Notes for September 28, 2000

1. Greetings and Felicitations!
   a. Go through handouts, class rules
2. Puzzle of the day
3. Overview of goals of computer security
   a. Security services
   b. Security and the software life cycle
   c. Roles of trust and assurance
4. How do you design a security policy?
   a. Risk analysis
   b. Analysis of other factors:
   c. Procedures
5. Risk analysis
   a. What are the threats?
   b. How likely are they to arise?
   c. How can they best be dealt with?
6. 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*.)
7. Procedures
   a. What procedures need to be put in place, and how will they affect security?
8. 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)
9. Role of trust
   a. What is trust?
   b. Who cares?

Puzzle of the Day

A hypothetical computer science department provides a Hypothetical Computer Science Instructional Facility. Students do their homework on the HCSIF computers. Suppose a student in a beginning programming class writes a program but fails to use the protection mechanisms to prevent others from reading it. A second student reads the first student's program.

1. If the security policy of the HCSIF says that students are not allowed to read homework-related files from other students, has the second student violated security? Has the first?
2. If the first student had used the protection mechanisms to prevent other students from reading the file, but the second student figured out a way to read the file, would your answer to part 1 change? If so, how?
3. If the first student told the second student to "feel free to look at my answer, just don't copy it," would your answer to part 1 change? If so, how?