internet users out there that will attack information systems.
- Three primary groups:
  - Hackers: who penetrates a system just to look around and see what is possible.
  - Crackers: who damage or destroy data if they are able to penetrate a system.
  - Phreaks: who breaks into an organization's phone system.

Malicious Hackers (2)

- The ways hackers attack: 5 steps
  - Reconnaissance : Collecting as much information as possible about the target network
  - Scanning: Looking for known vulnerabilities to compromise to gain access to the network.
  - Gaining access: If not → perform a denial-of-service attack
  - Maintaining access: Uploading a backdoor application
  - Cover his track: Modifying log files

Malicious Code

- Malicious code (malware) is defined as any code that is designed to make a system perform any operation with the knowledge of the system owner
- Some common malicious code:
  - Virus
  - Worm
  - Trojan horse
  - Logic bomb

Denial-of-Service Attacks

- A type of attack prevents anyone from accessing to the network.
- To overload the system about resources or network's telecommunication lines
- DoS: a system attacks a targets system
- DDoS (distributed denial of service)
  - Uses zombie hosts to create a "many-to-one" attack
  - It is difficult to defend this attack

Social Engineering

- The goal of social engineering is to trick someone into providing valuable information or access to that information or resource.
- The social engineer exploits weakness of human nature::
  - The desire to be helpful
  - A tendency to trust people
  - The fear of getting into trouble
  - The willingness to cut corners
- Common types of Social Engineering
  - Human-based social engineering
  - Computer-based social engineering

Human-based social engineering

- Dumpster Diving & Shoulder Surfing
- Impersonation
- Posing as Important User
- Third-person Authorization
- Technical Support

Computer-based social engineering

- Phising
- Vishing
- Pop-up Windows
- Mail attachments
- Fake websites
- Interesting software

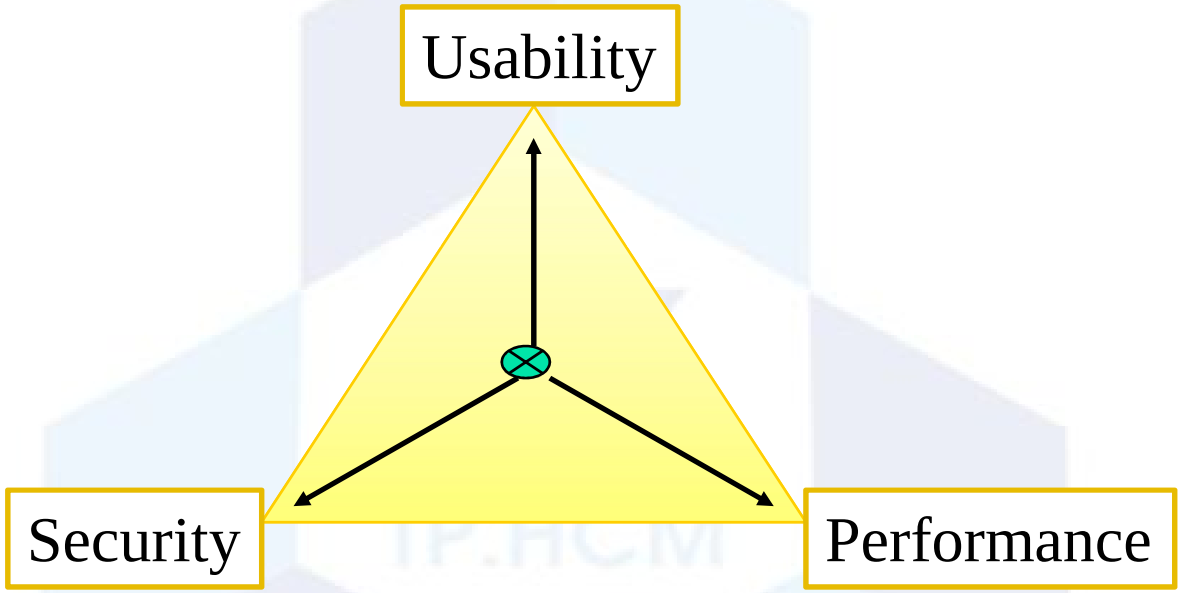
Define a security policy

Identify threats → **Define a security policy** → Choose security mechanism

- Policy says what is, and is not, allowed.
- Security begins with a clear and comprehensive security policy.
- Different policies for different needs. Composition of conflict policies may cause vulnerabilities.
- Policies for compliance: Companies respond by creating a policy that ensures compliance.
  - NIST, SP800, ISO17799, HIPAA

Define a security policy (2)

- A security policy should balance among three factors:



Choose security mechanism

- Mechanisms enforce policies.
- Security mechanisms may be
  - Technical, in which controls in the computer enforce the policy; for example, the requirement that a user supply a password to authenticate herself before using the computer
  - Procedural, in which controls outside the system enforce the policy; for example, firing someone for ringing in a disk containing a program obtained from an untrusted source

Database security mechanism

- Access control
- Inference control
- Flow control
- Encryption

Access control

- ***Access control***: The security mechanism for restricting access to the database as a whole.
- Basic steps:

Identification:

