

Outline for October 14, 2022

Reading: *text*, §13.5–13.8, 15.1–15.5 **Assignments:** Homework 2, due October 21; Progress report, due Nov 4

1. Defenses
 - (a) For trial and error at login: dropping or back-off
 - (b) For thwarting dictionary attacks: salting
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. 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. Identity
 - (a) Files, objects
 - (b) Users, groups, roles
8. Certificates