Outline for November 25, 2014

Reading: *text*, §12, 16, 32

1. Passwords
   a. Problem: common passwords
   b. May be pass phrases: goal is to make search space as large as possible, distribution as uniform as possible
   c. Other ways to force good password selection: random, pronounceable, computer-aided selection
2. Password Storage
   a. In the clear; Multics story
   b. Enciphered; key must be kept available
   c. Hashed; show UNIX versions, including salt
3. Attacks
   a. Exhaustive search: password is 1 to 8 chars, say 96 possibles; it's about 7×10^{16}
   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
4. 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   a. Pick age so when password is guessed, it's no longer valid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
5. 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
6. 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 on wire or network
7. Biometrics
   a. Depend on physical characteristics
   b. Examples: pattern of typing (remarkably effective), retinal scans, etc.
8. Location
   a. Bind user to some location detection device (human, GPS)
   b. Authenticate by location of the device
9. Information flow
   a. Information flow policy, confidentiality policy, integrity policy
   b. Example
10. Entropy
    a. Random variables
    b. Joint probability
    c. Conditional probability
    d. Entropy (or uncertainty in bits)
    e. Joint entropy
    f. Conditional entropy
11. Entropy-based analysis
    a. Flow of information from x to y
    b. Implicit flow of information