Outline for November 19, 2003

Reading: Chapter 18

Discussion Problem

You discover a security flaw in the operating system on your company's computer. The flaw enables any user to read any other user's 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.

1. Suppose an exploitation of t he vulnerability could be prevented by proper system configuration. Which of the above courses of action would you take, and why?
2. If an exploitation of the vulnerability could be detected (but not prevented) by system administrators, how would this change your answer to question 1?
3. Now suppose no exploitation of the vulnerability can be detected or prevented. Would this change your answer, and if so, how?

Outline for the Day

1. Assurance
   a. Trustworthy entities
   b. Security assurance
   c. Trusted system
   d. Why assurance is needed
   e. Requirements
   f. Assurance and software life cycle
2. Building trusted systems
   a. Stage 1: conception
   b. Stage 2: manufacture
   c. Deployment
   d. Maintenance