A user provides his identity

Authentication:

A user shows proof to confirm the claimed identity

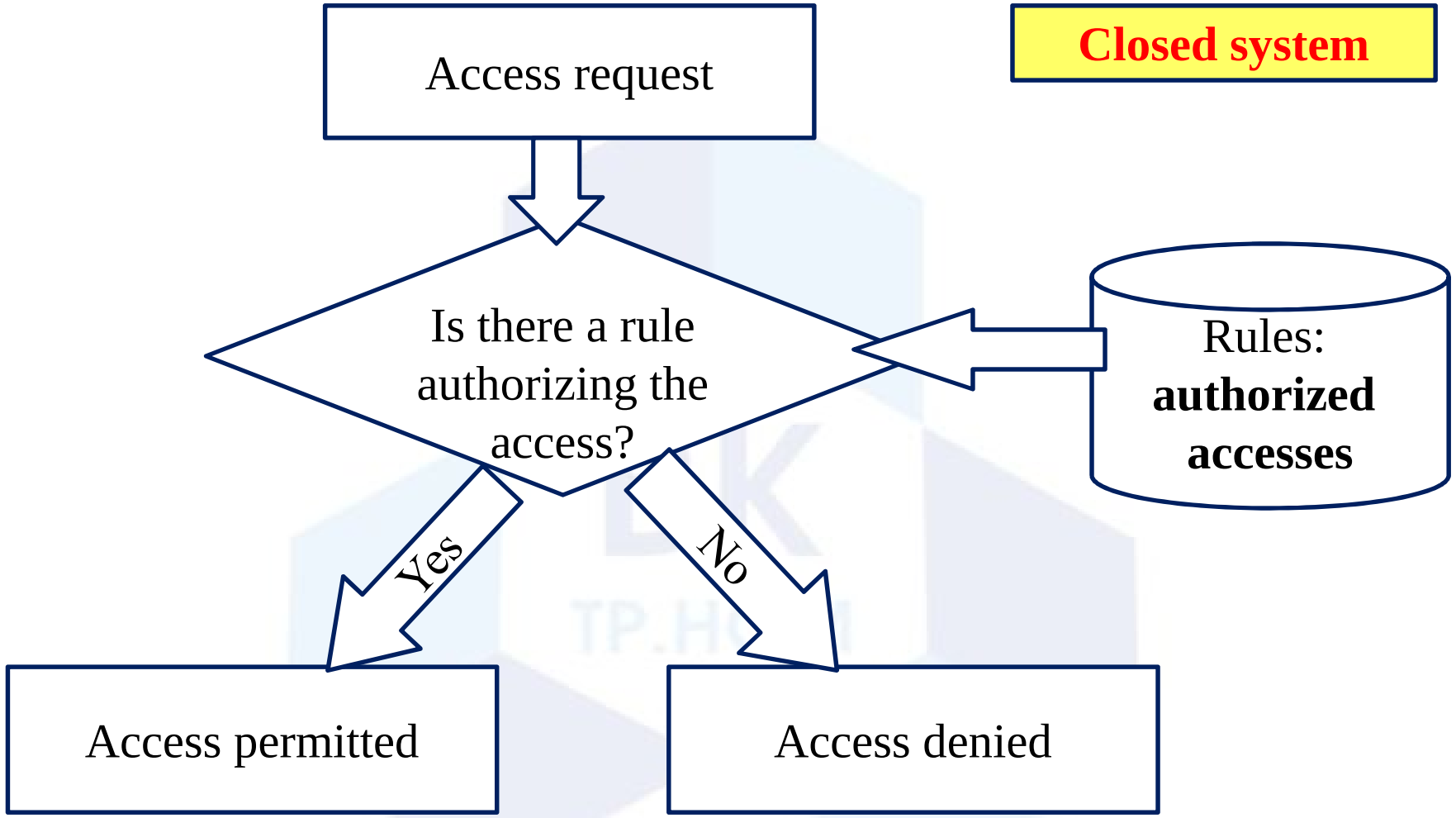
Authorization:

