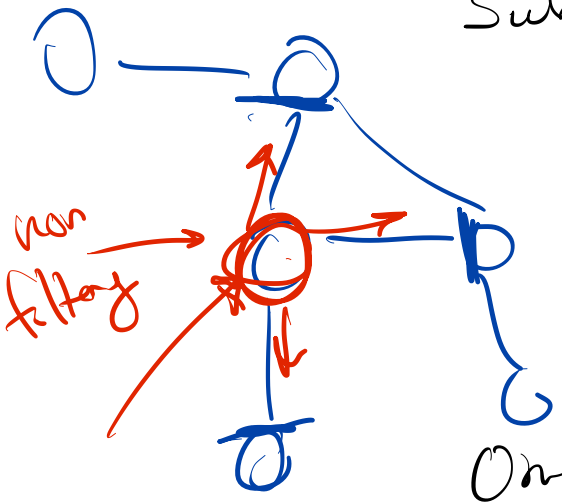
CS558 Network Security

Lecture 8: DoS and DDoS

BOSTON UNIVERSITY

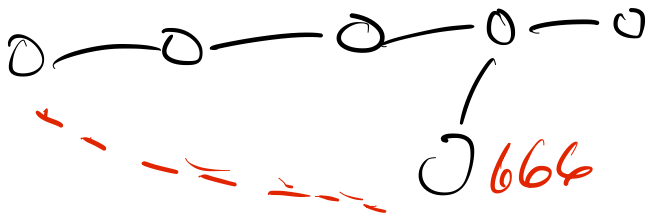
Review BGPSec:



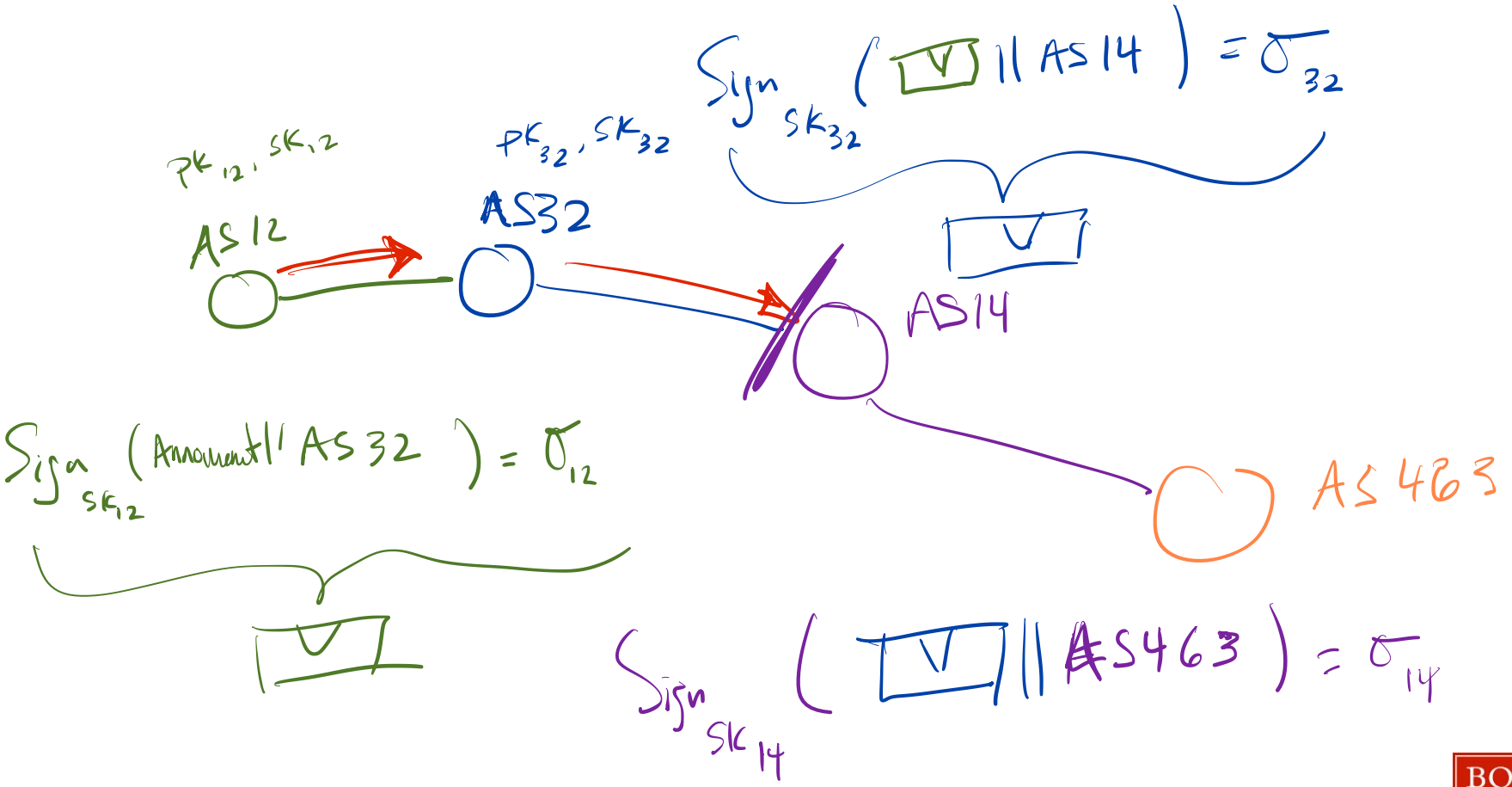
Sub prefix hijacks → announcement was more specific than actual announcement

