Lecture 22 Outline  
May 21, 2018

Reading: §12  
Assignments: Homework 4, due on May 25, 2018 at 11:59pm  
Lab 3, due on May 23, 2018 at 11:59pm

1. Firewalls  
a. Why use them?  
b. Packet-level or filtering firewalls  
c. Application layer or proxy firewalls

2. Network organization  
a. Inside/outside  
b. Inside/DMZ/outside  
c. How email and web services (and others) are handled

3. Denial of service attacks  
a. SYN cookies  
b. Adaptive time-out

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. 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a. Pick age so when password is guessed, it’s no longer valid  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

8. 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

9. 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

10. Biometrics  
a. Depend on physical characteristics  
b. Examples: pattern of typing (remarkably effective), retinal scans, etc.

11. Location  
a. Bind user to some location detection device (human, GPS)  
b. Authenticate by location of the device