Lecture 28 Outline (June 3, 2015)

Reading: §15, 22 (*not* 22.6), [Nac97] **Assignment**: Homework 4, due June 3, 2015 (*no late assignments accepted*)

1. Greeting and felicitations!
   a. Review sessions:
      i. Friday, June 5 at 1:10pm–2:00pm in 1003 Giedt Hall
      ii. Monday, June 8 at 4:10pm–5:00pm in 26 Wellman
   b. Office hours:
      i. Friday, June 5 at 3:10pm–4:00pm
      ii. Monday, June 8 at 2:10pm–3:00pm
      iii. Tuesday, June 9 at 12:10pm–1:00pm
2. Capabilities
   a. Capability-based addressing
   b. Inheritance of C-Lists
   c. Revocation: use of a global descriptor table
3. Lock and Key
   a. Types and locks
4. 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
5. Types of malicious logic
   a. Trojan horse
      i. Replicating Trojan horse
      ii. Thompson's compiler-based replicating Trojan horse
   b. Computer virus
      i. Boot sector infector
      ii. Executable infector
      iii. Multipartite
      iv. TSR (terminate and stay resident)
      v. Stealth
      vi. Encrypted
      vii. Polymorphic
      viii. Metamorphic
      ix. Macro
   c. Computer worm
   d. Bacterium, rabbit
   e. Logic bomb
   f. Others