→ RPKI + ROA
Validate announcement origin
Building a chain of keys

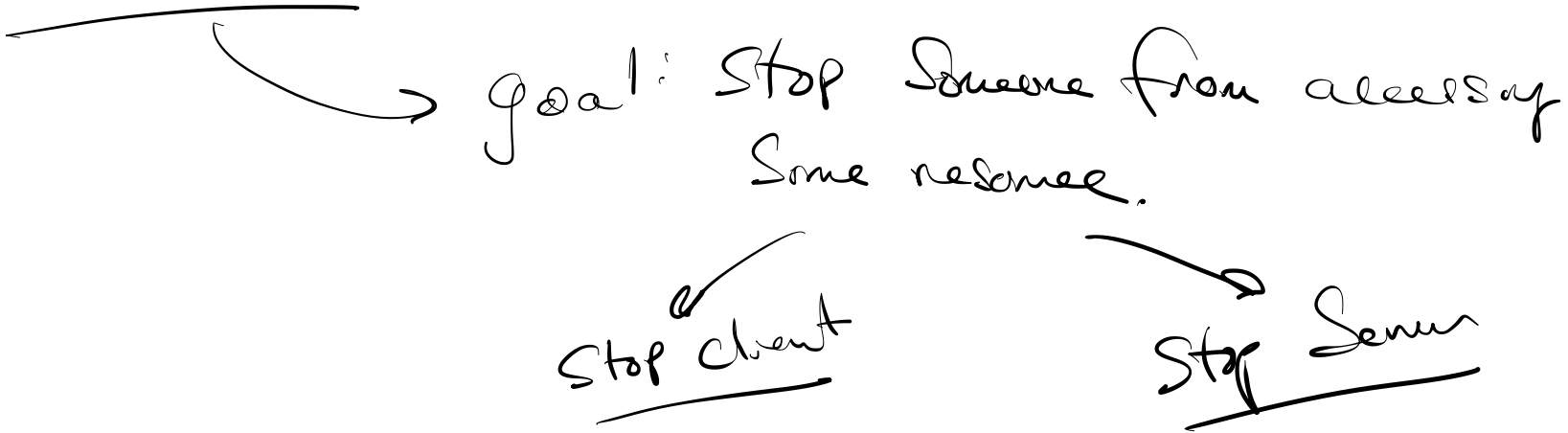
One hop attack

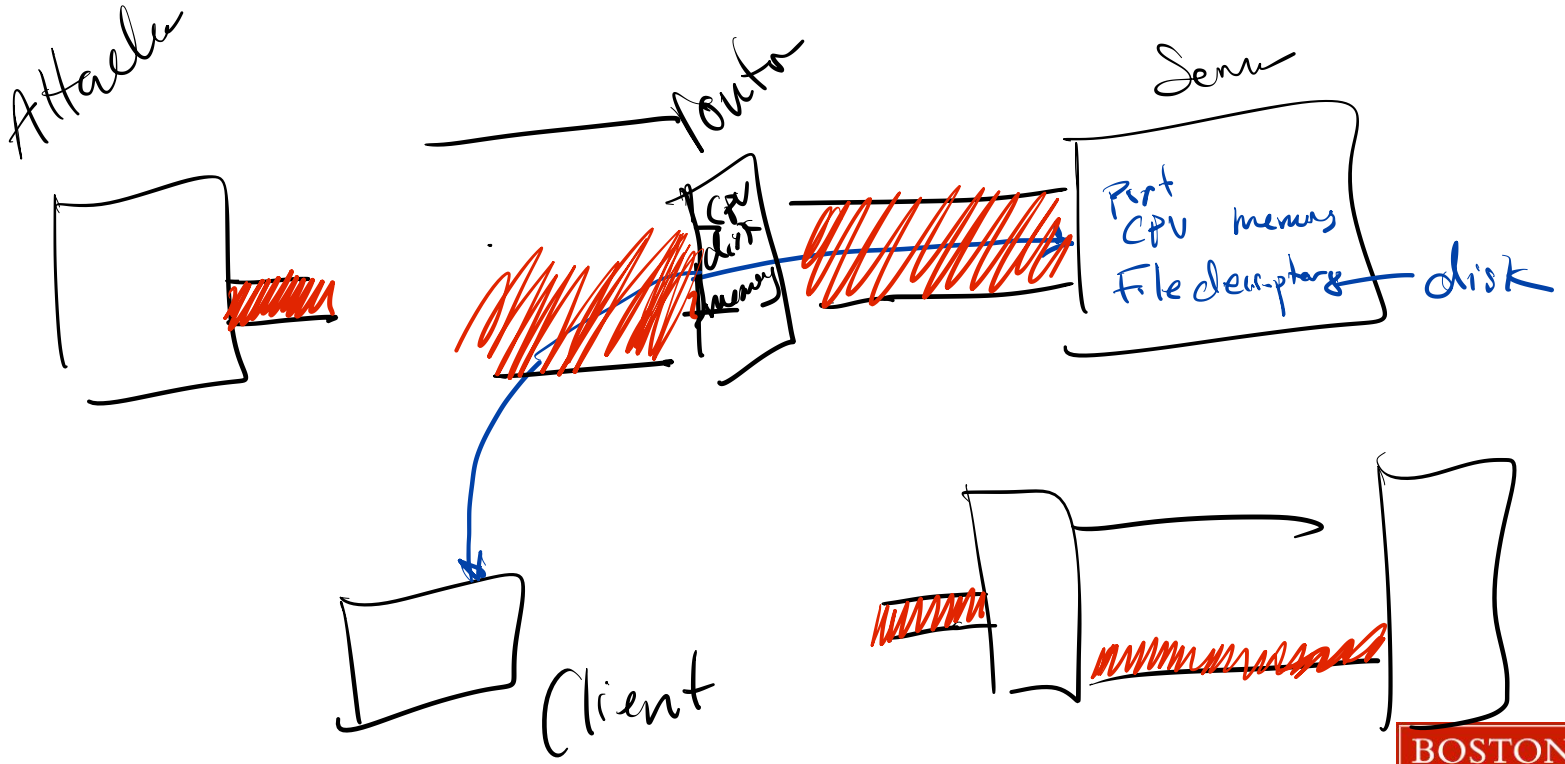


BGP Sec
authenticate the path an announcement took

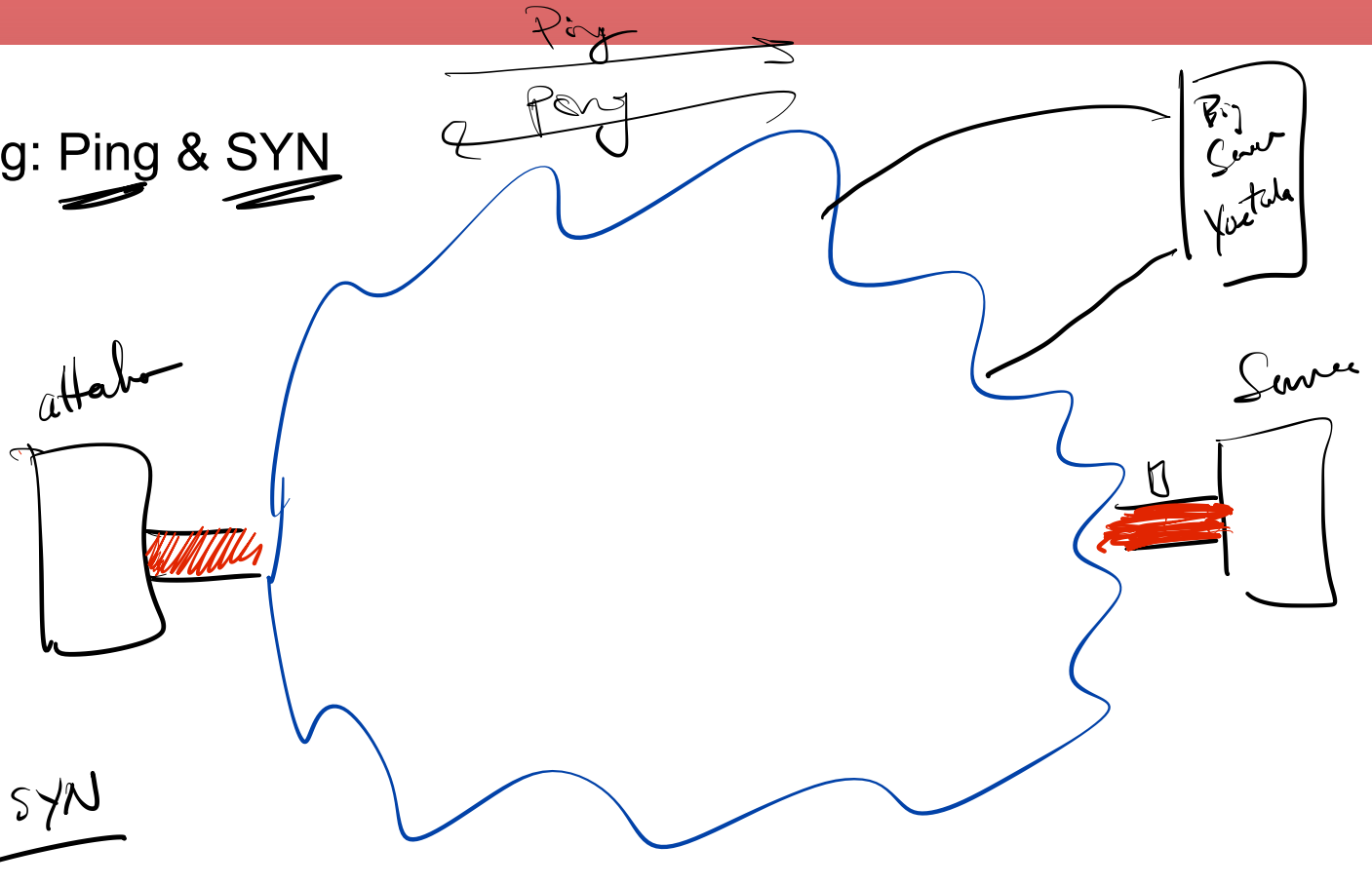


Denial of Service

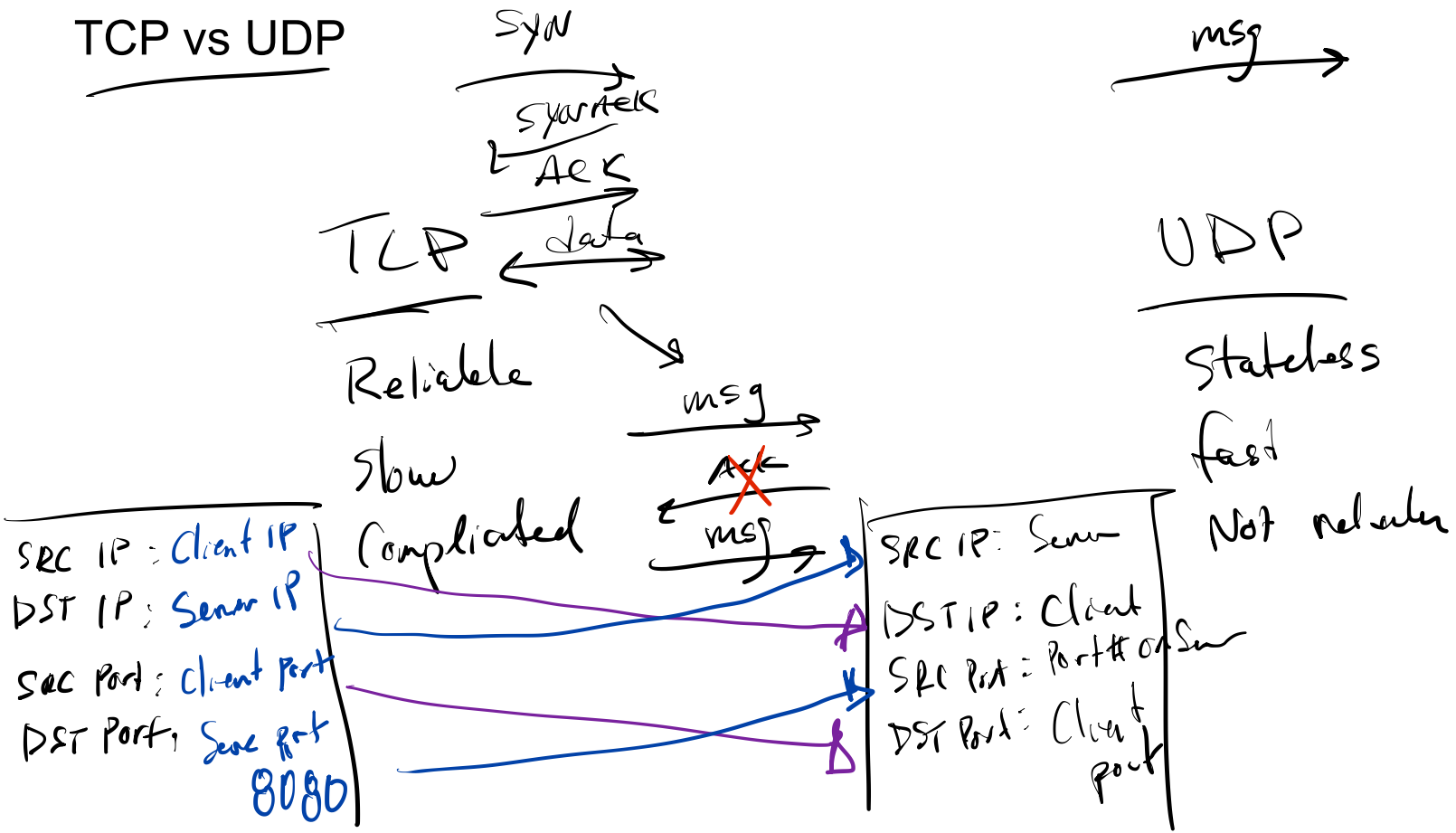




