System Protection & System Security

System Protection: Goals of Protection, Principles and domain of protection, Access Matrix, Access Control, Revocation of access Rights.

1. System Protection:

System protection in an OS refers to the mechanisms implemented by the OS to ensure the security and integrity of the system.

System protection involves various techniques to prevent unauthorized access, misuse or modification of the OS and its resources.

There are several ways in which an OS can provide system protection:

User Authentication:

The OS requires users to authenticate themselves before accessing the system.
User names and passwords are commonly used for this purpose.

Access Control:

The OS uses access control lists (ACLs) to determine which users (or) processes have permission to access specific resources (or) perform specific actions.

Encryption:

The OS can use encryption to protect sensitive data and prevent unauthorized access.

Firewall :

A firewall is a software program that monitors and controls incoming and outgoing network traffic based on predefined security rules.

Antivirus Software:

Antivirus software is used to protect the system from viruses, malware, and other malicious software.

System Updates and Patches :

The OS must be kept ~~on~~ up-to-date with the latest security patches and updates to prevent known vulnerabilities from being exploited.

Protection :-

Protection refers to a mechanism which controls the access of programs, processes or users to the resources defined by a computer system.

Need of Protection:

→ To prevent the access of unauthorized users.

→ To ensure that each active programs or processes in the system uses resources only as the started policy.

⇒ To improve reliability by detecting latent errors.

Role of Protection:

The role of protection is to provide a mechanism that implement policies which defines the uses of resources in the computer system.

Some policies are defined at the time of design of the system, some are designed by management of the system and some are defined by the users of the system to protect their own files and programs.

Policy is different from mechanism. Mechanisms determine how something will be done and policies determine what will be done.

Advantages:-

→ Ensures the security and integrity of the system.
→ Prevents unauthorized access, misuse, or modification of the OS. and its resources
→ Protects sensitive data.
→ Provides a secure environment for users and applications.
→ Prevents malware and other security threats
→ Allows for safe sharing of resources and data among users and applications.

Disadvantages:

→ Can be complex and difficult to implement and manage.
→ May slow down system performance due to increased security measures.
→ Can create additional costs for implementing and maintaining security measures
→ Can create a false sense of security if users are not properly educated.
→ Can cause compatibility issues with some applications or hardware.

2. Goals of Protection :-

The goals of protection in various contents such as personal security, data security and environmental conservation, resources, and environment from harm, risks (or) negative impacts

Here are some common goals of protection.

Security and Safety:

The primary goal of protection is to ensure the security and safety of individuals, communities, (or) assets.

Preventing Harm:

Protection aims to prevent harm (or) injury to people, animals (or) the environment.

Preserving Privacy:

In the content of data security and privacy, protection seeks to safeguard personal (or) sensitive information from unauthorized access.

Preventing Theft and Fraud:

Protection strives to prevent theft, fraud, and unauthorized use of assets, resources.

Maintaining Integrity:

In data security and information technology, protection aims to preserve the integrity of data.

Cybersecurity:

Protection involves safeguarding computer systems networks, and information from cyber threats like hacking, malware, and data breaches.

Financial Protection:
This goal includes measures like insurance and risk management to protect individuals and business from financial losses.

3. Principles and Domain of Protection:-

~~Principles of Protection:~~

The principles and domains of protection in an OS are crucial for maintaining a secure and reliable computing environment.
Here are the key principles and domains of protection in OS:

Principle of Least Privilege:
This principle states that a user (or) process should only be granted the minimum level of access and privileges necessary to perform its tasks.

Authentication and Authorization:
The OS ensures that users are authenticated, verifying their identities, and then authorizes them to access specific resources based on their assigned permissions.

Access Control:
Access control mechanisms enforce restrictions on users actions, preventing unauthorized access to resources, files, and system functions.

Process Isolation:
processes running on the OS are isolated from each other, ensuring that one process can not interfere with the execution of another process.

Memory Protection:

Memory protection prevents processes from accessing the memory space of other processes (or) the OS kernel.

File System Security:

The OS implements file permissions and encryption to protect files from unauthorized access and modifications.

Network security:

Network security features such as firewalls and encryption, help protect the OS and its resources from unauthorized access.

Auditing and Logging:

The OS keeps track of system events, user activities, and potential security breaches through auditing and logging mechanisms.

