Lecture 25, May 29

Reading: §15, 22 (*not* 22.6), [Nac97][1] **Assignments due:** Homework #5, due June 6, 2013 at 11:55pm

Discussion Problem. *The IP Commission Report: The Report of the Commission on the Theft of American Intellectual Property*, released late last week, has the following recommendation (see p. 81):

> Additionally, software can be written that will allow only authorized users to open files containing valuable information. If an unauthorized person accesses the information, a range of actions might then occur. For example, the file could be rendered inaccessible and the unauthorized user's computer could be locked down, with instructions on how to contact law enforcement to get the password needed to unlock the account. Such measures do not violate existing laws on the use of the Internet, yet they serve to blunt attacks and stabilize a cyber incident to provide both time and evidence for law enforcement to become involved.

What problems might this idea (specifically, making the file inaccessible and locking the user's computer) pose?

Lecture outline.

1. Lock and Key
   a. Types and locks
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. 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

[1] This is available in the Resources area of SmartSite; look in the folder "Handouts"