March 9, 2023 Outline

Reading: *text*, §18.3.3, 14, 31.1–31.4 **Assignments:** Homework #4, due March 14

1. Mitigating covert channels
   (a) Preallocation and hold until process terminates
   (b) Impose uniformity
   (c) Randomize resource allocation
   (d) Efficiency/performance vs. security
2. Principles of secure design
   (a) Principle of least privilege
      i. 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
      i. Principle of psychological acceptability
3. Program security
   (a) The program
   (b) Requirements analysis
   (c) Design
   (d) First level refinement
   (e) Second level refinement
   (f) Error handling