

University of Rochester
CSC290B
Introduction to Computer Security

Design Principles

January 20, 2009

Design Principles

[Saltzer & Schroeder, *The Protection of Information in Computer Systems*.
Proceedings of the IEEE 63, 9 (September 1975)]

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

Overview

- **Simplicity**
 - Less to go wrong
 - Fewer possible inconsistencies
 - Easy to understand
- **Restriction**
 - Minimize access
 - Inhibit communication

Least Privilege

- A subject should be given only those privileges necessary to complete its task
 - Function, not identity, controls
 - Rights added as needed, discarded after use
 - Minimal protection domain

Fail-Safe Defaults

- Default action is to deny access
- If action fails, system as secure as when action began

Economy of Mechanism

- Keep it as simple as possible
 - KISS Principle
- Simpler means less can go wrong
 - And when errors occur, they are easier to understand and fix
- Interfaces and interactions

Complete Mediation

- Check every access
- Usually done once, on first action
 - UNIX: access checked on open, not checked thereafter
- If permissions change after, may get unauthorized access

Open Design

- Security should not depend on secrecy of design or implementation
 - Popularly misunderstood to mean that source code should be public
 - “Security through obscurity”
 - Does not apply to information such as passwords or cryptographic keys

Open Design: see also Kerckhoffs' principle

[Auguste Kerckhoffs, "La cryptographie militaire", Journal des sciences militaires, vol. IX, pp. 5–83, Jan. 1883, pp. 161–191, Feb. 1883]

- Design principles for military ciphers:
 - The system must be practically, if not mathematically, indecipherable;
 - *It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;*
 - Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents;
 - It must be applicable to telegraphic correspondence;
 - It must be portable, and its usage and function must not require the concurrence of several people;
 - Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

Separation of Privilege

- Require multiple conditions to grant privilege
 - Separation of duty
 - Defense in depth

Least Common Mechanism

- Mechanisms should not be shared
 - Information can flow along shared channels
 - Covert channels
- Isolation
 - Virtual machines
 - Sandboxes

Psychological Acceptability

- Security mechanisms should not add to difficulty of accessing resource
 - Hide complexity introduced by security mechanisms
 - 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

Acknowledgements

- Substantial portions of these slides are ©2002-2004 Matt Bishop and used with permission