Virtualization and Sandboxing:

Virtualization technologies can create isolated environments to run applications securely.

Secure Boot:

Secure boot ensures that the OS and its components are securely loaded and have not been tempered with during the boot process.

System Call Interface:

The OS provides a system call interface that allows processes to request services from the kernel.

4. Access Matrix :-

An access matrix is a security model used in computer systems and OS to represent and control access rights and permissions ~~for various subjects~~

It provides a systematic way of defining and managing access control for different entities in a system.

The access matrix is typically represented as a table with rows representing subjects and columns representing objects.

Each cell in the matrix indicates the access rights or permissions that a particular subject has on a specific object.

The access ~~ka~~ rights can be binary (allow or deny) or more granular (read, write, execute etc).

Eg

	obj1	obj2	obj3	----	objn
sub1	R/w	R	-		-
sub2	-	-	R/w		-
sub3	-	-	-		R
:	---	---	---		---
subm	-	R/w	-		R/w

In this example, the access matrix shows access rights for 'm' subjects to n objects.

The letters 'R' and 'W' represent read and write permissions, while '-' denotes that access is denied.

The access matrix can be quite large and complex in real world scenarios with many users, resources, and access rights.

It helps system administrators and security managers to have a comprehensive view of access control, making it easier to manage permissions and identify potential security risks.

Access matrices can be implemented using various access control mechanisms, such as.

→ DAC - Discretionary Access Control.

→ MAC - Mandatory Access Control.

→ RBAC - Role-Based Access Control

→ ABAC - Attribute Based Access Control.

3. Access Control :-

Access control is a security technique that regulates who (or) what can view (or) use resources in a computing environment.

It is a fundamental concept in security that minimizes risk to the business (or) organization.

There are 2 types of access control.

→ Physical

→ Logical

Physical access control limits access to campuses, buildings, rooms and physical IT assets.

Logical access control limits connections to computer networks, system files and data.

Physical access control panels restrict to entry rooms and buildings as well as alarms and lockdown capabilities, to prevent unauthorized access.

Logical access control systems perform identification authentication and authorization of users and entities by evaluating required logic credentials that can include passwords, personal identification numbers, biometric scans, security tokens (or) other authentication factors.

The goal of access control is to minimize the security risk of unauthorized access to physical and logical systems.

How access control works:-

Access controls identify an individual (or) entity, verify the person (or) application is who (or) what it claims to be and authorizes the access level set of actions associated with the username or IP address.

Organizations use different access control models depending on their compliance requirements and the security levels of IT they are trying to protect.

Types of Access Control :-

MAC:-

MAC - Mandatory Access Control.
This is a security model in which access rights are regulated by a central authority based on multiple levels of security.

MAC grants (or) denies access to resource objects based on the information security clearance of the user (or) device.

DAC :-

DAC - Discretionary Access ~~Con~~ Control.
This is an access control method in which owners (or) administrators of the protected system, data (or) resource set the policies

defining who (or) what is authorized to access the resource.

Many of these systems enable administrators to limit the propagation of access rights.

RBAC :-

RBAC - Role-Based Access Control.

This is a widely used access control mechanism that restricts access to computer resources based on individuals on groups with defined business functions.

Rule-BAC :-

This is a security model in which the system administrator defines the rules that govern access to resource objects.

Attribute Based AC :-

This is a methodology that manages access rights by evaluating a set of rules, policies and relationships using the attributes of users, systems and environmental conditions.

6. Revocation of Access Rights :-

The revocation of access rights also known as access control revocation, is the process of removing previously granted permissions (or) privileges from users, processes (or) entities in a computer system (or) network.

Access rights revocation is an essential aspect of access control and security management, as it helps prevent unauthorized access and ensures that users only have access to the resources.

Here's how the revocation of access rights works.

Reasons for Revocation:

Access rights may need to be revoked for various reasons, including

-> Termination of an employee.

-> change in roles or responsibilities.

-> security breaches

-> Violation of policies.

Access Rights Review:

Regular access rights reviews are essential to identify and correct any inconsistencies or unnecessary permissions granted to users or processes.

Access Rights Removal:

When its determined that access rights need to be revoked, the necessary actions are taken to remove the associated permissions.

Immediate Revocation:

In certain situations, access rights may need to be revoked immediately such as in cases of security breaches.

Communicating Changes:

Its crucial to communicate access rights changes to affected users and stakeholders.

