COS3023/N Operating Systems and Concurrency

Topic 6- Security & Protection

Lecturer : Ms. Sha

Security and Protection

Security and protection

Introduction

- Protection refers to a mechanism for controlling the access of programs, processes or users to the resources
- Must provide means for specifying the controls to be imposed
- We distinguish between protection and security
- Security is a measure of confidence that the integrity of a system and its data will be preserved

Security and protection

Goals of protection

Reasons for protection

- Prevent the mischievous, intentional violation of an access restriction
- Ensure that each program component uses system resources only in ways consistent with system policies

A protection oriented system provides means to distinguish between authorised and unauthorised usage

Security and protection

Principles of protection

- A key principle for protection is the principle of least privilege
- Programs, users and systems are given just enough privileges to perform their tasks
- Should enable to provide privileges when needed and disable them otherwise
- Separate account for each user

Security and protection

Domain of protection

- A computer system is a collection of processes and objects
- Hardware objects: CPU, memory, printers, disks...
- Software objects: Files, programs, semaphores, ...
- A process should be allowed to access only those objects for which it has authorisation

Security and protection

Access control

owner, group, list of users

- The access to objects can be restricted in a similar way as the access to files
- For each object, access control information is added
- Example: Role-based access control (Solaris 10)
  - Processes are assigned privileges
  - A privilege is the right to execute a system call or to use an option within that call

→ opening a file with write access

Security and protection

The security problem

- Security violations can be categorised as intentional or accidental
- It is easier to protect against accidental security violations
- Protection methods mostly consider accidental security violations
- A threat is a potential for a security violation
- An attack is the attempt to break security

Security and protection

The security problem

Breach of confidentiality Unauthorised reading of data. Goal of the intruder: Capture secret data

Breach of integrity Unauthorised modification of data. E.g. modification of source code

Breach of availability Unauthorised destruction of data

Theft of service Unauthorised use of resources. E.g. intruder may install a daemon that acts as a file server

Denial of service Preventing legitimate use of the system.

Security and protection

The security problem

masquerading - pretend to b someone else.

To protect a system, we must take security measures at four levels:

- Physical
- Human
- Operating system
- Network

↳ application.

Security and protection

The security problem

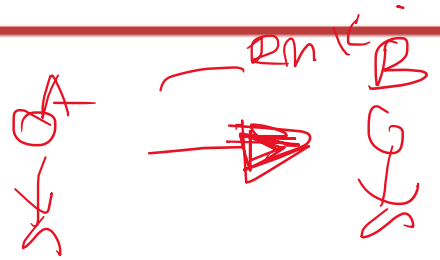
To protect a system, we must take security measures at four levels:

Physical The site containing the computer system must be physically secured against armed or surreptitious entry by intruders

limit area
lock.

Security and protection

The security problem



social engineering
↳ uses deception to persuade people to give up confidential info.

To protect a system, we must take security measures at four levels:

Human Authorisation must be done carefully to assure that only appropriate users have access to the system. Users may also be tricked into providing access rights (e.g. phishing)

dumpster diving

phishing

trash, shady phone, shady notes

dumpster

Security and protection

The security problem

To protect a system, we must take security measures at four levels:

Operating system System must protect itself from accidental or purposeful security breaches

- Runaway process could constitute an accidental denial-of-service attack
- Query to a service could reveal passwords
- Stack overflow could allow the launching of unauthorised processes
- ...

