Design Principles

Principle of Least Privilege

A subject should be given only those privileges that it needs in order to complete its tasks

Principle of Fail-Safe Defaults

Unless a subject is given explicit access to an object, it should be denied access to that object

Principle of Economy of Mechanism

Security mechanisms should be as simple as possible

Principle of Complete Mediation

All access to objects be checked to ensure that they are allowed

Principle of Open Design

Security of a mechanism should not depend on the secrecy of its design or implementation

Principle of Separation of Privilege

A system should not grant permission based on a single condition

Principle of Least Common Mechanism

Mechanisms used to access resources should not be shared

Principle of Psychological Acceptability

Security Mechanisms should not make the resource more difficult to access than if the security mechanism were not present

Fence Post Problem

- You are building a fence 100 feet long
- You want a fence post every 10 feet
- How many fence posts do you need?

Rage

- Process a range of item N through M
- N = 5
- M = 17
- How many items are you processing?

Errors?

- How would you classify these errors?

Errors?

- How would you classify these errors?
- Off by one.

Types of Attacks

- Format String
- Buffer Overflow
- Heap Overflow