Ch-7- Security and Protection

* Explain Security Environment in Operating System.

=> Every computer system and software design must handle all security risk.

The Process of ensuring OS availabity, confidentiality, Integrity is known as operating system security.

OS Security refers to the process or measures taken to protect the Operating system from dangers.

Process have to also protection From viruses, worms and remote hacker instrusions.

Security refers to providing safety for computer system resources like software, CPU, memory, disks etc.

System Security may be threatened through two violations

1) Threat
2) Attack

1 Threat:

A Program that has the potential to harm the system seriously this is called Threat.

There are two types of Threat.

(i) Program Threat
(ii) System Threat

(i) Program Threat:

Program Threat occur when a user program causes these process to do malicious operations.

(ii) System Threat:

System Threat may be used to trigger the program threats over an entire network.

2 Attack:

A breach of Security that allows unauthorized access to a resource, this is called Attack.

This is the Goal of Security System.

(a) Integrity:

~~That~~ Unauthorized user must not be allowed to access the system's objects.

(b) Secrecy:

The system's object must only be available to small number of authorized user.

(c) Availability:

All system resources must be accessible to all authorized users

Page No.
Date : / /

* Explain Design Principle of Security system.

=> This are the basic Design Principle of security system.

1 Least Privilege :

It requires that users be given the minimum permission to perform their tasks.

2 Economy of Mechanism :

A system should be designed to minimize the number of distinct components.

3 Fail - Safe Defaults :

Fail - Safe defaults are security setting that are prevent unauthorized use of resources.

4 Complete Mediation :

System should be reviewed and updated on a regular basis.

Page No.
Date : / /

5 Open Design:

System should be design in such a way that they can be easily inspected or analyzed.

6 Separation of Privilage:

System should be design in such way that user should not be able to access all areas of system

7 Least Comman Mechanism:

System should be designed so that there is a minimum number of Mechanism shared by all users.

8 Psychological Acceptability:

User have to accept all the security measures implemented in a system.

Page No.
Date : / /

* Explain User Authentication in Operating System.

=> Authentication is the process of verifying the identity of a user or information.

User Authentication is the process of verifying of a user when that user logs in a system.

There are different types of authentication systems.

1 Single-Factor Authentication:

In this authentication, user has to enter the username and the password to confirm whether that user is logging or not.

2 Two-Factor Authentication:

In this authentication, User has to give username, password and other information.

3 Multi - Factor Authentication:

In this authentication, more than one factor of authentication is needed.

There are Basic Authentication Method.

1 Password :

Password Verification is the most popular and commonly used authentication method.

A Password is a secrect text that is supposed to ~~be~~ known only to a users.

If User enter right Password than User is logged in the system.

2 Physical Identification:

This method includes machine-readable symbols, cards or smart cards.

This allows authentication without the storage of passwords in system.

3 Biometrics:

This methods of authentication is based on the unique biological characteristics of each users.

This are the comman use Biometrics method.

- Facial Characteristics
- Fingerprints
- Hand Geometry
- Retinal Pattern
- Voice

* Explain Protection Mechanism.

=> Protection is important in a multiuser environment when multiple user use computer resources such as CPU, memory etc.

It is the operating system's

responsibility to offer a mechanism that protects each process from other process.

A Protection mechanism that controls the access of programs, processes or user defined resources.

It needs the Protection of computer resources like the software, memory, processor etc.

- Needs of Protection Mechanism:

1 There are may be security risks like unauthorized reading, writing in the system.

2 It helps to ensure data security, process security against unauthorized user access.

3 It is important to ensure no access right breaches, no viruses in the existing data.

4 Its purpose is to ensure that only the System's policies access Program, resources or data.

- Role of Protection Mechanism:

Protection Mechanism is use for implementing policies that define the use of resources.

In Protection Mechanism, every Program has distinct policies For using resources and policies may change over time.

* Explain Protection Domain and Access Control List

=> Protection Domain:

The Protection policies limit the access of each process with respect to their resource handling.

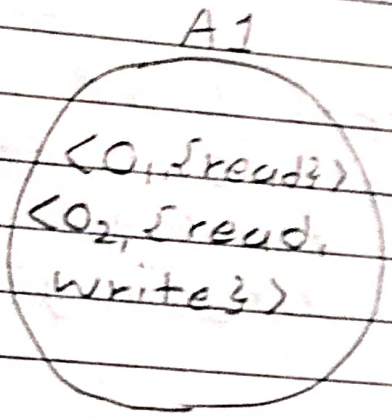
A Process is bound to use only those resources which it require to complete its task.

A computer system has processes and Objects, which are treated as abstract data types.

These Domain element is described as <object, {set of operations on object}>.

Each Domain consist of a set of object and the operations that can be performed on them.

Ex.



Here, A1 is a Process, and it consist Two object.

Object O_1 and Object O_2 consist different operation.

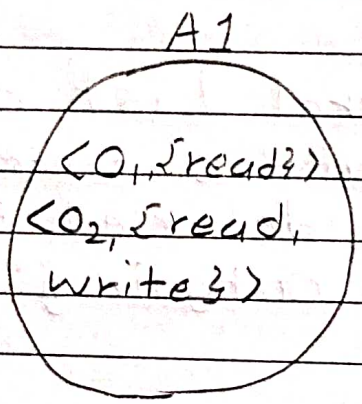
Object O_1 can perform only read operation.

Object O_2 can Perform only read and write operation.

These Domain element is described as <object, {set of operations on Object}>.

Each Domain consist of a set of object and the operations that can be performed on them.

Ex.



Here, A1 is a Process, and it consist Two Object.

Object O_1 and Object O_2 consist different operation.

Object O_1 can perform only read operation.

Object O_2 can Perform only read and write operation.

=> Access Control List:

Access Control List is a set rules defined for controlling network traffic. and

Access Control List reduse network traffics.

Access Control List are used to filtter traffic based on the set of rules defined for the incoming or outgoing of the network.

Access Control list rules defined are matched serial wise.

Access Control List should be applied to inbound or outbound of the interface.

Inbound Access List:

When an access list is applied on inbound packets of the interface then First the packets will be processed according

to the access list and then routed to the outbound interface

Outbound access lists:

When an access list is applied on outbound packets of the interface then First the packets will be routed and then processed at the outbound interface