May 19, 2017 Outline

Reading: *Chapters from revised text*, §14, 18.1–18.2.2.1

Due: Homework #3, May 19
Final project, June 7

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. Isolation: non-virtual machines
   a. Library operating systems
   b. Sandboxes
   c. Program rewriting