Notes for January 31, 1997

1. Hello
   a. Should have homeworks back by Monday
2. Puzzle of the day
   a. Key point: executing arbitrary programs on your system, appending to/overwriting programs
3. Ultimate in aging: One-Time Pads
   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
4. 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 (will discuss more sophisticated network-based protocols later)
5. Biometrics
   a. Depend on physical characteristics
   b. Examples: pattern of typing (remarkably effective), retinal scans, etc.
6. Location
   a. Bind user to some location detection device (human, GPS)
   b. Authenticate by location of the device
7. Notion of “privilege”
   a. Go through OS idea quickly
   b. Protection rings in Multics
   c. Nesting program units
8. Different forms of access control
   a. UNIX method
   b. ACLs: describe, revocation issue
   c. MULTICS rings: (b1, b2) access bracket - can access freely; (b2, b3) call bracket - can call segment through gate; so (4, 6, 9) as example
   d. Capabilities: file descriptors in UNIX