Operating Systems Security

Prepared by Assist . Prof .
Imad Matti
AL-mamoon University
Cyber Security Engineering Department
2026

Introduction

1. What is an Operating System?

An operating system is the system software that:

- Runs the computer
- Manages programs
- Controls files, memory, and the CPU

Examples:

Windows – Linux – macOS – Android

2. What is Operating System Security?

Operating System Security means:

Protecting the **computer** and **data** from **unauthorized access** or **misuse**.

In simple words:

- **Prevent** strangers from using the computer
- **Protect** files from being deleted or stolen
- **Stop harmful** programs (viruses)

Operating systems security is the practice of protecting the software that runs on computers, tablets, and smart phones. It involves keeping the operating system (OS) safe from threats such as viruses, hackers, and malware.

3. Why Do We Need OS Security?

Without security:

- Anyone can use the computer
- Any program can delete files
- Viruses can damage the system

Simple example:

A computer without a password → anyone can open and use it.

Main Goals of Operating System Security

When we talk about security, we should think of protecting **three** things:

Operating system security is based on **three** main goals, often called the **CIA Triad**:

1. Confidentiality (secrecy) (السرية)

Ensures that only authorized users **can access certain data.**

You want to ensure that secret and private files and information are only available to intended persons.

- **Example:**
  Your personal files or photos cannot be opened by someone else using your computer.
- Protects sensitive information from being stolen or seen by unauthorized users.

2. Integrity (السلامة / التكامل)

- **Ensures that data and system resources are** not changed without permission**.**

- **Example:**
  A program cannot change your grades, delete system files, or modify important documents.
- Prevents accidental or malicious changes.

3. Availability (الإتاحة)

- Ensures that the system and resources are **always available when needed**.

- You want your laptop or smart phone to be available to use anytime you decide to use it.
-

- **Example:**
  If your computer freezes or stops working because of deadlock or a virus, availability is lost.
- This links directly to what we discussed about **deadlock** earlier.

Basic Security Mechanisms in Operating Systems

After understanding the goals, operating systems use **simple mechanisms** to achieve them:

A) Authentication (المصادقة)

- Checking **who is using the system**.
- **Examples:**
  - Username + Password
  - Phone PIN or fingerprint
- Makes sure that only authorized users can log in.

B) Access Control & Permissions (التحكم بالوصول)

- Defines **what a user or program can do**.
- **Examples:**
  - Read, write, or delete a file
  - Student cannot delete the teacher's files
- Helps enforce confidentiality and integrity.

C) User Roles & Least Privilege (أقل امتياز)

- Regular users: limited permissions
- Administrators / Root: full permissions
- Principle: give **only the necessary permissions**

- **Example:**
  You cannot install software without administrator approval.

D) File and Memory Protection (حماية الملفات والذاكرة)

- Some files are **read-only**
- Programs cannot access memory of other programs
- Prevents accidental or malicious damage
- **Example:**
  Your operating system files cannot be deleted easily.

E) Protection against Malware (الحماية من البرامج الضارة)

- Viruses, worms, and trojans can damage data or system
- Operating system uses:
  - Antivirus software
  - Safe update mechanisms
- **Example:**
  Do not download unknown programs to avoid infecting your system.

F) Updates and Patching (التحديثات الأمنية)

- Keep system software up to date
- Fix security holes and bugs
- **Example:**
  Updating Windows or Android keeps your system safe from known attacks.

What is Operating Systems Security?

Operating systems security is the practice of protecting the software that runs on computers, tablets, and smart phones. It involves keeping the operating system (OS) safe from threats such as viruses, hackers, and malware.

Why is Operating Systems Security Important?

Operating systems act as the backbone of any device. They manage hardware and software resources and allow users to perform tasks. If an operating system is not secure, it can lead to data breaches, theft of personal information, and loss of valuable data. By securing the OS, we also protect the applications and data that run on it.

Key Components of Operating Systems Security

1. **User Authentication:** This process ensures that only authorized users can access the operating system. It often involves using passwords, PINs, or biometric methods like fingerprints.
2. **Permissions and Access Control:** Operating systems use permissions to control who can view or use files and programs. This helps prevent unauthorized access to sensitive information.
3. **Updates and Patches:** Regularly updating the operating system is crucial. These updates fix security holes that can be exploited by attackers.

4. **Firewalls:** A firewall is a security feature that monitors incoming and outgoing network traffic. It helps block malicious attacks before they can reach the operating system.
5. **Antivirus and Antimalware Software:** These programs protect the operating system by detecting and removing harmful software that can cause damage.
6. **Data Encryption:** Encrypting data makes it unreadable to anyone without the correct key. This includes sensitive information stored on your device.

