Outline for October 9, 2006

Reading: §13; §23.1–23.2

1. Greetings and felicitations!
   a. Puzzle of the day
2. Principles of Secure Design
   a. Principle of Complete Mediation
   b. Principle of Open Design
   c. Principle of Separation of Privilege
   d. Principle of Least Common Mechanism
   e. Principle of Psychological Acceptability
3. Penetration Studies
   a. Why? Why not direct analysis?
   b. Effectiveness
   c. Interpretation
4. Flaw Hypothesis Methodology
   a. System analysis
   b. Hypothesis generation
   c. Hypothesis testing
   d. Generalization