Operating System Security

Every computer system and software design must handle all security risks and implement the necessary measures to enforce security policies.

At the same time, it's critical to strike a balance because strong security measures might increase costs while also limiting the system's usability, utility, and smooth operation.

As a result, system designers must assure efficient performance without compromising security.

What is Operating System Security?

The process of ensuring OS availability, confidentiality, integrity is known as operating system security.

OS security refers to the processes or measures taken to protect the operating system from dangers, including viruses, worms, malware, and remote hacker intrusions.

Operating system security comprises all preventive-control procedures that protect any system assets that could be stolen, modified, or deleted if OS security is breached.

Security refers to providing safety for computer system resources like software, CPU, memory, disks, etc. It can protect against all threats, including viruses and unauthorized access. It can be enforced by assuring the operating system's integrity, confidentiality, and availability.

If an illegal user runs a computer application, the computer or data stored may be seriously damaged.

System security may be threatened through two violations, and these are as follows:

1. Threat

A program that has the potential to harm the system seriously.

2. Attack

A breach of security that allows unauthorized access to a resource.

There are two types of security breaches that can harm the system: malicious and accidental.

Malicious threats are a type of destructive computer code or web script that is designed to cause system vulnerabilities that lead to back doors and security breaches.

On the other hand, Accidental Threats are comparatively easier to protect against.

Security may be compromised through the breaches. Some of the breaches are as follows:

1. Breach of integrity

This violation has unauthorized data modification.

2. Theft of service

It involves the unauthorized use of resources.

3. Breach of confidentiality

It involves the unauthorized reading of data.

4. Breach of availability

It involves the unauthorized destruction of data.

5. Denial of service

It includes preventing legitimate use of the system. Some attacks may be accidental.

The goal of Security System

There are several goals of system security. Some of them are as follows:

1. Integrity

Unauthorized users must not be allowed to access the system's objects, and users with insufficient rights should not modify the system's critical files and resources.

2. Secrecy

The system's objects must only be available to a small number of authorized users.

The system files should not be accessible to everyone.

3. Availability

All system resources must be accessible to all authorized users, i.e., no single user/process should be able to consume all system resources.

If such a situation arises, service denial may occur. In this case, malware may restrict system resources and preventing legitimate processes from accessing them.

Types of Threats

There are mainly two types of threats that occur. These are as follows:

Program threats

The operating system's processes and kernel carry out the specified task as directed.

Program Threats occur when a user program causes these processes to do malicious operations.

The common example of a program threat is that when a program is installed on a computer, it could store and transfer user credentials to a hacker.

There are various program threats. Some of them are as follows:

1.Virus

A virus may replicate itself on the system.

Viruses are extremely dangerous and can modify/delete user files as well as crash computers.

A virus is a little piece of code that is implemented on the system program.

As the user interacts with the program, the virus becomes embedded in other files and programs, potentially rendering the system inoperable.

2. Trojan Horse

This type of application captures user login credentials.

It stores them to transfer them to a malicious user who can then log in to the computer and access system resources.

3. Logic Bomb

A logic bomb is a situation in which software only misbehaves when particular criteria are met; otherwise, it functions normally.

4. Trap Door

A trap door is when a program that is supposed to work as expected has a security weakness in itscode that allows it to do illegal actions without the user's knowledge.

System Threats

System threats are described as the misuse of system services and network connections to cause user problems.

These threats may be used to trigger the program threats over an entire network, known as program attacks.

System threats make an environment in which OS resources and user files may be misused.

There are various system threats. Some of them are as follows:

1. Port Scanning

It is a method by which the cracker determines the system's vulnerabilities for an attack.

It is a fully automated process that includes connecting to a specific port via TCP/IP.

To protect the attacker's identity, port scanning attacks are launched through Zombie Systems, which previously independent systems now serve their owners while being utilized for such terrible purposes.

2. Worm

The worm is a process that can choke a system's performance by exhausting all system resources.

