Outline for January 24, 2002

Reading: §19.2, §2.1–2.2, §4.1–4.5

1. Greetings and Felicitations!
2. Puzzle of the day
3. Peeling the Onion
   a. You know very little (not even phone numbers or IP addresses)
   b. You know the phone number/IP address of system, but nothing else
   c. You have an unprivileged (guest) account on the system.
   d. You have an account with limited privileges.
4. Example Penetration Studies
   a. Michigan Terminal System
   b. Burroughs System
   c. Attacking the Organization Directly
5. Access Control Matrix
   a. Subjects, objects, and rights
6. HRU Result
   a. Notion of leakage in terms of ACM
   b. Determining security of a generic system with generic rights is undecidable
   c. Meaning: can't derive a generic algorithm; must look at (sets of) individual cases
7. Policy
   a. Sets of authorized, unauthorized states
   b. Secure systems in terms of states
   c. Mechanism vs. policy
8. Types of Policies
   a. Military/government vs. confidentiality
   b. Commercial vs. integrity
9. Types of Access Control
   a. Mandatory access control
   b. Discretionary access control
   c. Originator-controlled access control
10. High-Level Policy Languages
    a. Characterization
    b. Example: DTEL
11. Low-Level Policy Languages
    a. Characterization
    b. Example: Tripwire configuration file