1 question will be asked from here

a reading

Design principles of security

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

Principles draw on ideas of simplicity and restriction.

Simplicity makes design and mechanisms easy to understand.

Simple design ->fewer problems. Problems that occur->easier to deal with.

**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 be given that access right.

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

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

**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.

**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.

**5)Principle of complete mediation**

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

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.

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

Especially true for cryptographic software and systems.

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

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

**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 of least astonishment similar to principle of psychological acceptability.

A screenshot of a computer screen

Description automatically generated