Lecture 18: November 4, 2019

Reading: *text*, §12.5.3, 13

Assignments: Lab 2, due November 6, 2019
Homework 3, due November 8, 2019

1. Greetings and felicitations!
   (a) Midterms should be back by Friday at the latest
2. Puzzle of the Day
3. TLS and SSL
   (a) Upper layer
      i. TLS handshake protocol
      ii. TLS change cipher spec protocol
      iii. TLS alert protocol
      iv. TLS heartbeat extension
      v. TLS application protocol
   (b) TLS vs. SSLv3
4. 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
5. 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
6. 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
7. Defenses
   (a) For trial and error at login: dropping or back-off
   (b) For thwarting dictionary attacks: salting
8. 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   (a) Pick age so when password is guessed, it's no longer valid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
9. 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
10. 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

11. Biometrics
    (a) Depend on physical characteristics
    (b) Examples: pattern of typing (remarkably effective), retinal scans, etc.
12. Location
    (a) Bind user to some location detection device (human, GPS)
    (b) Authenticate by location of the device