Lecture 19 Outline

May 14, 2018

Reading: §12.3, 12.4.2

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

1. Networks and ciphers
   a. Where to put the encryption
   b. Link vs. end-to-end
2. TLS and SSL
   a. Session, connection
   b. Cryptographic mechanisms
   c. Lower layer: TLS record protocol
   d. Upper layer
      i. TLS handshake protocol
      ii. TLS change cipher spec protocol
      iii. TLS alert protocol
      iv. TS heartbeat extension
      v. TLS application protocol
   e. TLS vs. SSLv3
3. Firewalls
   a. Why use them?