Lecture 13 Outline

Reading: *text*, §4.5, 5.1–5.2.1   **Assignments due:** Homework #2, due April 27, 2011 at 11:55pm
                                                        Midterm on May 2, 2011 *in class*

Discussion Problem. What do you think of the following homework assignment?
Important note: This is *not* an assignment for this class. I am *only* asking what you think of it. The assignment is reported on the web at `http://isc.sans.org/diary.php?storyid=1155`.

> **The Task**
>
> Student is to perform a remote security evaluation of one or more computer systems. The evaluation should be conducted over the Internet, using tools available in the public domain.
>
> **What the student must submit**
>
> In conducting this work, you should imagine yourself to be a security contracted by the owner of the computer system(s) to perform a security evaluation.
>
> The student must provide a written report which has the following sections: Executive summary, description of tools and techniques used, dates and times of investigations, examples of data collected, evaluation data, overall evaluation of the system(s) including vulnerabilities.

1. Greetings and felicitations!
   a. Midterm will be on *Monday*, *May 2*, in class
   b. I will post a sample midterm on Tuesday of this week
2. High-level policy languages
   a. Characterization
   b. Example: DTEL
3. Low-level policy languages
   a. Characterization
   b. Example: *tripwire* configuration file
4. Goals of confidentiality policies
5. Bell-LaPadula Model with levels only
   a. Security levels
   b. Simple security property
   c. *-property
   d. Discretionary security property
6. Full Bell-LaPadula Model
   a. Add in compartments
   b. *dom* relation
   c. Simple security property
   d. *-Property
   e. Discretionary security property