Outline for March 29, 2006

Reading: *text*, §1, 13

1. Greetings and felicitations!
   a. Review class information handouts
2. Sketch of class
   a. Begin with overview
   b. Limits of security: what we can do–and can't do
   c. Policy models done formally
   d. Policy model composition
   e. Information flow models
   f. Theory of malicious logic
3. Policy and mechanism
4. Trust and assumptions
5. Assurance
   a. Requirements and threat analysis
   b. Specification
   c. Design
   d. Implementation
   e. Deployment, maintenance, operation, retirement
   f. Underlying assumptions
6. Stuff you won't hear again
   a. Legal, custom constraints
   b. Organizational problems
   c. People problems
7. Principles of secure design
   a. Basis: simplicity and restriction
   b. Principle of least privilege
   c. Principle of fail-safe defaults
   d. Principle of economy of mechanism
   e. Principle of complete mediation
   f. Principle of open design
   g. Principle of separation of privilege
   h. Principle of least common mechanism
   i. Principle of psychological acceptability