Messing with TCP

Transport Control Protocol

Transport Layer = communication between processes

TCP provides reliable connections

3-way handshake to establish connections

* every packet has “flags” SYN, ACK: set to 0/1

client

SYN initial seq #

Server

SYN + ACK ack seq #, init seq #

ack seq #

Ack

every packet has sequence #

IP Spoofing: send packets, masquerading as someone else

Ex: Attacker X wants to masquerade as A to B

must be on same LAN

establishes one-sided TCP connection

X can send but not receive

Projects, y'all!

Bruce Schneier

Homework

Friday meet in MLM 206
Guessing seq #’s:
older TCP implementations made it easy
bad random number generation is bad

**SYN flood attack:**

half-open connections consume resources (seq #’s, etc)
until they time out
bound on # of half-open connections
waiting in SYN-queue
when queue is full, new connections are rejected/dropped

**Countermeasure:**

1. expel oldest half-open connection from SYN-queue
2. SYN-cookies

   idea: choose init seq # cleverly!

   Init seq, # = timestamp || MAC(t || src IP)
   then forget seq # (no server resources!)
   receive an ACK from IP/port
   check MAC against t || MAC
   and t not too far in past