Lecture 24, May 24

Reading: §12, 15 **Assignments due:** Homework #4, due May 24, 2013 at 11:55pm

Discussion Problem. The U. S. government has proposed expanding wiretap design laws to include Internet services and software such as voice-over-IP (VoIP), instant messaging, Xbox Live, and other services.[1] What technical problems might such a wiretap "back door" create?

Lecture outline.

1. Challenge-response systems
   a. Computer issues challenge, user presents response to verify secret information known/item possessed
   b. Example operations: $f(x) = x + 1$, random, string (for users without computers), time of day, computer sends $E(x)$, you answer $E(D(E(x)) + 1)$
   c. Note: password never sent on wire or network
2. Biometrics
   a. Depend on physical characteristics
   b. Examples: pattern of typing (remarkably effective), retinal scans, etc.
3. Location
   a. Bind user to some location detection device (human, GPS)
   b. Authenticate by location of the device
4. Access Control Lists
   a. UNIX method
   b. ACLs: describe, revocation issue
5. Capabilities
   a. Capability-based addressing
   b. Inheritance of C-Lists
   c. Revocation: use of a global descriptor table
6. Lock and Key
   a. Associate with each object a lock; associate with each process that has access to object a key (it's a cross between ACLs and C-Lists)
   b. Example: use crypto (Gifford). X object enciphered with key K. Associate an opener R with X. Then:
      OR-Access: K can be recovered with any D_i in a list of n deciphering transformations, so $R = (E_1(K), E_2(K), \ldots, E_n(K))$ and any process with access to any of the D_i's can access the file
      AND-Access: need all n deciphering functions to get K: $R = E_1(E_2(\ldots E_n(K)\ldots))$
   c. Types and locks
7. 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

[1] Charlie Savage, "U.S. Weighs Wide Overhaul of Wiretap Laws," *New York Times* (May 7, 2013); available at `http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html?_r=0`.