Notes for November 11, 1998

1. Greetings and Felicitations!
2. Puzzle of the Day
3. Ultimate in aging: One-Time Passwords
   a. 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. Identity
   b. Functionality
   c. Granularity
8. 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
9. 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
10. Privilege in Languages
    a. Nesting program units
    b. Temporary upgrading of privileges
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
    d. Capabilities: file descriptors in UNIX