Monitoring and Logging:

Access control systems should log access rights and access attempts.

Automated Revocation:

In modern systems, access rights revocation can often be automated through identity and access management (IAM) systems.

By promptly removing unnecessary (or inappropriate permissions and continuously reviewing and adjusting access rights, organizations can reduce the risk of unauthorized access and potential security breaches.

System Security: Introduction, Program threats, system and network threats, Cryptography as a security, User authentication, Implementing security defenses, firewalling to protect systems and networks, Computer security classification.

1. System Security:-

Security refers to providing protection to the computer systems resources such as CPU, memory, disk, software programs, and most importantly data/information stored in the computer system.

If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it.

So, a computer must be protected against unauthorized access, malicious access to system memory, viruses, worms etc.

Here are some key aspects of system security in an OS:

Access Control:

Access control mechanisms regulate and control who can access the system, applications, files, and other resources.

User Authentication:

The OS verifies the identities of users attempting to log in. or log out.

Authorization:-

Once a user is authenticated, the os determines their access rights and permissions.

File and Directory Permissions:

The OS allows administrators to set permissions on files and directories, determing which users or groups can read, write or execute them.

Encryption:

System security often involves data encryption to protect sensitive information from unauthorized access.

Firewalls:

Firewalls are used to control and monitor network traffic, preventing unauthorized access and protecting the system from network based attacks.

Malware Protection:

The OS can incorporate antivirus software and other security tools to detect and remove malware (viruses, worms, Trojans etc).

Secure Boot:

Secure boot ensures that only trusted and signed boot loaders and OS components are loaded during system startup.

Patch Management:

Regularly updating the OS with security patches and software updates helps address known vulnerabilities.

Backup and Disaster Recovery:

Implementing backup strategies and disaster recovery plans helps ensure data recovery in case of data loss or system failures.

Virtualization and Sandboxing:
Using virtualization and sandboxing technologies helps isolate applications and processes.

Secure Remote Access:
Implementing secure remote access protocols, such as VPNs (Virtual Private Networks), ensures that remote connections are encrypted and protected.

2. Program Threats:-

Program threats also known as software threats (or software vulnerabilities, refer to potential weaknesses and security risks that exist in computer programs (or software applications.

One of the common example of program threat is a program installed in a computer which can store and send user credentials via network to some hacker.

Following are the list of well known program threats.

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

Trap Door:
It perform illegal action without knowledge of user then it is called ~~as~~ Trap Door.

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.

Virus:-

Virus as name suggest can replicate themselves on computer system. They are highly dangerous and can modify (or) delete user files, crash systems.

Buffer Overflow:-

Occurs when a program writes more data into a buffer (temporary data storage) than it can hold, leading to memory corruption.

Injection Attacks:

Attackers inject malicious code (eg. SQL Injection command injection) into an application to exploit vulnerabilities.

Cross Site Scripting:

XSS allows attackers to inject malicious scripts into web applications, which are then executed by unsuspecting users browsers.

Path Traversal:

Enables attackers to navigate through the directory structure of a system to access unauthorized files and directories

Zero-Day Exploits:

Attacks that target previously unknown vulnerabilities for which no patches or fixes are available.

To address program threats, software developers and organizations should follow secure coding practices, conduct regular security assessments and testing, apply software updates and patches and implement security controls and best practices throughout the software development lifecycle.

3. System and Network Threats:

System threats refers to misuse of system services and network connections to put the user in trouble.

System threats can be used to launch program threats on a complete network called as program attack.

Following is the list of some well-known 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.

Worm processes can even shut down an entire network.

Port Scanning:

Port scanning is a mechanism by which a hacker can detects system vulnerabilities to make an attack on the system.

Malware:

Malicious software, including viruses, worms, Trojans, ransomware, and spyware, designed to distrupt, damage or gain unauthorized access to systems and data.

Root kits:

Conceal malicious software by modifying system code and evading detection.

Insider Threats:

Malicious or negligent actions by employees or individuals with authorized access to the system.

Data Breaches:

Unauthorized access, disclosure, or theft of sensitive data.

System and Network threats encompass a wide range of risks and potential attacks that target computer systems, networks, and the data they handle.

Man-in-the-Middle (MitM) Attacks:

Intercept and manipulate communication b/w two parties, often to eavesdrop or modify data.

