Design Principles

CS461/ECE422

Computer Security I

Fall 2009

Based on slides provided by Matt Bishop for use with **Computer Security: Art and Science**

Reading Material

- Chapter 13 Computer Security: Art and Science

Overview

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

Saltzer and Schroeder 75

Summary of Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of Privilege
- Least Privilege
- Least Common Mechanisms
- Psychological Acceptability

Economy of Mechanism

- *Keep the design as simple and small as possible*
- Simpler means less can go wrong
  - And when errors occur, they are easier to understand and fix
- Interfaces and interactions

Fail-Safe Defaults

- *Base access decisions on permission rather than exclusion*
- Burden of proof is on the principal seeking permission
- If the protection system fails, then legitimate access is denied but illegitimate access is also denied

Complete Mediation

- *Every access to every object must be checked for authority*
- Usually done once, on first action
  - UNIX: access checked on open, not checked thereafter
- If permissions change after, may get unauthorized access
- Proposals to gain performance by remembering the result of an authority check should be examined skeptically

Open Design

- *The design should not be secret*
- Do 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

Separation of Privilege

- *Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key.*
- Require multiple conditions to grant privilege
  - Separation of duty
  - Defense in depth

Least Privilege

- *Every program and every user of the system should operate using the least set of privileges necessary to complete the job*
- 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

Least Common Mechanism

- *Minimize the amount of mechanism common to more than one user and depended on by all users*
- Mechanisms should not be shared
  - Information can flow along shared channels
  - Covert channels
- Isolation
  - Virtual machines
  - Sandboxes

Psychological Acceptability

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

Examine Scenarios

- Paper overhead

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