The system specifies the user's access rights to resources

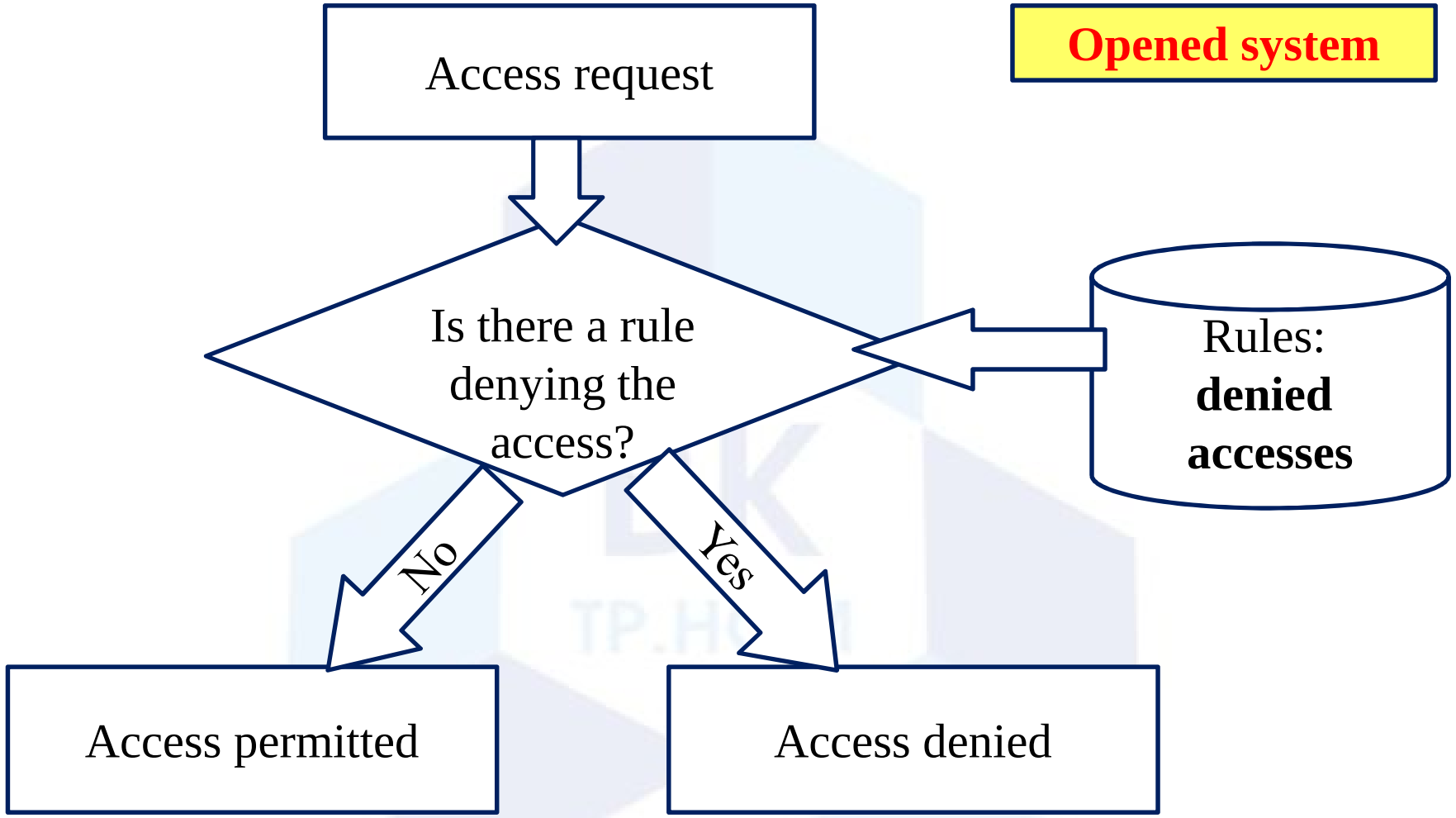
Access control (2)

- Handled by creating user accounts and passwords to control login process by the