Outline for October 16, 2024

Reading: *text*, §12.4, 13 **Due:** Homework 2, due October 23; Project progress report, due November 1

1. Fast Exponentiation
2. Privacy-enhanced email
3. 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
4. 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
5. 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
6. Defenses
   (a) For trial and error at login: dropping or back-off
   (b) For thwarting dictionary attacks: salting
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. 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
9. Biometrics
   (a) Depend on physical characteristics
   (b) Examples: pattern of typing (remarkably effective), retinal scans, etc.
10. Location
    (a) Bind user to some location detection device (human, GPS)
    (b) Authenticate by location of the device
11. Multi-factor authentication