Shreyas Patil
PA12
1032210832
PSS CCA Theory Assignment

Vidyalekhan
DATE
PAGE

Q- List and state information security design principles with an example.

Ans. Information security design principles are foundational guidelines that help in designing and implementing secure systems.

1. Least Privilege Principle: Users should only be granted the minimum level of access or permission necessary to perform their tasks.
example: Regular employees may have access to certain files and folders required for their job role, while administrators have access to more sensitive areas such as system configurations and user management.

2. Defense in depth Principle: Implement multiple layers of security controls to protect against various type of threats. If one layer is breached, other layers provide additional protection.

3. Fail-Safe defaults principle: Systems should be configured to deny all access by default and only allow access to authorized users or processes.

4. Separation of duties principle: Divide tasks and responsibilities among multiple individuals to prevent a single person or group from having complete over sensitive functions.

5. Economy of Mechanism Principle: Keep security mechanisms as simple as possible to reduce the potential for vulnerabilities and improve understanding and auditability.
EX: A company uses a widely tested and implements a recognized encryption standard like AES to protect sensitive data.