Outline for January 31, 2008

Reading: text, §23.2, 2.1–2.3, 3.1–3.2

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 the 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 the first question?
3. Now suppose no exploitation of the vulnerability can be detected or prevented. Would this change your answer, and if so, how?

Lecture Outline

1. 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
2. Elimination
3. Examples
   a. Burroughs system
   b. Corporate site
4. Access Control Matrix
   a. Subjects, objects, and rights
   b. Primitive commands: create subject/object, enter right, delete right, destroy subject/object
   c. Commands and conditions: create-file, various flavors of grant-right to show conditions and nested commands
   d. Copy flag
   a. Attenuation of privileges
5. HRU Result
   a. Notion of leakage in terms of ACM
   b. Determining security of a generic system with generic rights and mono-operational commands is decidable
   c. Determining security of a generic system with generic rights is undecidable
   d. Meaning: can't derive a generic algorithm; must look at (sets of) individual case