Security and protection

The security problem

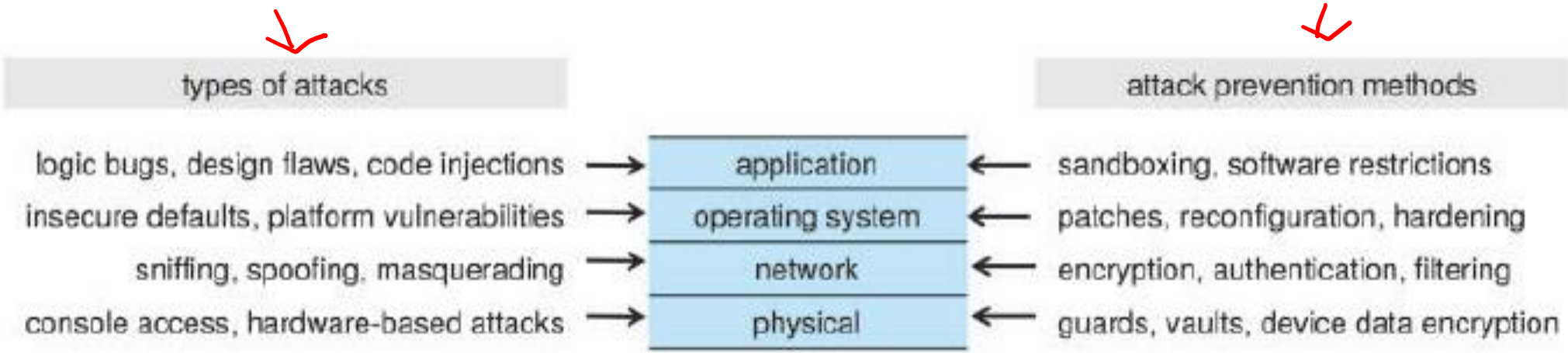
server, mobile device, IOT → networked. → potential vector to unauthorized access.

To protect a system, we must take security measures at four levels:

Network Interception of data on network lines could reveal private data; Interception of data could constitute a remote denial-of-service attack

Application → 3rd party → risk.

The Four-layered Model of Security



Threats

What is a threat?

- refers to anything that has the potential to cause serious harm to a **computer** system.
- A **threat** is something that may or may not happen, but has the potential to cause serious damage.

Threats

- Program threats

Operating system's processes and kernel do the designated task as instructed.

If a user program made these process do malicious(intended to harm) tasks then it is known as Program Threats.

One of the common example of program threat is a program installed in a computer which can store and send user credentials(name/password) via network to some hackers.

