# Notes for October 2, 1998

1. Greetings and Felicitations!
   a. Go through handouts, class rules
   b. Will require adding some vulnerabilities to the DOVES database as part of the course
   c. May perform a penetration exercise on an as-yet-undetermined system
2. Puzzle of the day
   a. Not appropriate; invasion of systems akin to invading a home or business; Times will ignore protesters as "irresponsible" or may attack symptom (try to find, prosecute attackers) or even find just one security problem rather than secure the site
   b. Idea here is to force Times to deal with problem of bad reporting (as attackers see it); this won't do it. Better would be to publicize stories written by the reporter with a line-by-line critique, and be sure all the Times' competitors get them (in other words, let the reporter's incompetence speak for itself, and in effect ask why a respectable newspaper would employ a reporter who can't get facts straight)
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