Notes for January 7, 1998

1. Greetings and Felicitations
   a. Go through handouts
   b. **Reading**: Pfleeger, pp. 1–18, 286–287, 467–471, 494–517; Garfinkel & Spafford, pp. 23–45, 779–798
2. Puzzle of the day
   a. Key point: policy vs. mechanism, with a sidebar on intent
3. How do you design a security policy? [Pfleeger, pp. 1–18]
   a. Risk analysis
   b. Analysis of other factors:
   c. Procedures
4. Risk analysis [Pfleeger, pp. 467–471; Garfinkel & Spafford, pp. 23–45]
   a. What are the threats?
   b. How likely are they to arise?
   c. How can they best be dealt with?
5. Analysis of other factors [Pfleeger, pp. 494–517; Garfinkel & Spafford, pp. 779–798]]
   a. What else affects the policy (federal or state law, needs, etc.)?
   b. Law: as above; discuss jurisdiction (federal or local), problems (illiteracy of authorities, etc.); chain of evidence
   c. Discuss cryptographic software controls (here, France, etc.)
6. Procedures
   a. What procedures need to be put in place, and how will they affect security?
7. Human Factors
   a. Principle of Psychological Acceptability (note: illegal violates this)
   b. Principle of common sense (it's not common; more when we discuss robust programming)
8. Design Principles [Pfleeger, pp. 286–287]
   a. Principle of Psychological Acceptability
   b. Principle of Least Privilege
   c. Principle of Fail-Safe Defaults
   d. Principle of Economy of Mechanism (KISS principle, redone)

[*ended here*]

   e. Principle of Complete Mediation
   f. Principle of Separation of Privilege
   g. Principle of Least Common Mechanism
   h. Principle of Open Design