

March 1, 2019 Outline

Reading: *text*, §17.6.2, 14, 18.1

Assignments: Homework 4, due March 8, 2019

1. Examples
 - a. Firewalls
2. Principles of secure design
 - a. Principle of least privilege
 - b. Principle of fail-safe defaults
 - c. Principle of economy of mechanism
 - d. Principle of complete mediation
 - e. Principle of open design
 - f. Principle of separation of privilege
 - g. Principle of least common mechanism
 - h. Principle of least astonishment
3. Confinement problem
 - a. What it is
 - b. Covert channels
 - c. Rule of transitive confinement
 - d. Difficulty of preventing leaking
4. Isolation: virtual machines
 - a. What it is