How to Improve Operating Systems Security

Improving operating systems security starts with being mindful of your device's health. Here are some tips:

- **Always use strong passwords and change them regularly.**
- **Install security updates and patches as soon as they are available.**
- **Use firewalls and antivirus software to add extra layers of protection.**
- **Be cautious with downloads and email attachments; only download from trusted sources.**
- **Regularly back up your data so you can recover it in case of a security breach.**

What is Protection and Security in Operating Systems?

OS uses two sets of techniques to counter threats to information namely:

- **Protection**
- **Security**

Protection

Protection tackles the system's **internal threats**.

Example: suppose In a small organization there are four employees p1, p2, p3, p4, and two data resources r1 and r2. The various departments frequently exchange information but not sensitive information between all employees. The employee's p1 and p2 can only access r1 data resources and employee's p3 and p4 can only access r2 resources. If the employee p1 tries to access the data resource r2, then the employee p1 is restricted from accessing that resource. Hence, p1 will not be able to access the r2 resource.

Security

Security tackles the system's **external threats**. The safety of their system resources such as saved data, disks, memory, etc. is secured by the **security** systems against harmful modifications, unauthorized access, and inconsistency. It provides a mechanism (encryption and authentication) to analyze the user before allowing access to the system.

Example: In the organization data resources are shared with many employees but a user who does not work for that specific company cannot access this information. Security can be achieved by three attributes: **confidentiality** (prevention of unauthorized resources and modification), **integrity** (prevention of all unauthorized users), and **availability** (unauthorized withholding of resources).

Threats to Protection and Security

A program that is malicious in nature and has harmful impacts on a system is called a **threat**. Protection and security in an operating system refer to the measures and procedures that can ensure the confidentiality, integrity, and availability (**CIA**) of operating systems. The main goal is to protect the OS from various threats, and malicious software such as trojans, worms, and other viruses, misconfigurations, and remote intrusions.

Common Threats That Occur in a System

In a system, some common threats include the following:

Virus

A computer virus is a form of malware, or malicious software, that transmits between computers and corrupts software and data. Generally, viruses are small pieces of code that are embedded in a system. They can corrupt files, erase data, crash systems, and other things, making them extremely dangerous. Also, they can expand by **replicating** themselves.

Trojan horse

A Trojan Horse Virus is a form of malware that downloads on a computer by impersonating a trustworthy program. A Trojan horse can get unauthorized access to a system's login information. A malicious user may then use them to enter the system.

Worm

A computer worm is a sort of malware whose main purpose is to keep operating on infected systems while self-replicating and infecting other computers. By using a system's resources to extreme levels, a worm can completely destroy it. It has the ability to produce duplicate copies that occupy all available resources and prevent any other processes from using them.

Trap Door

A trap door is basically a back door into software that anyone can use to access any system without having to follow the normal security access procedures. It may exist in a system without the user's knowledge. As they're so hard to detect, trap doors need programmers or developers to thoroughly examine all of the system's components in order to find them.

Denial of Service (رفض تقديم الخدمة)

A Denial-of-Service (DoS) **attack** aims to shut down a computer system or network so that its intended users are unable to access it. **These kinds of attacks prevent authorized users from accessing a system.**

Methods to Ensure Protection and Security in Operating System

- **Keep a Data Backup:** It is a safe option in case of data corruption due to problems in protection and security, you can always require it from the Backup.
- **Beware of suspicious emails and links:** When we visit some malicious link over the internet, it can cause a serious issue by acquiring user access.
- **Secure Authentication and Authorization:** OS should provide secure authentication and authorization for access to resources and also users should keep the credentials safe to avoid illegal access to resources.
- **Use Secure Wi-Fi Only:** Sometimes using free wifi or insecure wifi may cause security issues, because attackers can transmit harmful programs over the network or record the activity etc, which could cause a big problem in the worst case.
- **Install anti-virus and malware protection:** It helps to remove and avoid viruses and malware from the system.
- **Manage access wisely:** The access should be provided to apps and software by thorough analysis because no software can harm our system until it acquires access. So, we can ensure to provide suitable access to software and we can always keep an eye on software to see what resources and access it is using.
- **Firewalls Utilities:** It enables us to monitor and filter network traffic. We can use firewalls to ensure that only authorized users are allowed to access or transfer data.