Database Management System (DBMS)
- Two types of access control system
  - Closed system
  - Open system

Closed System



Opened System



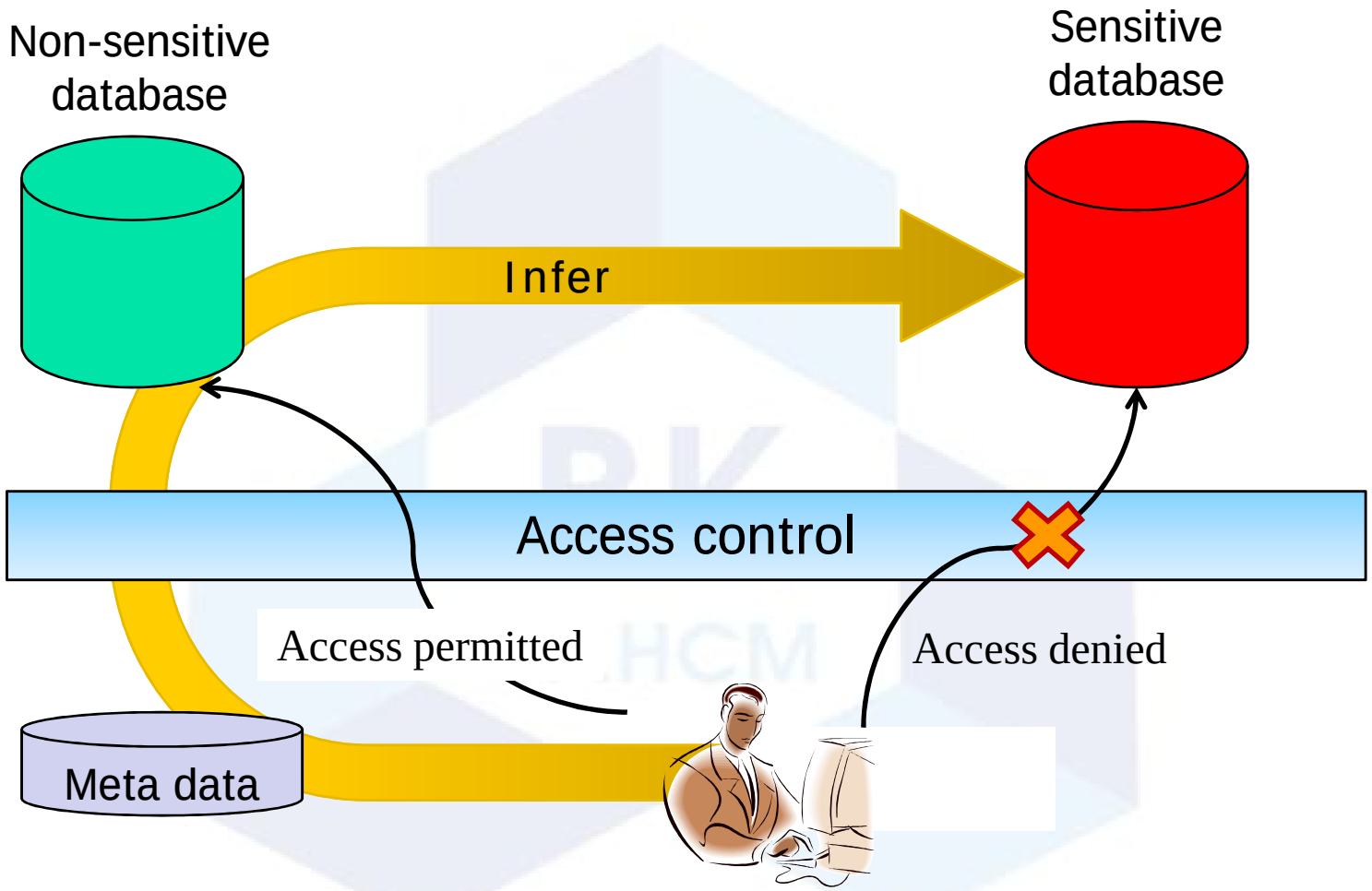
Access control (3)