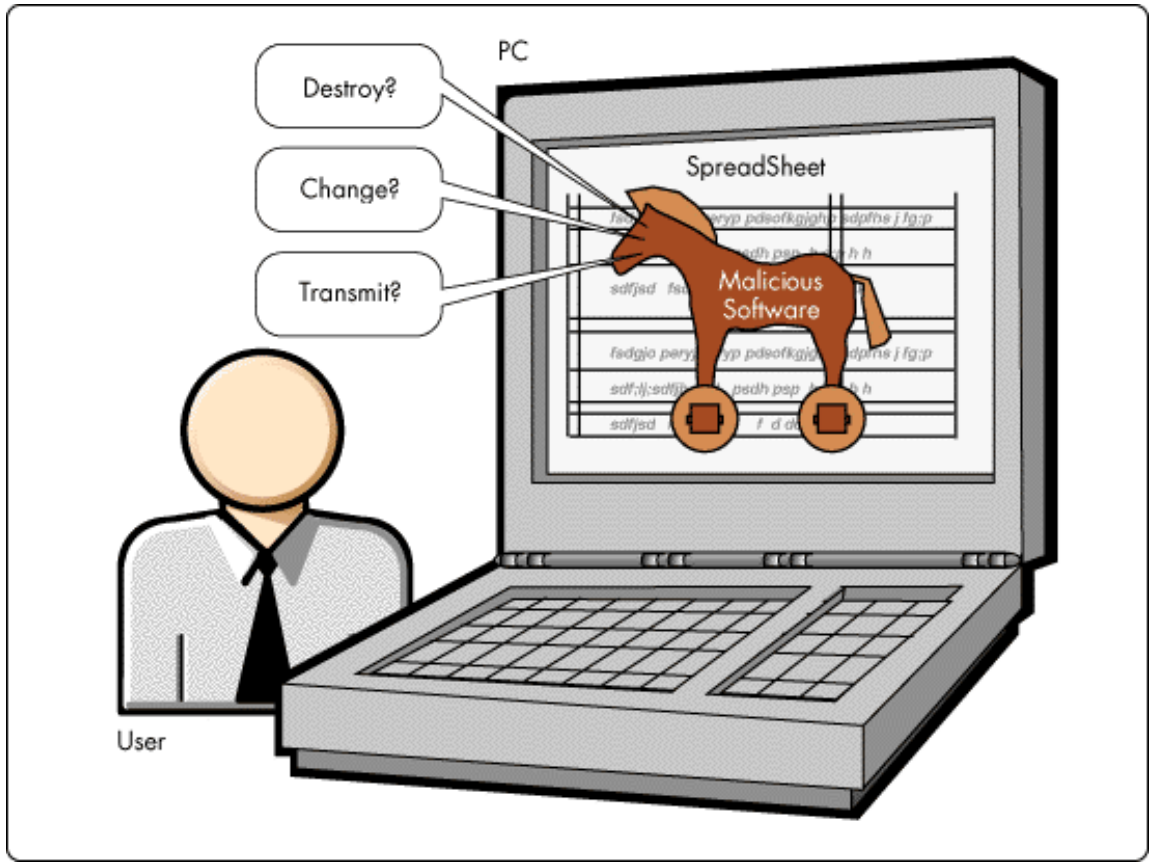
Malware

- Malware is software designed to exploit, disable or damage computer systems.
- There are many ways to perform such activities, and we explore the major variations in this section.

Example of Program Threats

- **Trojan Horse** – Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources.

Spyware –

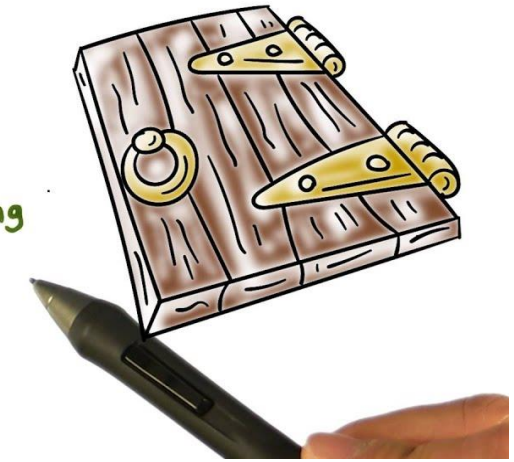


Example of Program Threats

- **Trap Door** – If a program which is designed to work as required, have a security hole in its code and perform illegal action without knowledge of user then it is called to have a trap door.
- A Trap Door is a secret entry point into a program that allows someone to gain access without normal methods of access authentication

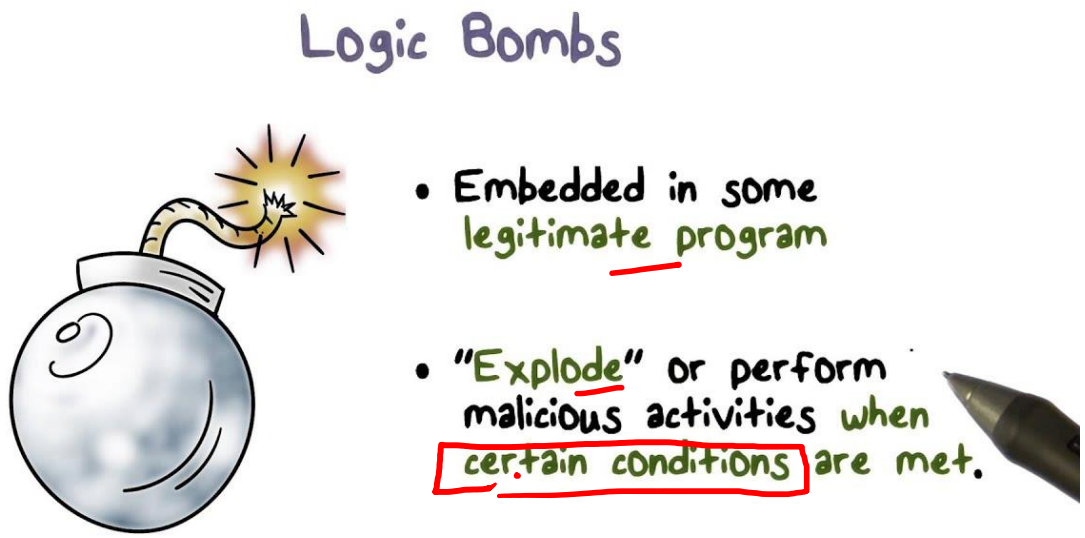
Trap Doors

- A secret entry point to a program or system.
- Typically works by recognizing some special sequence of input or special user ID.



