

## Outline for October 12, 2022

**Reading:** *text*, §12.1,12.4, 13

**Assignments:** Homework 2, due October 21; Progress report, due Nov 4

---

1. Privacy-enhanced email
2. Authentication
  - (a) Validating client (user) identity
  - (b) Validating server (system) identity
  - (c) Validating both (mutual authentication)
  - (d) Basis: what you know/have/are, where you are
3. Passwords
  - (a) Problem: common passwords, easy to guess passwords
  - (b) Best: use passphrases: goal is to make search space as large as possible, distribution as uniform as possible
4. Attacks
  - (a) Exhaustive search
  - (b) Guessing
  - (c) Scavenging: passwords often typed where they might be recorded as login name, in other contexts, etc.
  - (d) Ask the user: very common with some public access services
5. Defenses
  - (a) For trial and error at login: dropping or back-off
  - (b) For thwarting dictionary attacks: salting
6. 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
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