- Access control rules:
  - Discretionary security mechanisms (DAC)
  - Mandatory security mechanisms (MAC)

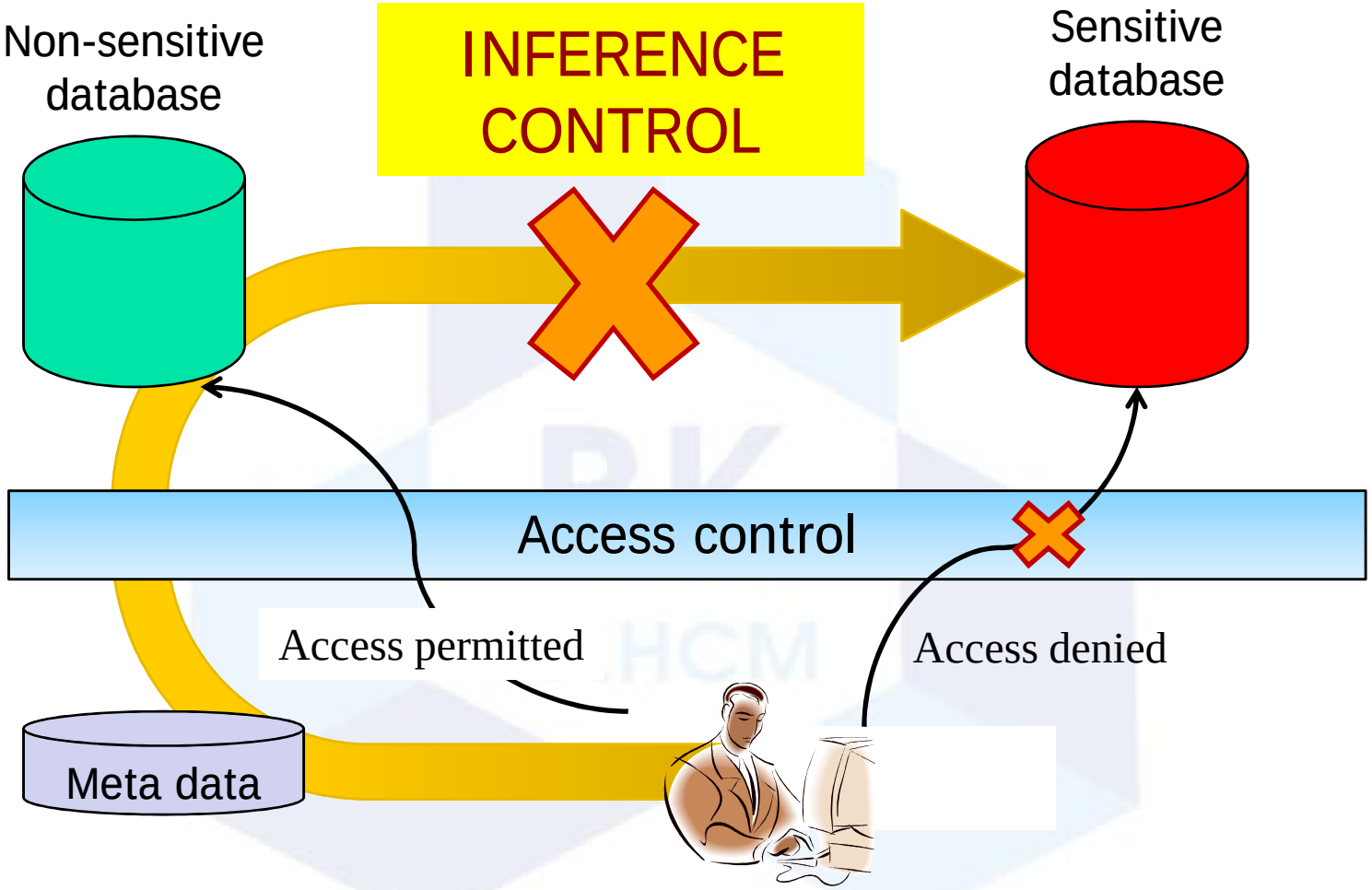
Inference control

- The security problem associated with databases is that of controlling the access to a statistical database, which is used to provide statistical information or summaries of values based on various criteria.
- ***Inference controls*** aim is at protecting data from indirect detection.
  - Set X of data : visible to user A
  - Set Y of data : invisible to user A
  - But … Y = f(X)
  - → If user A know function f, he can apply it to find out Y!!!!

Inference attack



Inference control



Flow control

- A **flow** between object X and object Y occurs when a program reads values from X and writes values into Y.
- **Flow control** prevents information from flowing from some objects into less protected objects so that it can reach unauthorized users.
- A **flow policy** specifies the channels which information is allowed to move.
  - Specifies just two classes of information: confidential (C) and non-confidential (N)
  - and allows all flows except those from class C to class N.

Flow control

- Channels that are pathways for information to flow implicitly in ways that violate the security flow implicitly in ways that violate the security policy of an organization are called **Covert Channels**.
  - Storage channel
  - Timing channel

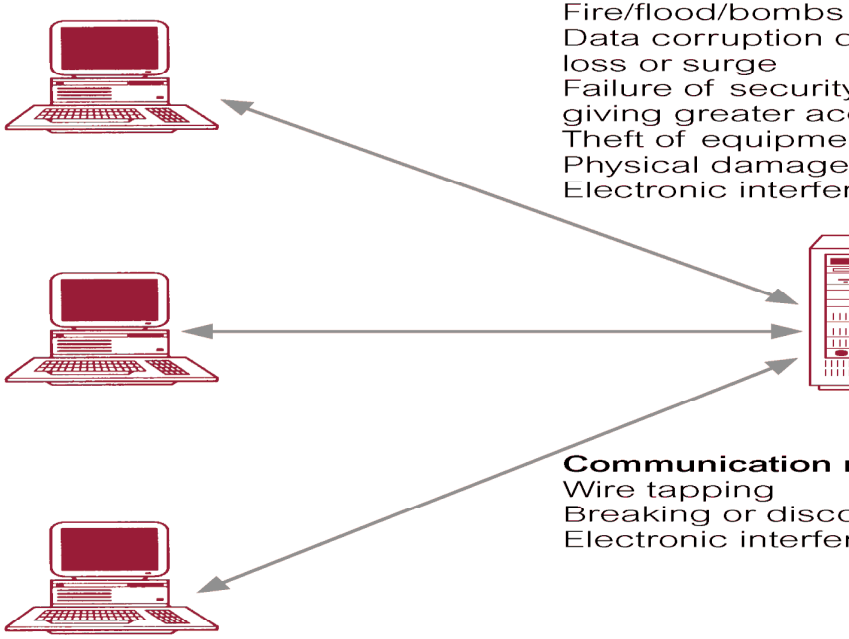
Encryption

- **Encryption** refers to mathematical calculations and algorithmic schemes that transform plaintext into cyphertext, a form that is non-readable to unauthorized parties.
- Only the user having a correct key can decrypt the cyphertext, transforming it to the original plaintext version.
- Data encryption is used to protect sensitive data (such as credit card numbers).

Outline

1. Basic concepts
2. Basic steps in Information Systems Security
3. Information System Components

Information System Components



Hardware
Fire/flood/bombs
Data corruption due to power loss or surge
Failure of security mechanisms giving greater access
Theft of equipment
Physical damage to equipment
Electronic interference and radiation

DBMS and Application Software
Failure of security mechanism giving greater access
Program alteration
Theft of programs

Communication networks
Wire tapping
Breaking or disconnection of cables
Electronic interference and radiation

Database
Unauthorized amendment or copying of data
Theft of data
Data corruption due to power loss or surge

Users
Using another person's means of access
Viewing and disclosing unauthorized data
Inadequate Staff training
Illegal entry by hacker
Blackmail
Introduction of viruses

