Outline for January 23, 2006

Reading: text, §13, 23

1. Greetings and felicitations!
   a. Puzzle of the day
2. Common Implementation Vulnerabilities
   a. Not resetting privileges (Purdue Games incident)
3. Principles of Secure Design
   a. Principle of Least Privilege
   b. Principle of Fail-Safe Defaults
   c. Principle of Economy of Mechanism
   d. Principle of Complete Mediation
   e. Principle of Open Design
   f. Principle of Separation of Privilege
   g. Principle of Least Common Mechanism
   h. Principle of Psychological Acceptability
4. Penetration Studies
   a. Why? Why not direct analysis?
   b. Effectiveness
   c. Interpretation
5. Flaw Hypothesis Methodology
   a. System analysis
   b. Hypothesis generation
   c. Hypothesis testing
   d. Generalization
6. System Analysis
   a. Learn everything you can about the system
   b. Learn everything you can about operational procedures
   c. Compare to other systems
7. Hypothesis Generation
   a. Study the system, look for inconsistencies in interfaces
   b. Compare to other systems' flaws
   c. Compare to vulnerabilities models
8. Hypothesis testing
   a. Look at system code, see if it would work (live experiment may be unneeded)
   b. If live experiment needed, observe usual protocols
9. Generalization
   a. See if other programs, interfaces, or subjects/objects suffer from the same problem
   b. See if this suggests a more generic type of flaw