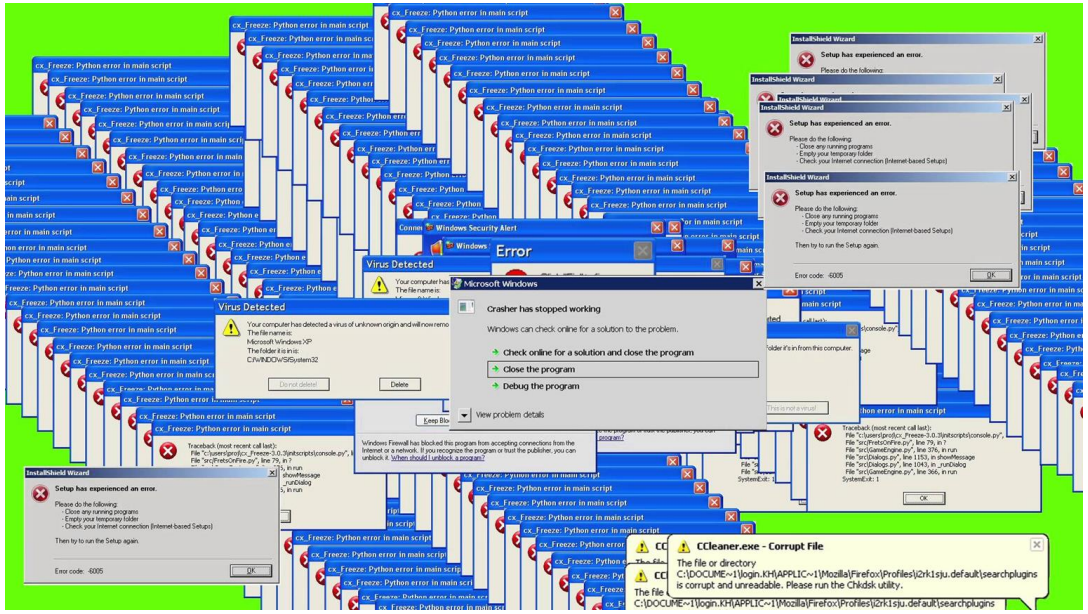
Example of Program Threats

- **Logic Bomb** – Logic bomb is a situation when a program misbehaves only when certain conditions met otherwise it works as a genuine program. It is harder to detect.



Example of Program Threats

- **Virus** – Virus as name suggest can replicate themselves on computer system. They are highly dangerous and can modify/delete user files, crash systems.
- A virus is generally a small code embedded in a program. As user accesses the program, the virus starts getting embedded in other files/ programs and can make system unusable for user.



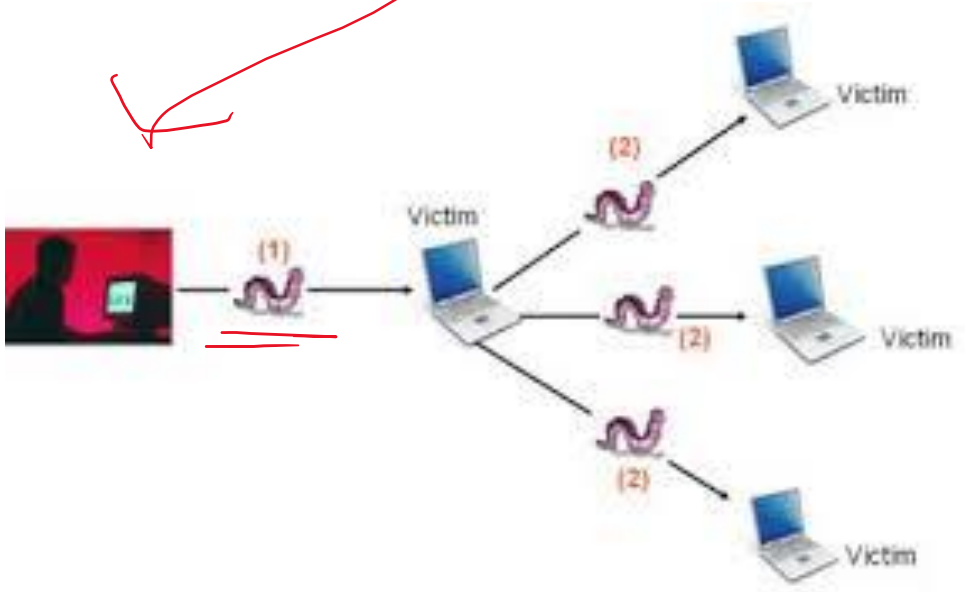
Threats

- System threats

refer to misuse of system services and network connections to put user in trouble. System threats creates such an environment that operating system resources/ user files are misused

