Outline for March 8, 2002

Reading: §13, §14, §15.1–15.4

1. Greetings and Felicitations
2. Puzzle of the day
3. Identity
   a. Principal and identity
   b. Users, groups, roles
   c. Identity on the web
   d. Host identity: static and dynamic identifiers
   e. State and cookies
   f. Anonymous remailers: type 1 and type 2 (mixmaster)
4. Principles of Secure Design
   a. Least Privilege
   b. Fail-Safe Defaults
   c. Economy of Mechanism
   d. Complete Mediation
   e. Open Design
   f. Separation of Privilege
   g. Least Common Mechanism
   h. Psychological Acceptability
5. Privilege in Languages
   a. Nesting program units
   b. Temporary upgrading of privileges
6. Access Control Lists
   a. UNIX method
   b. ACLs: describe, revocation issue
7. MULTICS ring mechanism
   a. MULTICS rings: used for both data and procedures; rights are REWA
   b. (b_1, b_2) access bracket - can access freely; (b_3, b_4) call bracket - can call segment through gate; so if a's access bracket is (32,35) and its call bracket is (36,39), then *assuming permission mode (REWA) allows access*, a procedure in:
      rings 0-31: can access a, but ring-crossing fault occurs
      rings 32-35: can access a, no ring-crossing fault
      rings 36-39: can access a, provided a valid gate is used as an entry point
      rings 40-63: cannot access a
   c. If the procedure is accessing a data segment d, no call bracket allowed; given the above, *assuming permission mode (REWA) allows access*, a procedure in:
      rings 0-32: can access d
      rings 33-35: can access d, but cannot write to it (W or A)
      rings 36-63: cannot access d
8. Capabilities
   a. Capability-based addressing: show picture of accessing object
   b. Show process limiting access by not inheriting all parent's capabilities
   c. Revocation: use of a global descriptor table