Outline for May 27, 2003

1. Reference monitor
   a. Concept
   b. Reference validation mechanism
   c. Security kernel
   d. Trusted computing base
2. Example of add-on vs. built-in: AT&T UNIX systems with MLS
3. Policy specification
   a. What it is
   b. Using a standard
   c. Creating new policy
   d. Mapping into existing policy model
   e. Example: System X
4. Justifying requirements
5. Techniques to support design assurance
   a. Subsystem, subcomponent, module
6. Design documents
   a. Security functions summary specification
   b. External functional specification
   c. Internal design description
7. Justifying design meets requirements
   a. Formal methods
   b. Review
8. Implementation assurance
   a. Programming language
   b. Modularity
   c. Security features (bounds checking, strong typing, *etc*.)
   d. Implementation management such as configuration management
9. Security testing
   a. Functional testing (black box testing)
   b. Structural testing (white box testing)