Lecture 7 Outline

Reading: *text*, §23.1–2; [4] **Assignments due:** Homework #1, due April 13, 2001 at 11:55pm

Discussion Problem. You discover a security flaw in the operating system on your companys computer. The flaw enables any user to read any other users files, regardless of their protection. You have several choices: you can keep quiet and hope no-one else discovers the flaw, or tell the company, or tell the system vendor, or announce it on the Internet.

a. Suppose an exploitation of the vulnerability could be prevented by proper system configuration. Which of the above courses of action would you take, and why?
b. If an exploitation of the vulnerability could be detected (but not prevented) by system administrators, how would this change your answer to the first question?
c. Now suppose no exploitation of the vulnerability can be detected or prevented. Would this change your answer, and if so, how?

1. 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 least astonishment
2. Penetration Studies
   a. Why? Why not direct analysis?
   b. Effectiveness
   c. Interpretation
3. Flaw Hypothesis Methodology
   a. System analysis
   b. Hypothesis generation
   c. Hypothesis testing
   d. Generalization
4. System Analysis
   a. Learn everything you can about the system
   b. Learn everything you can about operational procedures
   c. Compare to other systems
5. Hypothesis Generation
   a. Study the system, look for inconsistencies in interfaces
   b. Compare to other systems' flaws
   c. Compare to vulnerabilities models