Outline for January 22, 2008

Reading: text, §4.1–4.6; [Wa70], pp. 1–25

Announcement: I am holding additional office hours this week, today from 12:15PM to 1:15PM and Wednesday from 12:00 noon to 1:00PM.

Discussion Problem. A hypothetical computer science department provides a Hypothetical Computer Science Instructional Facility. Students do their homework on the HCSIF computers. Suppose a student in a beginning programming class writes a program but fails to use the protection mechanisms to prevent others from reading it. A second student reads the first student's program.

1. If the security policy of the HCSIF says that students are not allowed to read homework-related files from other students, has the second student violated security? Has the first?
2. If the first student had used the protection mechanisms to prevent other students from reading the file, but the second student figured out a way to read the file, would your answer to part 1 change? If so, how?
3. If the first student told the second student to "feel free to look at my answer, just don't copy it," would your answer to part 1 change? If so, how?

Lecture Outline

1. "Security through Obscurity"
2. Example of a policy: UC Davis e-mail policy
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
6. High-Level Policy Languages
    a. Characterization
    b. Example: DTEL
7. Low-Level Policy Languages
    a. Characterization
    b. Example: Tripwire configuration file