- **Encryption and Decryption Based transfer:** The data content must be transferred according to an encryption algorithm that can only be reversed with the appropriate decryption key. This process protects your data from unauthorized access over the internet, also even if data is stolen it would always remain unreadable.
-

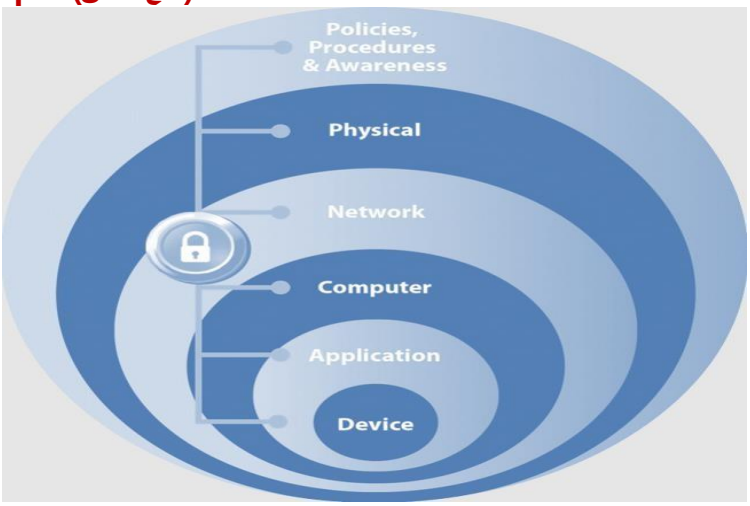
Be cautious when sharing personal information: The personal information and credentials must be shared only with trusted and safe sources by not doing so attackers can use this information for their intent which could be harmful to the system's security.

Cyber Security Architecture:

Five Principles to Follow (and One to Avoid)

In today's digital landscape, where cyber attacks and data breaches **(انتهاكات)** are more prevalent(سائد) than ever, securing your organization is paramount (مهم) . **Cyber security architecture serves as the foundation that protects your systems from these ever-evolving threats(تهديدات). But how do you design an architecture that can withstand (يقاوم) such challenges**? There are five key principles every cyber security architecture should follow — and one common mistake to avoid.

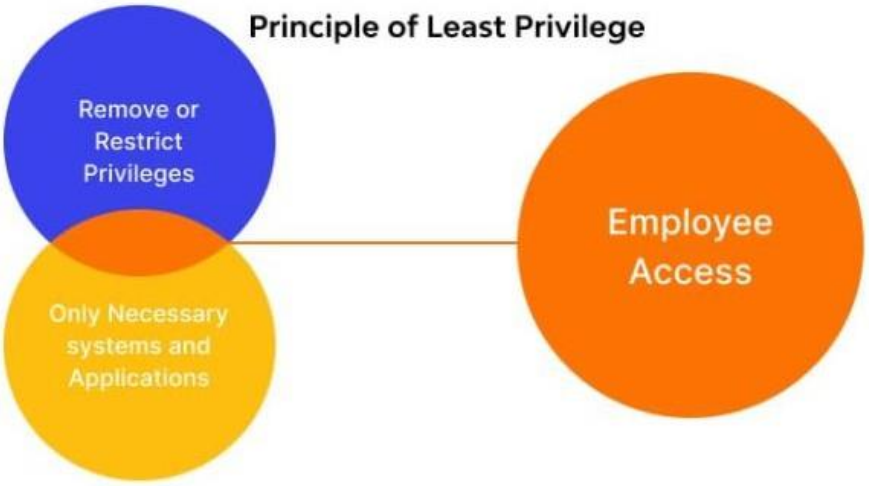
1. **Defense in Depth (دفاع متعمق)**



The first and perhaps most essential principle is **defense in depth**. **Rather than relying (الاعتماد) on one security layer, you implement multiple layers that make it harder for attackers to penetrate.**

The key idea here is **avoiding single points of failure**. If one layer of defense fails, the others are still in place to protect the system.

2. Principle of Least Privilege



The **principle of least privilege** emphasizes limiting access rights to only those who need it to do their jobs. Users should have the minimum level of access necessary, and that access should be temporary.

Simple Example: Office Access Control

- **Employee:** Has a key card that only opens the front door and their specific department area.
- **Office Manager:** Has a key card that opens all department areas and the supply room.
- **Security Guard:** Has a master key that opens all doors.

If an employee loses their key card, the intruder can only access the employee's desk, not the supply room or the entire building. If the master key is lost, the damage is higher, but the policy ensures not everyone has that level of access, reducing risk.