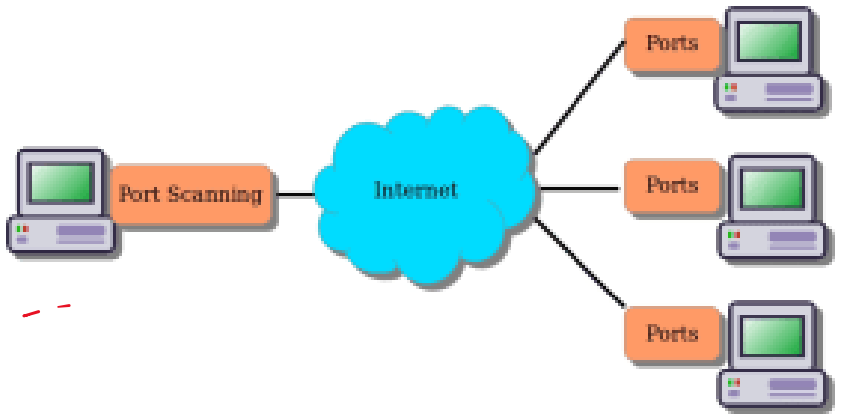
Example of System Threats

- **Worm** – Worm is a process which can choked down a system performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy uses system resources, prevents all other processes to get required resources.
- Worms processes can even shut down an entire network.



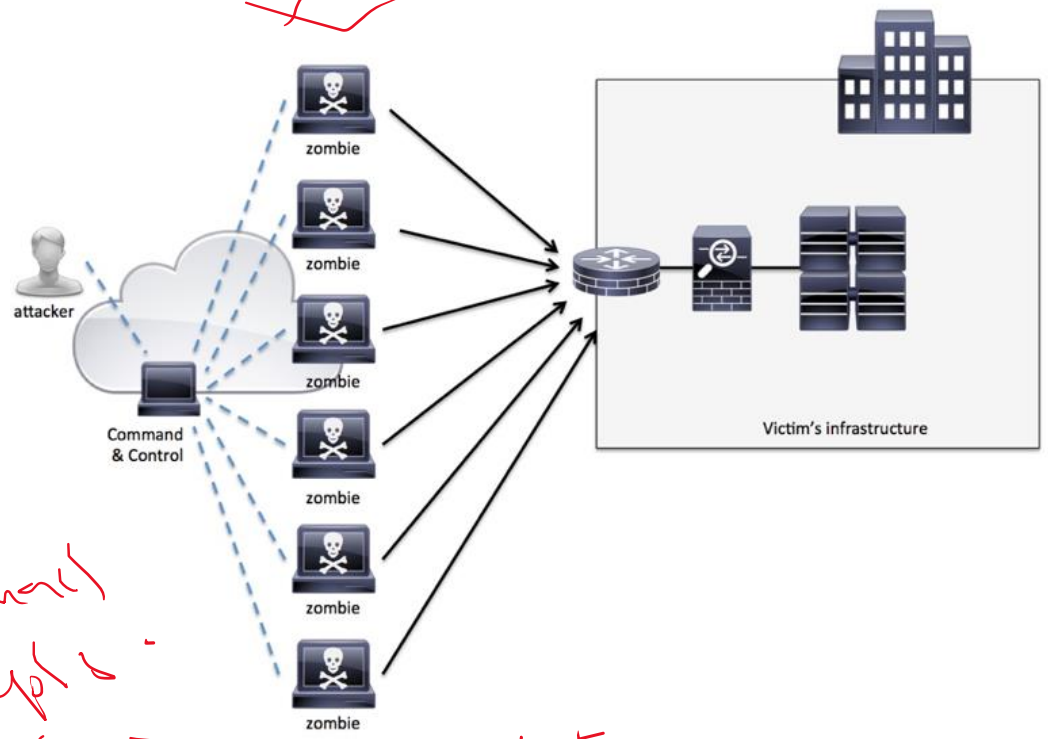
Example of System Threats

- **Port Scanning** – Port scanning is a mechanism or means by which a hacker can detects system vulnerabilities to make an attack on the system.



