Design Principles

Dr. Ahmad Almulhem

Computer Engineering Department, KFUPM

Spring 2008
Outline

1. Overview

2. Design Principles
   - Least Privilege
   - Fail-Safe Defaults
   - Economy of Mechanism
   - Complete Mediation
   - Open Design
   - Separation of Privilege
   - Least Common Mechanism
   - Psychological Acceptability

3. Key Points
Overview

Design Principles

Principles underlie the design and implementation of mechanisms supporting security policies.

- Simplicity
  - Easy to understand
  - Less to go wrong
  - Less sanity checks
  - Fewer possible inconsistencies in policy

- Restriction
  - Minimize access
  - Minimize communication (information flow)
Principle #1: Least Privilege

A subject should be given only those privileges necessary to complete its task.
- If a subject does not need an access right, the subject should not have that right.

- Function (not identity) controls rights assignment
- Rights added as needed, discarded after use
- Minimal protection domain (resources that the process may access)
Principle #2: Fail-Safe Defaults

Default action is to deny access

- Access rights are explicitly granted
- If action fails, system as secure as when action began
Principle #3: Economy of Mechanism

Keep security mechanisms as simple as possible
- KISS Principle

- Simpler means less can go wrong
- When errors occur, they are easier to understand and fix
- Watch for interfaces and interactions
Principle #4: Complete Mediation

Check every access whether it is allowed

- Usually done once, on first action
- UNIX: access checked on open, not checked thereafter (caching)
- If permissions change after, may get unauthorized access
Open Design

Principle #5: Open Design

Security should not depend on *secrecy* of design or implementation

- **“Security through obscurity”**
  - If security depends on the ignorance of a user, a knowledgeable user will defeat it
  - Technical means: disassemblers, analysis
  - Non-technical means: searching garbage (dumpster-diving)

- Popularly misunderstood to mean that source code should be public

- Does not apply to information such as passwords or cryptographic keys
Principle #6: Separation of Privilege

Require multiple conditions to grant privilege

- Separation of duty
- Bank example: Checks more than $75,000 must be signed by two officers
- Unix example: A user change to root if
  1- user knows the root password
  2- user in wheel group
Principle #7: Least Common Mechanism

Mechanisms should not be shared

- Information can flow along shared channels
- Covert channels
- Isolation
  - Virtual machines
  - Sandboxes
Psychological Acceptability

**Principle #8: Psychological Acceptability**

Security mechanisms should not add to difficulty of accessing resource

- Hide complexity introduced by security mechanisms
- Security burden should be minimal and reasonable
- Ease of installation, configuration, use
- Human factors critical here
Key Points

- Principles of secure design underlie all security-related mechanisms
- Require:
  - Good understanding of goal of mechanism and environment in which it is to be used
  - Careful analysis and design
  - Careful implementation