3. Separation of Duties

The **separation of duties principle ensures no single person can control an entire system, reducing the risk of insider threats**. Think of it like having two keys to open a secure door — one held by each of two different people. Neither person can open the door alone, requiring collusion for compromise.

In **IT**, this often looks like:

- A requester submits a request for access.
- An approver decides if access should be granted.
- The action is only taken after approval.

Operating system security hinges on five core principles—

Least Privilege,
Defense in Depth,
Fail-Safe Defaults,
Economy of Mechanism, and Complete Mediation

to protect against unauthorized access and maintain system integrity. These principles, often implemented through access controls, encryption, and auditing, ensure that only authorized users access resources, data is secure, and systems are resilient to attacks.

1. Least Privilege

- **Explanation:** Users and processes are granted the minimum level of access permissions necessary to perform their job, reducing the potential damage from compromised accounts.
- **Example:** A standard user account cannot install system-wide software or modify system files; only the administrator account has these privileges.

2. Defense in Depth

- **Explanation:** Implementing multiple, layered security controls so that if one mechanism fails, others are in place to protect the system.
- **Example:** A system is protected by a firewall, antivirus software, and strong user authentication, rather than just one of these.

3. Fail-Safe Defaults

- **Explanation:** Defaulting to a secure state, such as denying all access, rather than allowing access by default.
- **Example:** A new user account created on the system has no permissions to access files until the administrator explicitly grants them.

4. Economy of Mechanism

- **Explanation:** Keeping security designs as simple and small as possible to minimize potential bugs, vulnerabilities, and unforeseen interactions.
- **Example:** Using a small, specialized security kernel to handle access control rather than a large, complex application with many features.

5. Complete Mediation

Explanation: Every access attempt to a resource must be checked for authorization, rather than relying on cached permissions.

Home works

Answer the following MCQ questions:

1. Which principle states that programs, users and even the systems be given just enough privileges to perform their task?

(a) Principle of operating system

(b) Principle of least privilege

(c) Principle of process scheduling

(d) None of the mentioned

2. For system protection, a process should access _____

(a) all the resources

(b) few resources but authorization is not required

(c) only those resources for which it has authorization

(d) All of the mentioned

3. The protection domain of a process contains _____

(a) object name

(b) rights-set

(c) both object name and rights-set

(d) None of the mentioned

4. If the set of resources available to the process is fixed throughout the process's lifetime then its domain is _____

(a) static

(b) dynamic

(c) neither static nor dynamic

(d) both static as well as dynamic

5. In domain structure what is Access-right equal to?

(a) Access-right = read-name, write-set

(b) Access-right = object-name, rights-set

(c) Access-right = read-name, execute-set

(d) Access-right = object-name, execute-set

6. Who can add new rights and remove some rights?

(a) User

(b) Any person

(c) Visitor

(d) Owner

7. Which of the following objects require protection?

(a) Memory

(b) Monitor

(c) Power supply unit

(d) All of the mentioned

8. What is a trap door in a program?

(a) A type of antivirus

(b) Security hole in a network

(c) A security hole, inserted at programming time in the system for later use

(d) None of the mentioned

9. File virus attaches itself to the _____

(a) source file

(b) object file

(c) executable file

(d) All of the mentioned

10. Which of the following is a good practice?

(a) Give full permission for remote transferring

(b) Grant read only permission

(c) Give both read and write permission but not execute

(d) Grant limited permission to specified account

11. Which of the following is a strong password?

(a) 19thAugust88

(b) Darshan025

(c) Engineering

(d) P@assw0rd

12. Which happens first authorization or authentication?

(a) Authorization

(b) Authentication

(c) Authorization & Authentication are same

(d) None of the mentioned

13. What is theft of service?

(a) This type of violation involves unauthorized reading of data

(b) This violation involves unauthorized modification of data

(c) This violation involves unauthorized destruction of data

(d) This violation involves unauthorized use of resources

14. What is Trojan horse?

(a) It is a useful way to encrypt password

(b) It is a user which steals valuable information

(c) It is a rogue program which tricks users

(d) It's a brute force attack algorithm

15. What is trap door?

(a) It is trap door in WarGames

(b) It is a hole in software left by designer

(c) It is a Trojan horse

(d) It is a virus which traps and locks user terminal

16. What is used to protect network from outside internet access?

(a) A trusted antivirus

(b) 24 hours scanning for virus

(c) Firewall to separate trusted and untrusted network

(d) Deny users access to websites which can potentially cause security leak

17. Which of the following is/are Design Principles of Security?

(a) Principles of least privileges

(b) Principles of separation of privileges

(c) Principles of least common mechanism

(d) All of the mentioned

18. Which Design Principles of Security states that subject should be given only those privileges that it requires?

(a) Principles of least privileges

(b) Principles of separation of privileges

(c) Principles of least common mechanism

(d) Principles of fail safe defaults

19. Which Design Principles of Security states that all the accesses to object be checked in order to ensure that they are allowed?

