Lecture 17 Outline

Reading: *text*, §19

1. Techniques to support design assurance
   a. Subsystem, subcomponent, module
2. Design documents
   a. Security functions summary specification
   b. External functional specification
   c. Internal design description
3. Justifying design meets requirements
   a. Formal methods