Outline for March 6, 2002

Reading: §12.2.3–12.6, §14

1. Greetings and Felicitations
2. Puzzle of the day
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    a. Pick age so when password is guessed, it's no longer valid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
8. 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 and type 2 (mixmaster)