Outline for March 4, 2002

Reading: §12.1–12.3

1. Greetings and Felicitations
2. Puzzle of the day
3. Authentication:
   a. validating client (user) identity
   b. validating server (system) identity
   c. validating both (mutual authentication)
4. Basis: what you know/have/are, where you are
5. Passwords
   a. How UNIX does selection
   b. Problem: common passwords; Go through Morris and Thompson ; Klein and mine, *etc*.
   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
6. Password Storage
   a. In the clear; MULTICS story
   b. Enciphers; key must be kept available; get to it and it's all over
   c. Hashed; present idea of one-way functions using identity and sum
   d. Show UNIX version
7. 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
8. 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   a. Pick age so when password is guessed, it's no longer valid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
9. 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
10. 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