

Outline for September 24, 2021

Reading: *text*, §14, 4.1–4.2

Assignments: Homework 1, due October 6; Project selection, due Oct 8

1. 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
2. Policy
 - (a) Sets of authorized, unauthorized states
 - (b) Secure systems in terms of states