Outline for October 29, 2025

Reading: *text*, §13.5–13.9, 18.1 **Due:** Homework 3, due November 5; Project selection, due November 7

1. Greetings and Felicitations!
2. Defenses
   (a) For trial and error at login: dropping or back-off
3. 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
4. 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 or a hardware token
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. Multi-factor authentication
8. Confinement problem
   (a) Total isolation
   (b) Isolation