Phishing:

Deceptive emails, websites, or messages used to trick users into revealing sensitive information.

Network Sniffing:

Capturing and analyzing network traffic to intercept and collect sensitive data.

Network Spoofing:

Impersonating trusted devices or users on a network to gain unauthorized access.

Brut-Force Attacks:

Repeatedly trying all possible combinations of passwords or encryption keys to gain access.

Packet Injection:

Inserting malicious packets into a data stream to disrupt or manipulate network communication.

ARP Poisoning | ARP Spoofing:

Manipulating Address Resolution Protocol tables to intercept or redirect network traffic.

DNS Spoofing:

Redirecting DNS queries to malicious servers to perform man-in-the-middle attacks.

Botnets:

Networks of compromised computers controlled by attackers to perform coordinated attacks, send spam, or conduct DDoS attacks.

To protect against these threats, organizations should implement a layered approach to security, which includes using firewalls, antivirus software, access controls, strong authentication methods, regular system patching, encryption and employee security training.

4. Cryptography as a Security:-

Cryptography is technique of securing information and communications through use of codes so that only those person for whome the information is intended can understand it and process it.

The prefix "crypt" means "hidden" and suffix graphy means "writing".

In cryptography the techniques which are used to protect information are obtained from mathematical concepts and set of rule based calculations known as algorithms to convert messages that maket it hard to decode it.

These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

In cryptography, the plain text is converted to cipher text which is decoded by the receiver and hence this process is known as encryption.

The process of conversion of cipher text to plain text this is known as decryption.

Features of Cryptography:

Confidentiality:

Information can only be accessed by the person for whom it is intended and no other person can access it.

Integrity:

Information can not be modified in storage or transition b/w sender and intended receiver without any addition to information being detected.

Authentication:

The identities ~~of~~ of sender and receiver are confired. As well as destination/origin of information is confirmed..

Non-Repudiation:

Non-repudiation ensures that a sender cannot deny sending a message or performing a transaction.

Secure Communication:

Cryptography enables secure communication over insecure channels by encrypting data during transmission.

Access Control:

Cryptography is used in access control mechanisms such as password hashing and encryption to protect user credentials and restrict unauthorized access to sensitive systems and data.

Data Protection and Privacy:

Cryptography is crucial for protecting sensitive personal and financial information.

Secure Storage:

Data encryption ensures that sensitive information stored in DB, cloud services (on portable devices remains protected.

Secure Transactions: => End to end encryption:-

Cryptography plays a significant role in secure online transactions, including e-commerce and financial transactions, protecting credit card information and sensitive financial data.

5. User Authentication:-

User authentication is the process of verifying the identity of a user to ensure that they are who they claim to be.

It is a critical component of a security system and is used to control access to various resources, systems and applications.

User authentication helps prevent unauthorized access, protect sensitive information, and maintain the overall security and integrity of computer system.

Username and Password:

User provides a unique username and a corresponding password, which they must enter correctly to gain access.

2FA - Two-Factor Authentication:

Also known as multi factor authentication - MFA. 2FA requires users to provide two (or) more authentication factors for access.

Biometric Authentication:-

Biometric authentication uses unique physical characteristics to verify a users identity. Common biometric methods include fingerprint recognition, facial recognition, iris scanning, voice recognition, and behavioral biometrics.

Token Based Authentication:-

In this method, users are provided with physical (or) virtual tokens that generate one-time passwords (or) cryptographic codes for each authentication attempt.

Certificate Based Authencation:

Digital certificates are used to authenticate users and devices. The certificate contains a public key.

SSO - Single SignOn:

SSO allows users to authenticate once and gain access to multiple applications and systems without re-entering their credentials.

Passwordless Authentication:

This method eliminates the need for traditional passwords and relies on other authentication factors such as biometrics (or) security keys.

Social Login:-

users can login using their existing social media accounts (eg. Google, FB etc) as authentication credentials.

Time Based OTP :-

A temporary code is generated based on the current time and a shared secret, which is used for authentication.

KBA - Knowledge Based Authentication :

Users answer predefined security questions (or) provide personal information to verify their identity.

Geolocation Authentication :

User locations are used as an additional factor for authentication.

---

6. Implementing security Defenses :-

Implementing security defenses is a critical aspect of ensuring the protection, integrity, and availability of computer systems, networks and data.

Security defenses aim to prevent, detect and respond to various threats and vulnerabilities that may compromise the security of an organization.

