1 Security Principles

2 Security Principles

- Least privilege
- Separation of duties
- Fail safe defaults or Implicit deny
- Job rotation
- Layered security (Complete Mediation)
- Defense in depth
- Security through obscurity
- Keep it simple
-
-

3 Least Privilege

- Least privilege means a subject (user, application, or process) should have only the necessary rights and privileges to perform its task with no additional permissions.
- By limiting an object's privilege, we limit the amount of harm that can be caused (accident or error)
- For example, a person should not be logged in as an administrator—they should be logged in with a regular user account, and change their context to do administrative duties.

4 Separation of Duties (Separation of privilege)

- For any given task, more than one individual needs to be involved.
- Applicable to physical environments as well as network and host security.
- No single individual can abuse the system.
- Example: defense system fires a nuclear weapon only if two different people both give the correct command
- In a computer system, separated keys apply to any situation in which two or more conditions must be met before access should be permitted
- Potential drawback is the cost.
  - Time – Tasks take longer
  - Money – Must pay two people instead of one
  -
-

5 Fail-safe defaults (Implicit Deny)

- Base access decisions on permission rather than exclusion
- If a particular situation is not covered by any of the rules, then access can not be granted.
- Any individual without proper authorization cannot be granted access.

- The alternative to implicit deny is to allow access unless a specific rule forbids it.

6 □ **Job Rotation**

- The rotation of individuals through different tasks and duties in the organization's IT department.
- The individuals gain a better perspective of all the elements of how the various parts of the IT department can help or hinder the organization.
- Prevents a single point of failure, where only one employee knows mission critical job tasks.
- Drawback: technical expertise takes years to develop

7 □ **Layered Security (Complete mediation)**

- Layered security implements different access controls and utilizing various tools and devices within a security system on multiple levels.
- Every access to every object must be checked for authority
- Compromising the system would take longer and cost more than its worth.
- Potential downside is the amount of work it takes to create and then maintain the system.

8 □

9 □ **Diversity of Defense**

- This concept complements the layered security approach.
- Diversity of defense involves making different layers of security dissimilar.
- Even if attackers know how to get through a system that compromises one layer; they may not know how to get through the next layer that employs a different system of security.

10 □ **Security Through Obscurity (Open design)**

- Security through obscurity states that the security is effective if the environment and protection mechanisms are confusing or supposedly not generally known.
- The concept’s only objective is to hide an object (not to implement a security control to protect the object).
- It’s not effective.
- The design should not be secret
-
-

11 □ **Keep It Simple (Economy of Mechanism)**

- The simple security rule is the practice of keeping security processes and tools is simple and elegant.
- Security processes and tools should be simple to use, simple to administer, and easy to troubleshoot.
- A system should only run the services that it needs to provide and no more.

12 **Least common mechanism**

- Minimize the amount of mechanism common to more than one user and depended on by all users.
- Every shared mechanism (especially one involving shared variables) represents a potential information path between users and must be designed with great care to be sure it does not unintentionally compromise security.
- Further, any mechanism serving all users must be certified to the satisfaction of every user, a job presumably harder than satisfying only one or a few users.
- For example, given the choice of implementing a new function as a supervisor procedure shared by all users or as a library procedure that can be handled as though it were the user's own, choose the latter course.
- Then, if one or a few users are not satisfied with the level of certification of the function, they can provide a substitute or not use it at all. Either way, they can avoid being harmed by a mistake in it.

13 **Psychological acceptability**

- It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly