Lecture 22: May 17, 2021

Reading: *text*, §12.5.3, 13 **Assignments:** Homework 4, due May 24

1. Problems with SSL
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
   (b) Ways to force good password selection: random, pronounceable, computer-aided selection
   (c) Best: use passphrases: goal is to make search space as large as possible, distribution as uniform as possible
4. Attacks
   (a) Exhaustive search
   (b) Inspired guessing: think of what people would like (see above)
   (c) Random guessing: can't defend against it; bad login messages aid it
   (d) Scavenging: passwords often typed where they might be recorded as login name, in other contexts, etc.
   (e) 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