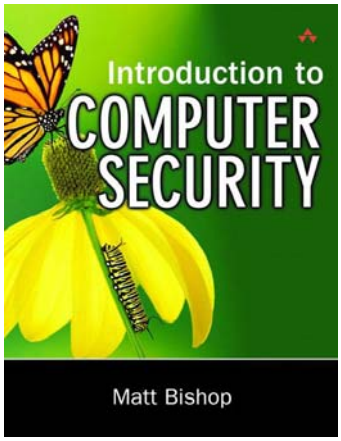
These Slides are prepared from
Matt Bishop slides and book "Introduction to Computer Security"
Benefiting from the Slides posted by Ahmad Al-Mulhem

Design Principles

Chapter 12



Adnan Gutub
gutub@kfupm.edu.sa

Computer Engineering Department
King Fahd University of Petroleum & Minerals
Dhahran, Saudi Arabia

Chapter 12: Design Principles

Overview

Designs Principles

1. Least Privilege
2. Fail-Safe Defaults
3. Economy of Mechanism
4. Complete Mediation
5. Open Design
6. Separation of Privilege
7. Least Common Mechanism
8. Psychological Acceptability

Overview

Design Principles

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

Simplicity

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

Restriction

- Minimize access
- Minimize communication (information flow)

Least Privilege

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)

Fail-Safe Defaults

Principle#2: Fail-Safe Defaults

Default action is to deny access

- Access rights are explicitly granted
  - It should be denied access otherwise
- If action fails, system as secure as when action began
  - Whenever a system security update is not complete, no changes are made to its security state
  - If the program fails, the system is safe

Economy of Mechanism

Principle#3: Economy of Mechanism

Keep security mechanisms as simple as possible

- Simpler means less can go wrong
  - when errors occur, they are easier to understand and fix
- Watch for Interfaces and interactions

Complete Mediation (Negotiation)

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
- If permissions change after, may get unauthorized access

Open Design

Principle#5: Open Design – as Kerckhkoffs Principle

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

- Popularly misunderstood to mean that source code should be public
- No "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)
- Does not apply to information such as passwords or cryptographic keys

Separation of Privilege

Principle#6: Separation of Privilege – similar to separation of duty

Require multiple conditions to grant privilege – single condition is not enough

- 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

Least Common Mechanism

Principle#7: Least Common Mechanism

Mechanisms used to access resources should not be shared

- Information can flow along shared channels

Isolation

- Virtual machines
- Sandboxes

Psychological Acceptability

Principle#8: Psychological Acceptability

Security mechanisms & human element

It should not add difficulty to accessing resources as if security mechanism is not present

- 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