CSCI 455: Principles of Computer Security

Set 02: Security Principles

Security Fundamental Principles

- "First Principles" from NSA National Centers of Academic Excellence (CAE) for CyberOps
- First fundamental security design principles provide the foundation to reliably …
  - Build security mechanisms (e.g., access control)
  - Implement security policies
- When followed …
  - First principles enable implementation of sound security mechanisms and systems
- When not completely followed …
  - Increase risk of exploitable vulnerability existence

What Students Need To Know

- List the first principles of security
- Describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies
- Analyze common security failures and identify specific design principles that have been violated
- Identify the needed design principle, given a specific scenario
- Describe why good human machine interfaces are important to system use
- Understand the interaction between security and system usability and the importance for minimizing the affects of security mechanisms

Saltzer and Schroeder: Security Principles

- Let's start at the beginning (if we knew when the beginning was!), but how about 1973?
  - http://web.mit.edu/Saltzer/www/publications/protection

Saltzer and Schroeder: Eight Security Principles

1. Least privilege
   - States that a subject should be given only those privileges that it needs in order to complete its task
2. Fail-safe defaults
   - States that, unless a subject is given explicit access to an object, it should be denied access to that object
3. Economy of mechanism
   - States that security mechanisms should be as simple as possible
4. Complete mediation
   - Requires that all accesses to objects be checked to ensure that they are allowed.

Saltzer and Schroeder: 8 Security Principles

5. Open design
   - States that the security of a mechanism should not depend on the secrecy of its design or implementation
6. Separation of privilege
   - States that a system should not grant permission based on a single condition
7. Least common mechanism
   - Mechanisms used to access resources should not be shared
8. Psychological acceptability
   - Security mechanisms must not make the resource more difficult to access than if mechanisms were not present

From CyberOps List

- General fundamental design principles
  - Simplicity
  - Open design
  - Design for iteration
  - Least astonishment
- Security design principles
  - Minimize secrets
  - Complete mediation
  - Fail-safe defaults
  - Least privilege
  - Economy of mechanisms
  - Minimize common mechanisms
  - Isolation, separation and encapsulation
- Methods for reducing complexity including
  - Abstraction
  - Modularity
  - Layering
  - Hierarchy