Lecture 27 Outline (June 1, 2015)

**Reading:** §12, 15

**Assignment:** Homework 4, due June 3, 2015 (no late assignments accepted)

1. Greetings and felicitations!
2. Challenge-response techniques
   a. One-time passwords
   b. Encrypted key exchange
   c. Hardware support
3. Biometrics
   a. Depend on physical characteristics
   b. Examples: pattern of typing (remarkably effective), retinal scans, etc.
4. Location
   a. Bind user to some location detection device (human, GPS)
   b. Authenticate by location of the device
5. Access Control Lists
   a. UNIX method
   b. ACLs: describe, revocation issue
6. Capabilities
   a. Capability-based addressing
   b. Inheritance of C-Lists
   c. Revocation: use of a global descriptor table
7. Lock and Key
   a. Types and locks
8. 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 \(d\)