Lecture 9: Authentication

Date: October 16, 2013 ***Homework Due***: Oct. 18 at 5:00pm

1. Attributes that identify you
   a. What you know
   b. What you have
   c. What you are
   d. Where you are
2. Passwords
   a. How to pick them (and what to look out for)
      i. Problem: common passwords
      ii. Complex passwords
      iii. Pass-phrases
   b. How they are stored
      i. In the clear (readable only by *root* or the authentication system
      ii. Enciphered (key must be available)
      iii. Cryptographically hashed; also, salted
   c. How long they are good for (password aging)
      i. Tracking previous passwords vs. expire after *n* days
      ii. One-time passwords (use once only)
   d. How people try to get your password
      i. Exhaustive search: password is 1 to 8 chars, say 96 possible chars; it's about 7×10^{15} guesses
      ii. Inspired guessing: think of what people would like (see above)
      iii. Random guessing: can't defend against it; bad login messages aid it
      iv. Scavenging: passwords often typed where they might be recorded as login name, in other contexts, etc.
      v. Ask the user: very common with some public access services
3. Challenge-response
   a. Computer issues challenge, user presents response to verify secret information known or item possessed
   b. Example operations: $f(x) = x + 1$, x random; string (for users without computers); something based on time of day; computer sends $E(x)$, you answer $E(D(E(x)) + 1)$
   c. Note: password never sent on wire or network
4. Biometrics
   a. Depend on physical characteristics
   b. Examples: pattern of typing (remarkably effective), retinal scans, etc.
5. Location
   a. Bind user to some location detection device (human, GPS)
   b. Authenticate by location of the device
6. Multi-factor authentication