Lecture 2 Outline (April 1, 2015)

Reading: *text*, §13, 18; [Bel07, Mei06, VE06]

---

1. Assurance
   a. Trustworthy entities
   b. Security assurance
   c. Trusted system
   d. Why assurance is needed
   e. Requirements
   f. Assurance and the software life cycle
2. 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