1 question will be asked from here

a reading

Design principles of security

Saltzer and Schroeder - 8 principles for design and implementation of security mechanisms

Principles draw on ideas of simplicity and restriction.

Simplicity makes designs and mechanisms easy to understand.

Simple designs ->leads to fewer problems.

Those problems that occur->easier to deal with.

Example – Program sendmail reads configuration data from a binary file .

System administrators generated binary file by “freezing” or compiling ,a text version of configuration file .

This created 3 interfaces – mechanism used to edit the text file, mechanism used to freeze text file, mechanism sendmail used to read frozen file.

Second interface required manual intervention -> often overlooked.

To minimize problem ,sendmail checked if frozen file was newer than text file.

If not ,warned the user to update frozen configuration file.

Security problem lies in assumptions that sendmail made.

Simplicity reduces potential for inconsistencies within a policy or set of policies.

Restriction minimizes power of an entity. The entity can access only information it needs

**1)Principle of least privilege** – A subject should be given only those privileges that it needs to complete its task.

If a subject does not need an access right, it should not have the access right.

Furthermore, function of a subject (as opposed to identity) – should control the assignment of rights.

If a specific action requires subject’s access rights be augmented, the extra rights should be relinquished immediately on completion of the action.

In practice ,most systems don’t have granularity of privileges and permissions required to apply this principle precisely.

**2)Principle of least authority** – A subject should be given only the authority that it needs to complete its task.

Permission – determining what actions a process can take on an object directly, and authority – effects a process can have on an object either directly (like process) or indirectly through interaction with other processes or subsystems.

**3)Principle of fail-safe defaults** – Unless a subject is given explicit access to an object ,it should be denied access to that object.

Restricts how privileges are initialized when subject or object is created.

Requires that default access to an object is None. Whenever access, privileges or some security related attribute is not explicitly granted, it should be denied.

If subject unable to complete action or task it should undo changes it made to security state of system before it terminates.

**4)Principle of economy of mechanism**

Security mechanisms should be as simple as possible.

If design and implementation are simple, fewer possibilities exist for errors. Checking and testing process less complex as fewer components and cases need to be tested.

Complex mechanisms often make assumptions about the system in which they run. If these assumptions incorrect ,it leads to security problems.

**5)Principle of complete mediation**

Requires all accesses to objects be checked to ensure they are allowed.

This principle restricts caching of information, which often leads to simpler implementation of mechanisms.

Whenever subject attempts to read an object operating system should mediate the action.

First it determines if subject is allowed to read the object.

If so ,it provides resources for read to occur.

If subject tries to read object again, system should check subject is still allowed to read the object.

Most systems would not make second check. They would cache results of first check and base second access on cached results.

**6) Principle of open design** – Security of a mechanism should not depend on secrecy of its design or implementation.

Suggests that security should not depend solely on secrecy.

Especially true for cryptographic software and systems.

Designers and implementers of a program must not depend on secrecy of details of their design and implementations to ensure security.

If the strength of the program’s security depends on ignorance of user, a knowledgeable user can defeat that security mechanism.

“security through obscurity” captures this concept.

Companies that market cryptographic software, frequently keep their algorithms secret.

Such secrecy adds little to security of system.

Keeping keys and passwords secret, does not violate this principle as key is not an algorithm. Keeping enciphering and deciphering algorithms secret, violates it.

**7)Principle of separation of privilege** – A system should not grant permission based on a single condition.

Company cheques for more than 75,000 must be signed by 2 officers of the company. If either doesn’t sign – cheque not valid.

Systems and programs granting access to resources should do so only when more than one condition is met.

This provides fine grained control over resource, additional assurance that the access is authorized.

**8)Principle of least common mechanism**

Mechanisms used to access resources should not be shared.

Sharing resources provides channel along which information can be transmitted, so such sharing should be minimized.

**9)Principle of least astonishment**

Security mechanisms should be designed so that users understand the reason that the mechanism works the way it does, and using the mechanism is simple.

Principle recognises human element in computer security.

Principle requires security mechanisms to use a model that target audience (users and administrators) can easily understand.

If audience’s mental model too different from one used by designers and implementers, their confusion can undermine security mechanism.

Principle of least astonishment similar to principle of psychological acceptability.

**Psychological acceptability**

Principle of least astonishment similar to principle of psychological acceptability ,one of the original principles.

Security mechanisms should not make resource more difficult to access than if security mechanisms were not present.

A screenshot of a computer screen

Description automatically generated

Difference between principle of psychological acceptability ,principle of least astonishment is that principle of least astonishment is an ideal and principle of psychological acceptability recognises that security mechanisms may add additional steps to accessing the resource