Example of System Threats

- **Denial of Service** – Denial of service attacks normally prevents user to make legitimate use of the system. For example, a user may not be able to use internet if denial of service attacks browser's content settings.



protection methods

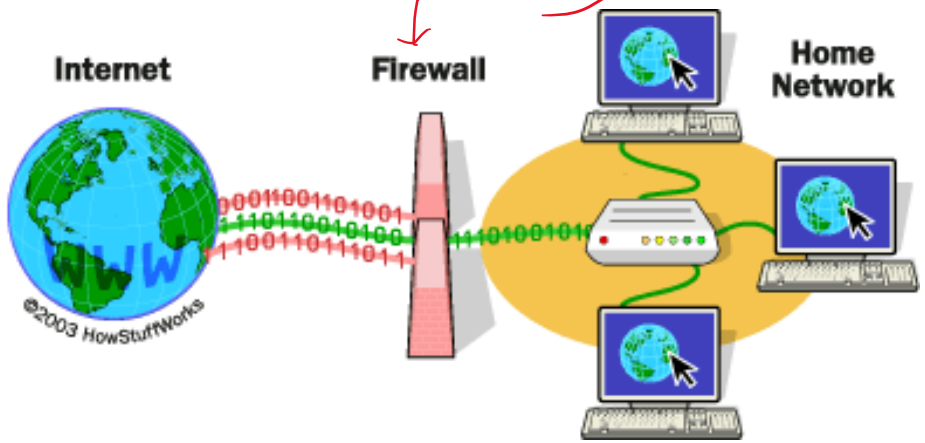
System protection methods:

- Antivirus software

is a computer program used to prevent, detect, and remove malware

- Firewalls

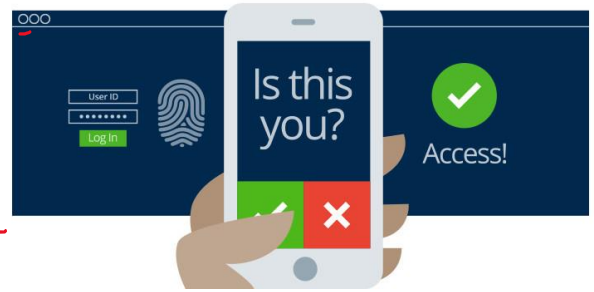
a network security system that monitors and controls over all your incoming and outgoing network t
defined set of security rules.



Other protection methods

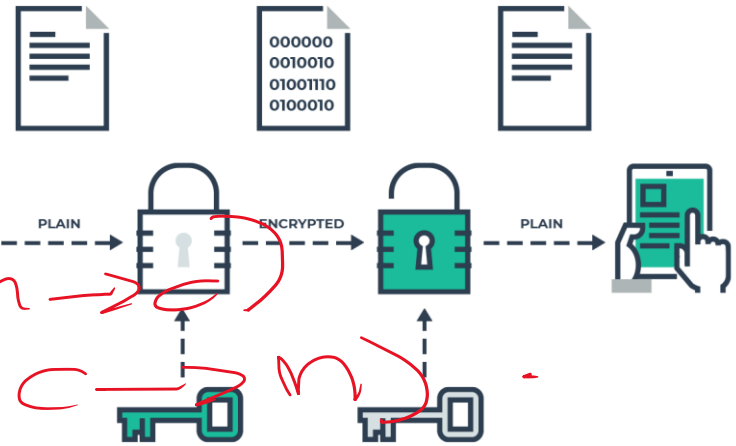
- Authentication

Authentication refers to identifying each user of the system and associating the executing programs with those users.



- Encryption

is the process of encoding a message or information in such a way that only authorized parties can access it.



Exercise

- Protection methods:

1) Firewall
2) Anti-virus
3) Password – OTP
4) Encryption
5) Authentication (biometric schemes- finger print retina print, face, voice

THANK YOU