Notes for November 10, 1999

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   a. Pick age so when password is guessed, it's no longer valid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 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™
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 (will discuss more sophisticated network-based protocols later)
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. User identification
   a. Go through UNIX idea of "real", "effective", "saved", "audit"
   b. Go through notion of "role" accounts; cite Secure Xenix, DG, etc.
   c. Go through PPNs (TOPS-10) and groups
   d. Review least privilege
9. Notion of "privilege"
   a. Identity
   b. Functionality
   c. Granularity
10. Privilege in OSes
    a. None (original IBM OS; protect with password, or anyone can read it)
    b. Fence, base and bounds registers; relocation
    c. Tagged architectures
    d. Memory management based schemes: segmentation, paging, and paged segmentation
11. 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