Here are some key steps and practices for implementing security defenses.

Security Policies and Procedures :

Develop and enforce robust security policies and procedures that outline the organization's security objectives and define roles, responsibilities.

Acces Control:-

Implement strong access controls to ensure that only authorized users have appropriate access to systems, applications and data.

Authentication and Autherization:

Use strong authentication methods and control user access based on the principle of least privilege.

Encryption:

Encrypt sensitive data to protect it from unauthorized access.

Firewalls and Network Segmentation:

Use firewalls and network segmentation to control traffic and isolate critical systems from potential threats.

IDPS:-

Intrusion Detection and Prevention Systems.

Deploy IDPS solutions to detect and respond to potential security breaches and attacks.

Antivirus and Antimalware Solutions:-

Install and regularly update antivirus and anti-malware software to protect against known threats.

Patch Management:-

Regularly apply security patches and updates to OS, applications and firmware to address known vulnerabilities

Backup and Disaster Recovery:-

Penetration Testing:

Conduct regular penetration techniques to identify vulnerabilities and weaknesses in the system security defenses.

Physical Security:

Implement physical security measures to protect access to data centers and critical infrastructure.

---

7. Firewalling to protect systems and Networks:

Firewalling is a crucial security measure used to protect computer systems and networks from unauthorized access, malicious activities, and potential cyber threats.

A firewall acts as a barrier b/w an internal network and external network (such as internet), controlling and monitoring incoming and outgoing network traffic based on predetermined security rules.

Here are the key ways in which firewalling helps protect systems and networks.

Packet Filtering:

Firewalls examine individual data packets in network traffic based on defined rules.

They can allow or block packets based on criteria such as source and destination IP addresses, port numbers, and protocols.

Network Segmentation:

Firewalls can be used to divide a network into smaller segments, each with its own security policies.

Application Layer Filtering:

Modern firewalls can inspect the content of data packets at the application layer, allowing them to detect and block specific types of content, such as malware, viruses and malicious scripts.

Intrusion Detection/Prevention:

Some advanced firewalls include intrusion detection and prevention capabilities, which can identify malicious ~~or~~ suspicious activities in real-time.

VPN:

Virtual Private Network. ~~supports~~.

Firewalls often provide support to secure VPN connections, allowing remote users to access the internal network securely over encrypted connections.

Logging and Auditing:

Firewalls can log network traffic and security events, providing valuable information for monitoring. ~~and~~

Protection Against DoS and DDoS Attacks:

Firewalls can be configured to mitigate Denial-of-service (DoS) and Distributed DoS attacks by filtering and rate-limiting traffic.

Security Updates and Threat Intelligence:

Firewall vendors regularly release security updates and threat intelligence feeds to keep the firewalls rules upto date. and effect against emerging threats..

8: Computer Security classification:-

As per the US department of Defense Trusted Computer Systems Evaluation Criteria there are 4 security classifications in computer system A, B, C, and D.

Each level has specific access controls and restrictions to ensure that data is appropriately handled and protected.

Here's an overview of the 4 security classification levels.

Type-A:-

class-A : (Top Secret).

→ The highest security classification level.

→ Uses formal design specifications and verification techniques.

→ Access to class A data is highly restricted, and only individuals with appropriate security clearance are granted acess.

Type-B:

classB : secret.

→ The second highest security classification level.

→ Access to class B data is also restricted, and individuals must have the appropriate security clearance and a valid reason to access this information.

It is of 3 types.

(i) B1 : Maintains the security label of each object in the system.

(ii) B2 : Extends the sensitivity labels to each system resource, such as storage objects.

(iii) B3 : Allows creating lists (or) user groups for access control to grant access (or) revoke access.

Type-C : Class-C : Confidential

→ The third security classification level.

→ Access to class-C data is limited to authorized individuals who have been cleared for this level of sensitivity.

→ Provides protection and user accountability using audit capabilities. It is of 2 types.

(i) C1 : Incorporates controls so that users can protect their private information.

(ii) C2 : Adds an individual level access control to the capabilities of a C1 level system.

Type-D :

Class-D : Unclassified.

→ The lowest security classification level.

→ Class-D data is accessible to a wide range of users without the need for special clearance. (or) restrictions.

→ It has minimum protection.

MS-DOS and windows 3.1 fall in this category.