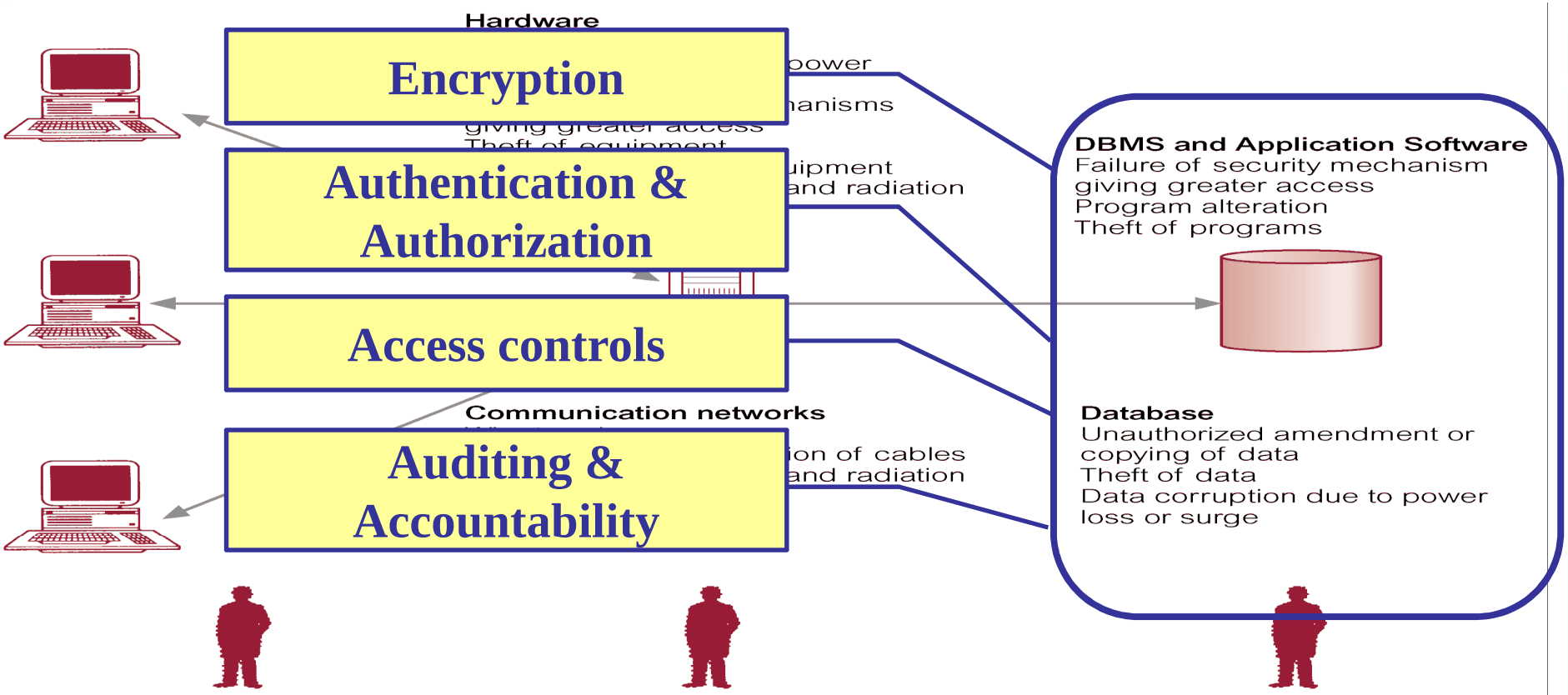
Programers/Operators
Creating trapdoors
Program alteration (such as creating software that is insecure)
Inadequate staff training
Inadequate security policies and procedures
Staff shortages or strikes