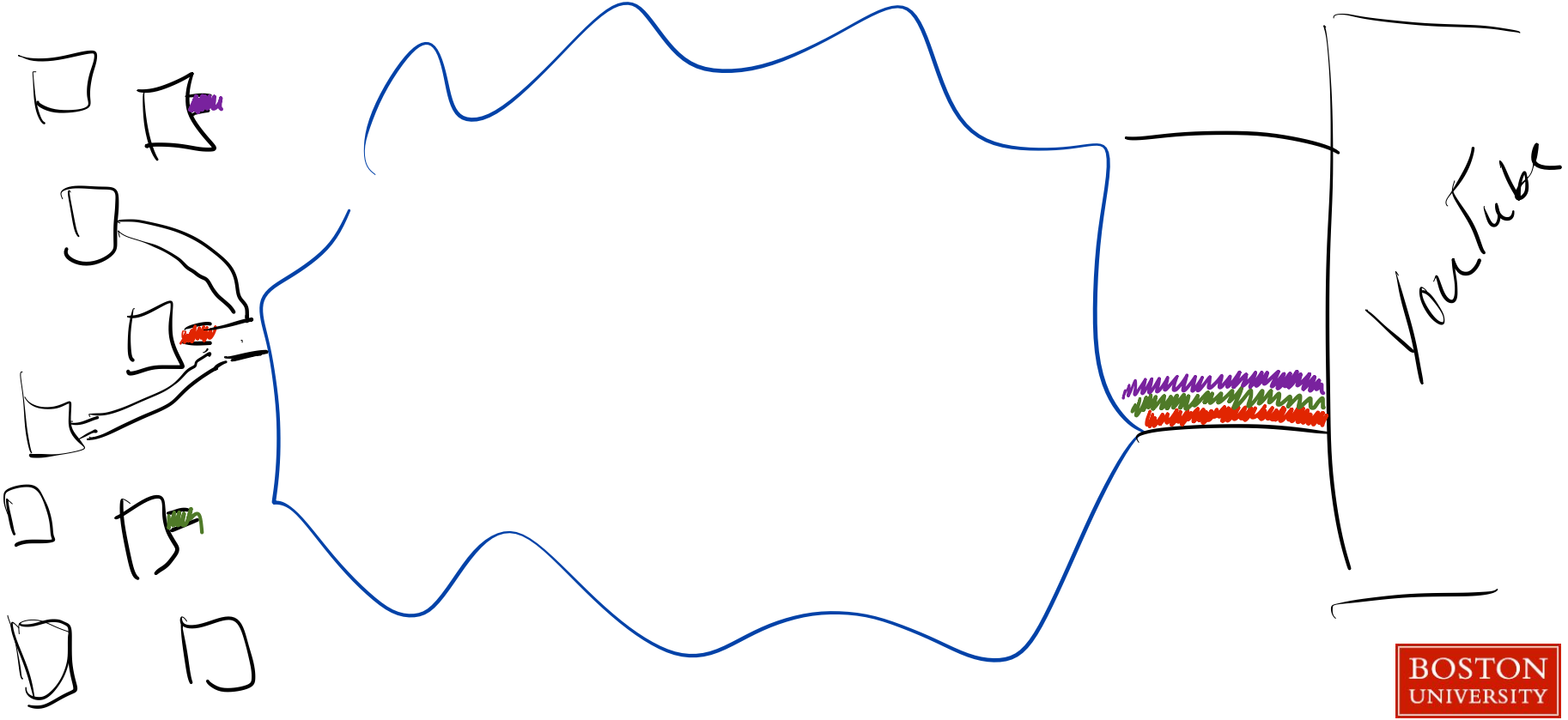
Flooding: Ping & SYN



