Outline for March 3, 2003

Reading: text, §12

Discussion Problem

“To fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy’s resistance without fighting. In the practical art of war, the best thing of all is to take the enemy’s country whole and intact; to shatter and destroy it is not so good. So, too, it is better to capture an army entire than to destroy it, to capture a regiment, a detachment, or a company entire than to destroy it.”

What does this paragraph say to a system administrator or security officer seeking insight to defend her systems?

Outline for the Day

1. Passwords
   a. How UNIX does selection
   b. Problem: common passwords
   c. May be pass phrases: goal is to make search space as large as possible, distribution as uniform as possible
   d. Other ways to force good password selection: random, pronounceable, computer-aided selection
   e. Go through problems, approaches to each, esp. proactive
2. Attack Schemes Directed to the Passwords
   a. Exhaustive search: UNIX is 1-8 chars, say 96 possibles; it’s about 7e16
   b. Inspired guessing: think of what people would like (see above)
   c. Random guessing: can’t defend against it; bad login messages aid it
   d. Scavenging: passwords often typed where they might be recorded (b’as login name, in other contexts, etc.)
   e. Ask the user: very common with some public access services
   f. Expected time to guess
3. 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   a. Pick age so when password is guessed, it’s no longer valid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
4. 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
   c. Example: S/Key
5. 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. Attack: monkey-in-the-middle
   e. Defense: mutual authentication
6. Biometrics
   a. Depend on physical characteristics
   b. Examples: pattern of typing (remarkably effective), retinal scans, etc.
7. Location
   a. Bind user to some location detection device (human, GPS)
   b. Authenticate by location of the device

---