

Lecture 2: March 31, 2021

Reading: *text*, §14; *Robust Programming* handout

Assignments: Homework 1, due April 7, 2021

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. Principles of robust programming
 - (a) Maximum stupidity
 - (b) Paranoia
 - (c) Dangerous implements
 - (d) Can't happen