Notes for January 8, 1997

1. Hello
   a. Correction: section is on F3:10-4:00PM (not W) and there is no meeting this week
2. Puzzle of the day
   a. Break into groups to discuss it for 5m or so, then present ideas
   b. Key points: attacker is toast, under the EPCA so are the sysadmins; if users are told that using their account means they waive their right to privacy, it's okay
3. Amplifcation
   a. Company reported to have 1-800 modems, no root password
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 (illiteracy of authorities, 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 keeping dangerous tools out of untrained hands
9. 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