Hochschule Konstanz
Fakultät Informatik

Introduction to IT Security

WIN+AIN

Hanno Langweg

01c Goals and Principles - Design Principles for Secure Systems

Saltzer/Schroeder (1975)

- One of the heavily-cited papers in computer security.
- Design principles are found in chapter 1
  - http://web.mit.edu/Saltzer/www/publications/protection/
  - http://www.acsac.org/secshelf/papers/protection_information.pdf

- Early collection of what should be common sense

"Experience has provided some useful principles that can guide the design and contribute to an implementation without security flaws."

(Saltzer/Schroeder 1975)

8+2 design principles

1. Economy of mechanism: Keep the **design** as **simple and small** as possible.

8+2 design principles

1. Economy of mechanism: Keep the **design** as **simple and small** as possible.
2. Fail-safe defaults: Base access decisions on **permission** rather than exclusion.

8+2 design principles

1. Economy of mechanism: Keep the **design** as **simple and small** as possible.
2. Fail-safe defaults: Base access decisions on **permission** rather than exclusion.
3. Complete mediation: **Every access** to every object **must be checked** for authority.

8+2 design principles

1. Economy of mechanism: Keep the **design** as **simple and small** as possible.
2. Fail-safe defaults: Base access decisions on **permission** rather than exclusion.
3. Complete mediation: **Every access** to every object **must be checked** for authority.
4. Open design: The **design should not be secret**.

8+2 design principles

5. 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.

Application of design principle: avoid highly privileged accounts like root/administrator that are attractive targets for attacks

8+2 design principles

5. 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.
6. Least privilege: Every program and every user of the system should operate using the **least set of privileges necessary** to complete the job.

8+2 design principles

7. Least common mechanism: **Minimize the amount of mechanism common** to more than one user and depended on by all users.

Application of design principle: Reduce amount of privileged code in libraries that needs to be reviewed.

8+2 design principles

7. Least common mechanism: **Minimize the amount of mechanism common** to more than one user and depended on by all users.
8. Psychological acceptability: It is essential that the human interface be designed for ease of use, so that **users** routinely and automatically **apply the protection mechanisms** correctly.

8+2 design principles

9. Work factor: Compare the **cost of circumventing the mechanism** with the resources of a potential attacker.

– **Application** of design principle: increase costs to find and exploit software vulnerabilities (costs = training, skills, tools, computation, hardware)

– **But**: might not hold in software security owing to *automation*

8+2 design principles

9. Work factor: Compare the **cost of circumventing the mechanism** with the resources of a potential attacker.
10. Compromise recording: In computer systems, mechanisms that **reliably record** that a compromise has occurred are used rarely, since it is difficult to guarantee discovery once security is broken.

– **Application** of design principle: enable logging and (automatically) analyse logs to detect attacks

Security architecture

- Architectural principles also found elsewhere
- Common Criteria, EAL2-EAL7
  ADV_ARC security architecture description (excerpt)
  - Security features **cannot be bypassed**.
  - Protection by TOE itself from **tampering by untrusted** active entities.
  - Description of **security domains** maintained by the TSF (TOE security functions) consistent with the SFRs (security functional requirements).
  - Secure TSF **initialisation** process.
  - ➔ Complete mediation, least privilege, separation of privilege, fail-safe defaults

Summary

- 8+2 design principles: Saltzer/Schroeder