

Outline for September 26, 2025

Reading: *text*, §14, 20.1.2.2, 4.1

Due: Homework 1, due October 8; Project selection, due Oct 10

1. Class overview
2. Principles of secure design
 - (a) Bases: simplicity, restrictiveness
 - (b) Principle of least privilege
 - i. Principle of least authority
 - (c) Principle of fail-safe defaults
 - (d) Principle of economy of mechanism
 - (e) Principle of complete mediation
 - (f) Principle of open design
 - (g) Principle of separation of privilege
 - (h) Principle of least common mechanism
 - (i) Principle of least astonishment
 - i. Principle of psychological acceptability
3. Reference monitor
 - (a) Entities, subjects, and objects
 - (b) What a reference monitor, reference validation mechanism are
 - (c) Relationship to policy
4. Policy
 - (a) Sets of authorized, unauthorized states