# Notes for October 5, 1998

1. Greetings and Felicitations!
   a. Web site up; some errors in General Information (John Hughes' mailing address) are fixed there
   b. John's hours: M1-3, Tu 3-4; mine, MWF 11-12. Ask if anyone can't make these.
   c. No class Wednesday, but discussion section then. (My office hrs cancelled then!)
   d. No office hours today; interviewing prospective admin assistant for the lab
2. The telnetd is the same size as the Bourne shell. So, it may have been replaced by the Bourne shell …
3. How do you design a security policy?
   a. Risk analysis
   b. Analysis of other factors:
   c. Procedures
4. Risk analysis
   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
   a. What else affects the policy (federal or state law, needs, *etc*.)?
   b. Law: as above; discuss jurisdiction (federal or local), problems (authorities' lack of knowledge about computers, *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
   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)
   e. Principle of Complete Mediation
   f. Principle of Separation of Privilege
   g. Principle of Least Common Mechanism
   h. Principle of Open Design