Lecture 17: May 8, 2026

Reading: *text*, §13.3.1–13.9 **Due:** Homework 3, due May 11, 2026

1. Greetings and felicitations!
2. Passwords
   (a) Ways to force good password selection: random, pronounceable, computer-aided selection
   (b) Best: use passphrases: goal is to make search space as large as possible, distribution as uniform as possible
3. Attacks
   (a) Exhaustive search
   (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 as login name, in other contexts, etc.
   (e) Ask the user: very common with some public access services
4. Defenses
   (a) For trial and error at login: dropping or back-off
   (b) For thwarting dictionary attacks: salting
5. 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   (a) Pick age so when password is guessed, it's no longer valid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
6. 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
7. 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 over network
8. Biometrics
   (a) Depend on physical characteristics
   (b) Examples: pattern of typing (remarkably effective), retinal scans, etc.
9. Location
   (a) Bind user to some location detection device (human, GPS)
   (b) Authenticate by location of the device
10. Multi-factor authentication
11. Access Control Lists
    (a) Full access control lists
    (b) Abbreviations (UNIX method)