Principles of Secure System Design

- [Saltzer and Shroeder 1975]

Principles of

- Economy of mechanism (simplicity => assurance)
- Fail-safe defaults (default deny)
- Complete mediation (look out for ways in which an access control mechanism may be bypassed)
- Open design (no security by obscurity)
- Separation of privilege (similar to separation of duty)
- Least privilege
- Least common mechanism (avoid unnecessary sharing)
- Psychological acceptability (onerous security requirements will be actively subverted by users)
Principles of Secure System Design

- Two principles mentioned, but not recommended in [Saltzer and Shroeder 1975]
  - Work factor: how much effort will it take to break a mechanisms, versus potential gain for the attacker
    - Difficult to estimate cost
    - Sometimes, difficult to estimate gain
  - Compromise recording (maintain adequate audit trail)
    - Difficult to ensure integrity of audit records maintained on a protected system
      - These records can be compromised if stored on protected system
      - Can work if audit trail can be protected, e.g., off-site storage, tamper-proof storage systems