Lecture 18 Outline

Reading: *text*, §19, 23.1-23.2

1. Justifying design meets requirements
   a. Reviews
2. Implementation assurance
   a. Programming language
   b. Modularity
   c. Security features (bounds checking, strong typing, etc.)
   d. Implementation management such as configuration management
3. Security testing
   a. Functional testing (black box testing)
   b. Structural testing (white box testing)
4. Penetration Studies
   a. Why? Why not direct analysis?
   b. Effectiveness
   c. Interpretation
5. Flaw Hypothesis Methodology
   a. System analysis
   b. Hypothesis generation
   c. Hypothesis testing
   d. Generalization