System Protection In Operating Systems and Development

MOHAMMED HASSAN

153102005

What is Security in OS?

- Operating system security is the process of ensuring operating system integrity, confidentiality and availability.
- Authentication of use, validation of messages malicious or accidental introduction of flaws, etc. are all under security as well.

Protection

- Protection refers to a mechanism in order to control the access of programs, processes, or users to the resources defined by a computer program.
- Protection certifies the resources of the computer in order to be used in a consistent manner.
- It also ensure that objects are accessed correctly and only by the designated processes.

Goal of Protection

- **CONFIDENTIALITY**: Requires that information maintained by a computer system be accessible only by authorised parties.
- **INTEGRITY**: Requires that a computer system's resource can only be altered by an authorised party.
- **AVAILABILITY**: Requires that a computer system can be accessed at required periods by the authorised party.
- **AUTHENTHICITY**: Requires that the computer system can confirm the identity of a user.

Principle of Protection

- *The principle of least privilege*: is an important concept in computer security, it dictates that every module (a process, a user, or a program) be given just enough privileges to perform their designated tasks.
- An operating system following the principle of least privilege implements various features so that a failure of a component does the minimum damage.
- The principle of least privilege can help in the production of a more secure computing environment.

Security Kernel

- Responsible for implementing the security mechanism for the whole operating system.
- Provides the security interfaces among the hardware, the operating system, and the other parts of the computing system.
- Implementation of a security kernel may degrade system performance with no guarantees.

Example of Security (Windows XP)

- It uses subject models to ensure access security, it manages permissions to each program ran.
- Security system is based on user accounts
  - Every user has its own unique security ID
  - Logging in ID creates different security access based on the user

THANK YOU!!!
ANY QUESTIONS…….