Outline for October 14, 2014

Reading: text, §15.4–15.5, 4.1–4.4

1. Lock and Key
   a. Shamir’s secret sharing scheme

2. MULTICS ring mechanism
   a. Rings, gates, ring-crossing faults
   b. Used for both data and procedures; rights are REWA
   c. \((b_1, b_2)\) 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 \(a\)
   d. 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 \(d\)

3. PACLs
   a. Creator kept with PACL, and only creator can change it
   b. PACLs associated with both subjects, objects
   c. Subject reads object: object’s PACL associated with subject; subject creates object: subject’s PACL
      associated with object

4. Policy
   a. Sets of authorized, unauthorized states
   b. Secure systems in terms of states
   c. Mechanism vs. policy

5. Types of Policies
   a. Military/government vs. confidentiality
   b. Commercial vs. integrity

6. Types of Access Control
   a. Mandatory access control
   b. Discretionary access control
   c. Originator-controlled access control

7. High-level policy languages
   a. Characterization
   b. Example: DTEL

8. Low-level policy languages
   a. Characterization
   b. Example: tripwire configuration file

9. Policies in natural language