Outline for March 5, 2003

Reading: text, §12.4–12.6, 14.1–14.4, 14.6, 15.1–15.4

Discussion Problem

The following is a passage from Sun Tsu's book *The Art of War*:

> There are three ways in which a sovereign can bring misfortune upon his army:
>
> By commanding the army to advance or retreat, being ignorant of the fact that it cannot obey. This is called hobbling the army.
>
> By attempting to govern an army in the same way as he administers a kingdom, being ignorant if the conditions that obtain in an army. This causes restlessness in the soldiers' minds. Humanity and justice are the principles on which to govern a state, but not an army; opportunism and flexibility, on the other hand, are military rather than civic virtues.
>
> By employing the officers of his army without discrimination, through ignorance of the military principle of adaptation to circumstances. This shakes the confidence of the soldiers.[1]

Does this apply to an organization with computers that are under attack, or are expected to be attacked? How?

Outline for the Day

1. Biometrics
   a. Depend on physical characteristics
   b. Examples: pattern of typing (remarkably effective), retinal scans, *etc*.
2. Location
   a. Bind user to some location detection device (human, GPS)
   b. Authenticate by location of the device
3. Combinations
   a. PAM
4. Identity
   a. Principal and identity
   b. Users, groups, roles
   c. Identity on the web
   d. Host identity: static and dynamic identifiers
   e. State and cookies
   f. Anonymous remailers: type 1 (cypherpunk) and type 2 (mixmaster)
5. Access Control Lists
   a. UNIX method
   b. ACLs: describe, revocation issue
6. Capabilities
   a. Capability-based addressing: show picture of accessing object
   b. Show process limiting access by not inheriting all parent's capabilities
   c. Revocation: use of a global descriptor table
7. Privilege in Languages
   a. Nesting program units
   b. Temporary upgrading of privileges
8. 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

---

1. Sun Tzu, *The Art of War*, Delta Publishing, New York, NY 10036 (1983) pp. 16*17*

$R = (E_1(K), E_2(K), ..., E_n(K))$ 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: $R = E_1(E_2(...E_n(K)...))$

c. Types and locks

9. MULTICS ring mechanism
   a. MULTICS rings: used for both data and procedures; rights are REWA
   b. (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*
   c. 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*