Data/Database Administrator
Inadequate security policies and procedures

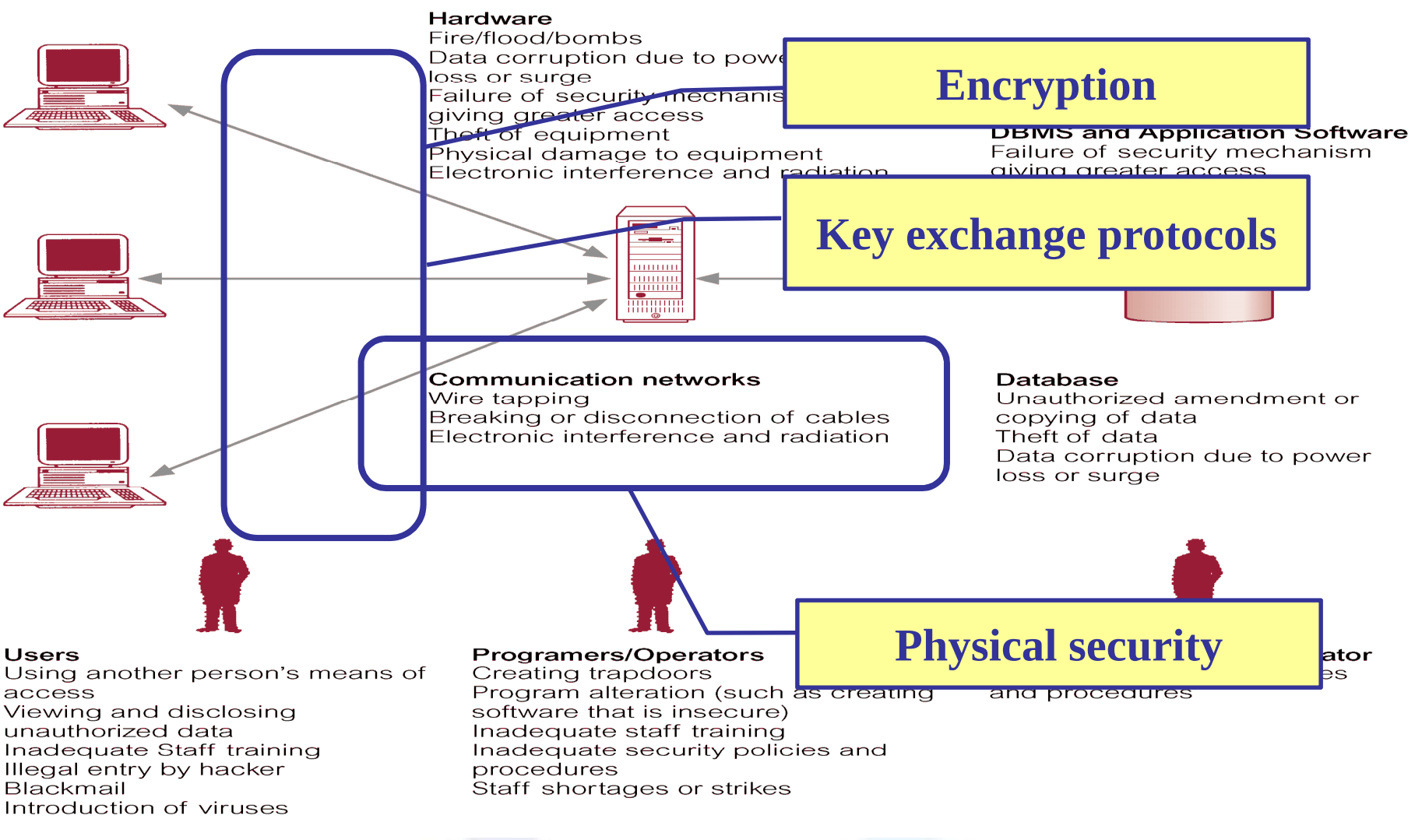
Information System Components (2)

- Hardware
- Communication network
- Database
- Database management system (DMBS) and application software
- Users
- Programmers/Operators
- Data/database administrator

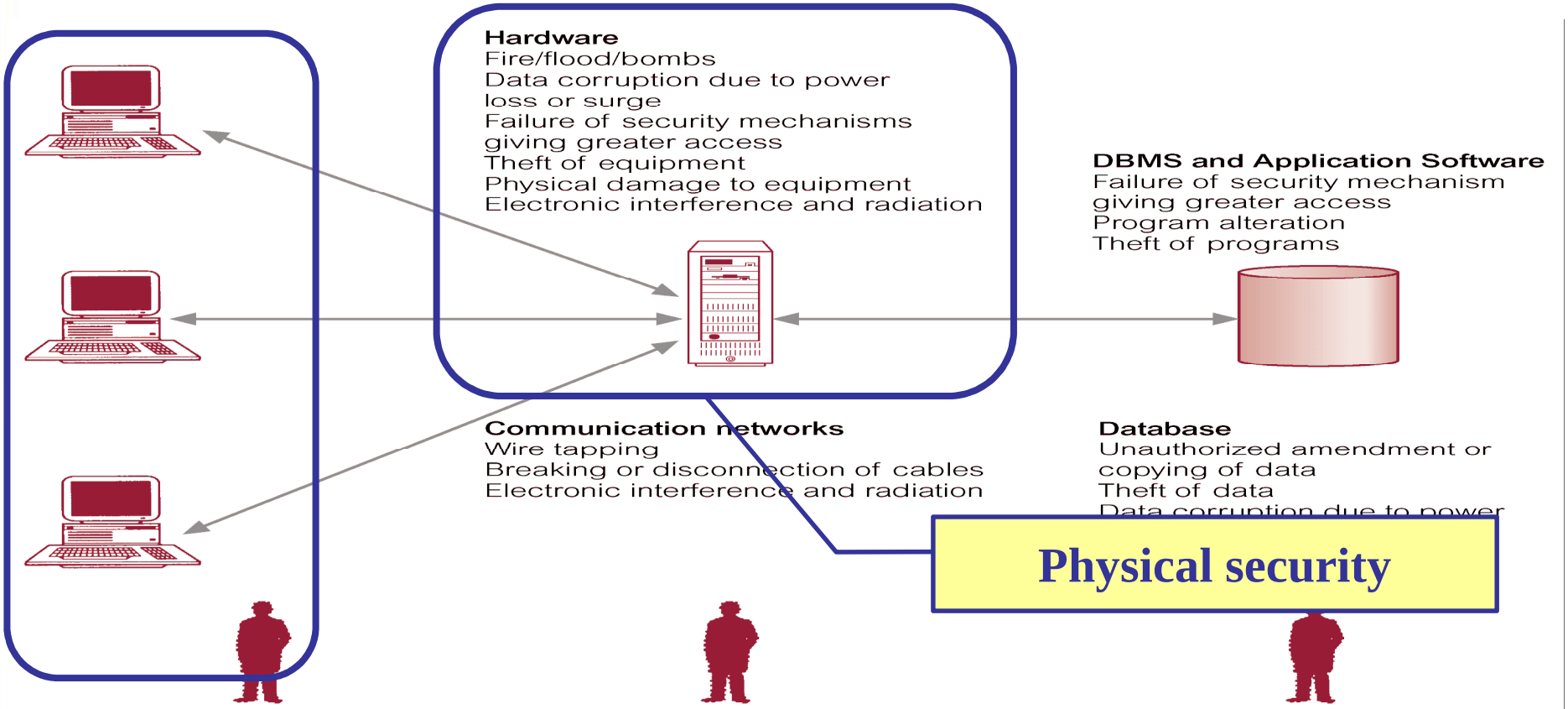
Information System Components (3)