A Worm process makes several clones, each consuming system resources and preventing all other processes from getting essential resources. Worm processes can even bring a network to a halt.

3. Denial of Service

Denial of service attacks usually prevents users from legitimately using the system.

For example, if a denial-of-service attack is executed against the browser's content settings, a user may be unable to access the internet.

Threats to Operating System

There are various threats to the operating system.

Some of them are as follows:

Malware

It contains viruses, worms, trojan horses, and other dangerous software.

These are generally short code snippets that may corrupt files, delete the data, replicate to propagate further, and even crash a system.

The malware frequently goes unnoticed by the victim user while criminals silently extract important data.

Network Intrusion

Network intruders are classified as masqueraders, misfeasors, and unauthorized users.

A masquerader is an unauthorized person who gains access to a system and uses an authorized person's account.

A misfeasor is a legitimate user who gains unauthorized access to and misuses programs, data, or resources.

A rogue user takes supervisory authority and tries to evade access constraints and audit collection.

Buffer Overflow

It is also known as buffer overrun.

It is the most common and dangerous security issue of the operating system.

It is defined as a condition at an interface under which more input may be placed into a buffer and a data holding area than the allotted capacity, and it may overwrite other information.

Attackers use such a situation to crash a system or insert specially created malware that allows them to take control of the system.

How to ensure Operating System Security?

There are various ways to ensure operating system security. These are as follows:

Authentication

The process of identifying every system user and associating the programs executing with those users is known as authentication.

The operating system is responsible for implementing a security system that ensures the authenticity of a user who is executing a specific program.

In general, operating systems identify and authenticate users in three ways.

1. Username/Password

Every user contains a unique username and password that should be input correctly before accessing a system.

2. User Attribution

These techniques usually include biometric verification, such as fingerprints, retina scans, etc. This authentication is based on user uniqueness and is compared to database samples already in the system. Users can only allow access if there is a match.

3. User card and Key

To login into the system, the user must punch a card into a card slot or enter a key produced by a key generator into an option provided by the operating system.

One Time passwords

Along with standard authentication, one-time passwords give an extra layer of security.

Every time a user attempts to log into the One-Time Password system, a unique password is needed.

Once a one-time password has been used, it cannot be reused. One-time passwords may be implemented in several ways.

1. Secret Key

The user is given a hardware device that can generate a secret id that is linked to the user's id. The system prompts for such a secret id, which must be generated each time you log in.

2. Random numbers

Users are given cards that have alphabets and numbers printed on them. The system requests numbers that correspond to a few alphabets chosen at random.

3. Network password

Some commercial applications issue one-time passwords to registered mobile/email addresses, which must be input before logging in.

Firewalls

Firewalls are essential for monitoring all incoming and outgoing traffic.

It imposes local security, defining the traffic that may travel through it.

Firewalls are an efficient way of protecting network systems or local systems from any network-based security threat.

Physical Security

The most important method of maintaining operating system security is physical security.

An attacker with physical access to a system may edit, remove, or steal important files since operating system code and configuration files are stored on the hard drive.

Operating System Security Policies and Procedures

Various operating system security policies may be implemented based on the organization that you are working in.

In general, an OS security policy is a document that specifies the procedures for ensuring that the operating system maintains a specific level of integrity, confidentiality, and availability.

OS Security protects systems and data from worms, malware, threats, ransomware, back door intrusions, viruses, etc.

Security policies handle all preventative activities and procedures to ensure an operating system's protection, including steal, edited, and deleted data.

As OS security policies and procedures cover a large area, there are various techniques to addressing them.

Some of them are as follows:
1. Installing and updating anti-virus software
2. Ensure the systems are patched or updated regularly
3. Implementing user management policies to protect user accounts and privileges.
4. Installing a firewall and ensuring that it is properly set to monitor all incoming and outgoing traffic.

OS security policies and procedures are developed and implemented to ensure that you must first determine which assets, systems, hardware, and date are the most vital to your organization.

Once that is completed, a policy can be developed to secure and safeguard them properly