Lecture 23: May 19, 2021

Reading: *text*, §13.5–13.9, 16.1

Assignments: Homework 4, due May 24
Lab 3, due May 26

1. 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   (a) Pick age so when password is guessed, it's no longer valid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
2. 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
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. Biometrics
   (a) Depend on physical characteristics
   (b) Examples: pattern of typing (remarkably effective), retinal scans, etc.
5. Location
   (a) Bind user to some location detection device (human, GPS)
   (b) Authenticate by location of the device
6. Multi-factor authentication
7. Access Control Lists
   (a) Full access control lists
   (b) Abbreviations (UNIX method)