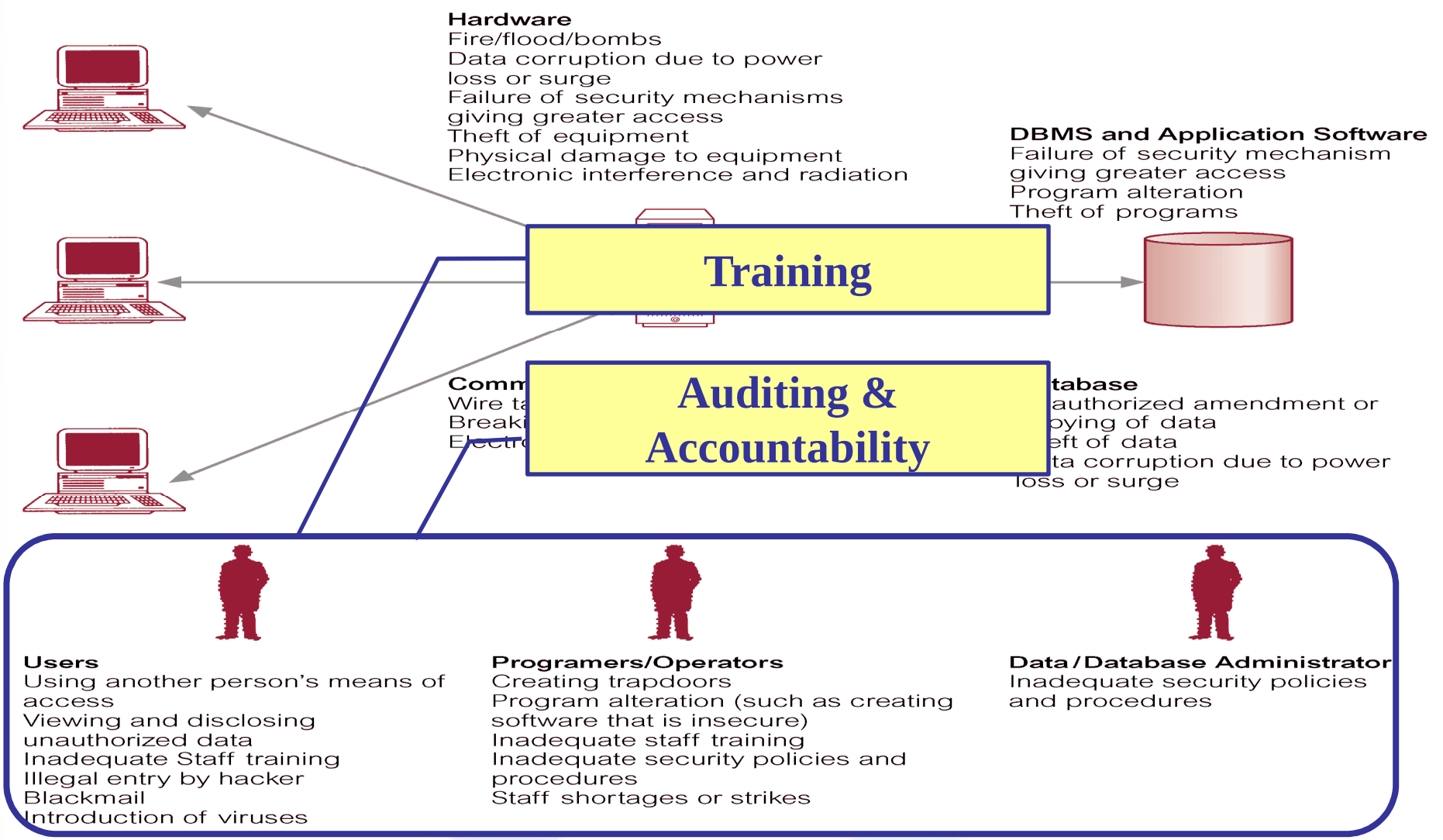
Information System Components (4)



Information System Components (5)



Information System Components (6)



Outline

1. Basic concepts
2. Basic steps in Information Systems Security
3. Information System Components


Question ?

Convert chanel – Timing Chanel

- In Python:

```
def validate_password(actual_pw,
  typed_pw):
  if len(actual_pw) <> len(typed_pw):
    return 0
  for i in len(actual_pw):
    if actual_pw[i] <> typed_pw[i]:
    return 0
  return 1
```