

Lecture 6 Outline

October 3, 2016

Reading: *text*, §14, 29

Assignments: Homework 1, due Oct. 5; Lab 1, due Oct. 3

1. Greetings and felicitations!
2. Puzzle of the Day
3. 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
4. Program security: example
 - a. Requirements and policy
 - b. Design
 - c. Refinement and implementation
 - d. Testing, maintenance, and operation
 - e. Distribution