Lecture 10, April 22

Reading: §2; 3.1–3.2 **Assignments due:** Homework #2, due April 26, 2013 at 11:55pm

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. 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
   e. Attenuation of privileges
2. 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
3. Policy
   a. Sets of authorized, unauthorized states
   b. Secure systems in terms of states
   c. Mechanism vs. policy
4. Types of Policies
   a. Military/government vs. confidentiality
   b. Commercial vs. integrity
5. Types of Access Control
   a. Mandatory access control
   b. Discretionary access control
   c. Originator-controlled access control