Outline for February 26, 2008

Reading: text, §12.2–12.5, 15.1–15.2

Discussion Problem. How does weapon development compare to developing computer security mechanisms?

> Weapons developers, when given a choice, always go for the complex, elaborate solution at the expense of the simple one. Complexity leads to higher costs: purchase costs, operations costs, and maintenance costs. Higher costs result in fewer weapons, which, in turn, lead to contrived tests and analyses to prove that the relatively few complex systems can overcome the larger numbers of the simpler, less expensive weapons of the enemy. The fewer the weapons, the tighter is the control of these precious assets by a centralized command structure. The elaborate paraphernalia that comes with the centralized command structure only adds to the complexity of the overall system.[1]

Lecture Outline

1. Password aging
   a. Pick age so when password is guessed, it's no longer valid
   b. Implementation: track previous passwords vs. upper, lower time bounds
2. Ultimate in aging: One-Time Password
   a. Password is valid for only one use
   b. May work from list, or new password may be generated from old by a function
3. 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
   d. Defeating dictionary attacks: encrypted key exchange protocol
4. Biometrics
   a. Depend on physical characteristics
   b. Examples: pattern of typing (remarkably effective), retinal scans, etc.
5. Location
   a. Bind user to some location detection device (human, GPS)
   b. Authenticate by location of the device
6. Access Control Lists
   a. UNIX method
   b. ACLs: describe, revocation issue
7. Capabilities
   a. Capability-based addressing

[1] J. Burton, *The Pentagon Wars*, Naval Institute Press, Annapolis, MD (1993), p. 41.