Lecture 17 Outline

May 24, 2016

Reading: *text*, §12, 13 **Assignments due:** Homework 4, on May 26

1. Greetings and felicitations!
   a. Discussion question
2. SSL
   a. How the program works
   b. Heartbleed
   c. Poodle
   d. Comparison with TLS
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   a. Pick age so when password is guessed, it's no longer valid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