Outline for May 22, 2013

Reading: §18, 19 **Assignments due:** Homework #4, due May 24, 2013

1. Assurance
   a. Assurance and software life cycle
2. Basics
   a. Threats
   b. Reference monitor, validation mechanism
   c. Design security in or layer it on?
3. Policy and requirements
   a. Security specifications
   b. Problems with precision
   c. Example: System X and Bell-LaPadula
   d. Justifying requirements
4. Techniques to support design assurance
   a. Subsystem, subcomponent, module
5. Design documents
   a. Security functions summary specification
   b. External functional specification
   c. Internal design description
6. Justifying design meets requirements