(a) Principles of least privileges

(b) Principles of separation of privileges

(c) Principles of complete mediation

(d) Principles of fail safe defaults

20. What forces the user to change password at first logon ?

(a) Default behavior of OS

(b) Part of AES encryption practice

(c) Devices being accessed forces the user

(d) Account administrator

21. What is trap door?

(a) It is a secret entry point into a program

(b) It is a hole in software left by designer

(c) Both A and B

(d) None of the mentioned

22. Which one is not an antivirus?

(a) Norton

(b) Quick Heal

(c) AVG

(d) MS Office

23. _____ software is a type of program designed and developed to protect computers from malware like viruses, computer worms, spyware etc.

(a) System

(b) Antivirus

(c) Fighter

(d) Preventer

24. The functions of Antivirus programs is/are _____

(a) scan the system

(b) detect viruses

(c) remove viruses

(d) All of the mentioned

25. _____ confirms your identity to grant access to the system.

(a) Authentication

(b) Authorization

(c) Encryption

(d) None of the mentioned

26. _____determines whether you are authorized to access the resources.

(a) Authentication

(b) Authorization

(c) Encryption

(d) None of the mentioned

27. When you log on to a PC with a user name and password you are _____

(a) Authenticating

(b) Authorizing

(c) Encrypting

(d) None of the mentioned

28. Which principle states that users and systems should be given just enough privileges to perform their tasks?
A) Mandatory Access Control
B) Principle of Least Privilege
C) Role-Based Access Control
D) Discretionary Access Control

29. What is a "trap door" in operating system security?
A) A type of firewall
B) A secure login mechanism
C) A security hole inserted at programming time for later use
D) A method to encrypt files

30. Which of the following is an attack designed to make a machine or network resource unavailable to its users?
A) Spoofed attack
B) Trojan horse
C) Denial-of-Service (DoS)
D) Logic bomb

31. Buffer overflow attack can lead to which of the following?
A) Increased system performance
B) Improved memory management
C) System crash or unauthorized code execution
D) Enhanced user authentication

32. A malicious program that disguises itself as a legitimate application is called a:
A) Virus
B) Worm
C) Trojan horse
D) Logic bomb

33. When an attempt is to make a machine or network resource unavailable to its intended users, the attack is called _____
a) denial-of-service attack
b) slow read attack
c) spoofed attack
d) starvation attack

34. The code segment that misuses its environment is called a _____
a) internal thief
b) trojan horse
c) code stacker
d) none of the mentioned

35. File virus attaches itself to the _____
a) source file
b) object file
c) executable file
d) all of the mentioned

36. In asymmetric encryption _____
a) same key is used for encryption and decryption
b) different keys are used encryption and decryption
c) no key is required for encryption and decryption
d) none of the mentioned

37. What is the breach of integrity?
a) This type of violation involves unauthorized reading of data
b) This violation involves unauthorized modification of data
c) This violation involves unauthorized destruction of data
d) This violation involves unauthorized use of resources

38. What is breach of confidentiality?
a) This type of violation involves unauthorized reading of data
b) This violation involves unauthorized modification of data
c) This violation involves unauthorized destruction of data
d) This violation involves unauthorized use of resources

39. What is theft of service?
a) This type of violation involves unauthorized reading of data
b) This violation involves unauthorized modification of data
c) This violation involves unauthorized destruction of data
d) This violation involves unauthorized use of resources

40. What is Cyber Security?
a) Cyber Security provides security against malware
b) Cyber Security provides security against cyber-terrorists
c) Cyber Security protects a system from cyber attacks
d) All of the mentioned

41. What does cyber security protect?
a) Cyber security protects criminals
b) Cyber security protects internet-connected systems
c) Cyber security protects hackers
d) None of the mentioned

42. Which of the following is a type of cyber security?
a) Cloud Security
b) Network Security
c) Application Security
d) All of the above

43. Which of the following is an objective of network security?
a) Confidentiality
b) Integrity
c) Availability
d) All of the above

44. Which of the following is an objective of network security?
a) Confidentiality
b) Integrity
c) Availability
d) All of the above

45. Which of the following is an objective of network security?
a) Confidentiality
b) Integrity
c) Availability
d) All of the above