Outline for October 23, 2023

Reading: *text*, §13, 15.1–15.5

Assignments: Homework 2, due October 23;
Background Research, due October 27

1. 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
2. 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
3. Biometrics
   (a) Depend on physical characteristics
   (b) Examples: pattern of typing (remarkably effective), retinal scans, etc.
4. Location
   (a) Bind user to some location detection device (human, GPS)
   (b) Authenticate by location of the device
5. Multi-factor authentication
6. Identity
   (a) Files, objects
   (b) Users, groups, roles
7. Certificates
   (a) X.509v4 Distinguished Names
   (b) Registration and certification authorities
   (c) Internet certification hierarchy