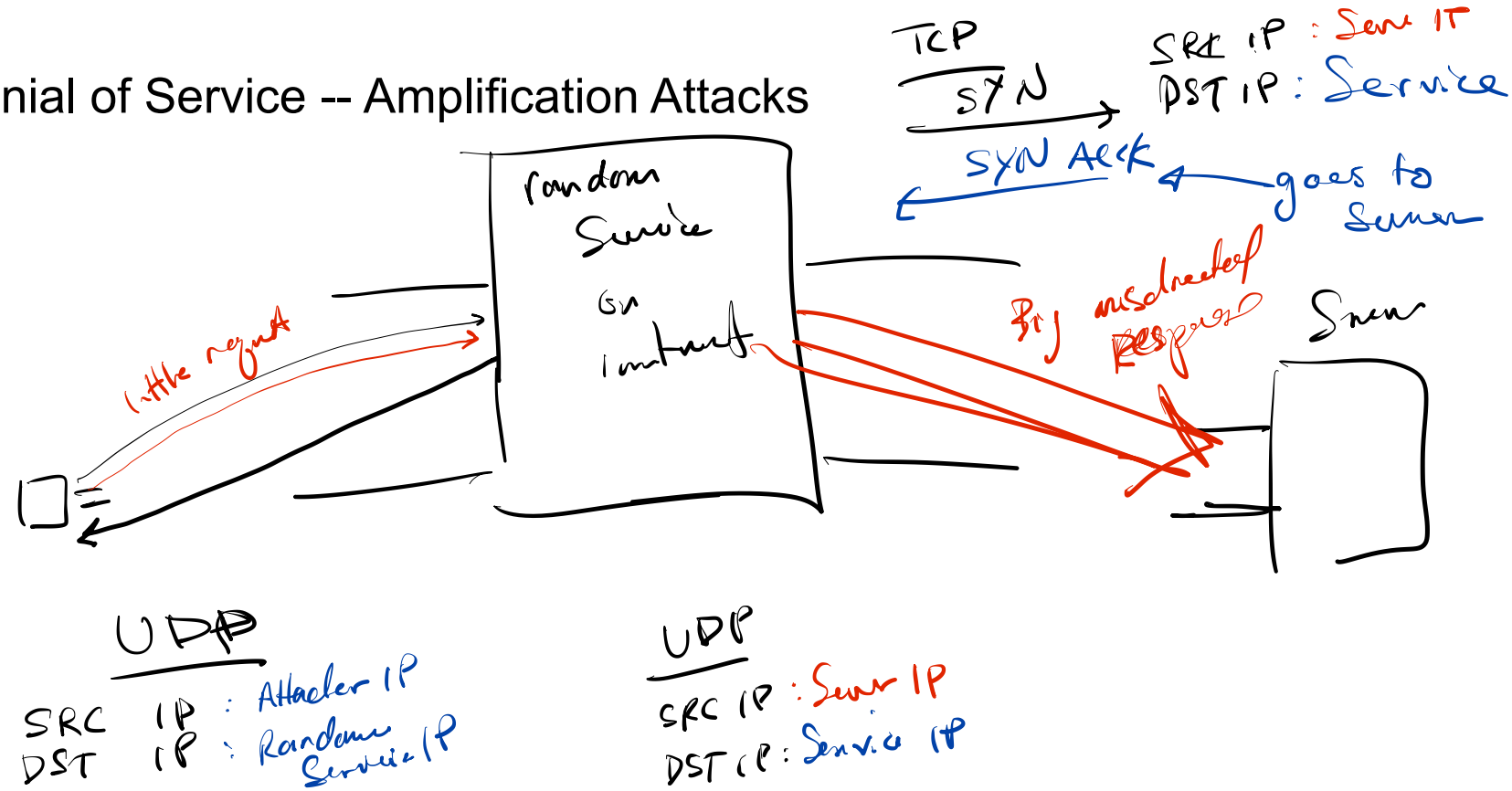
TCP vs UDP



Distributed Denial of Service

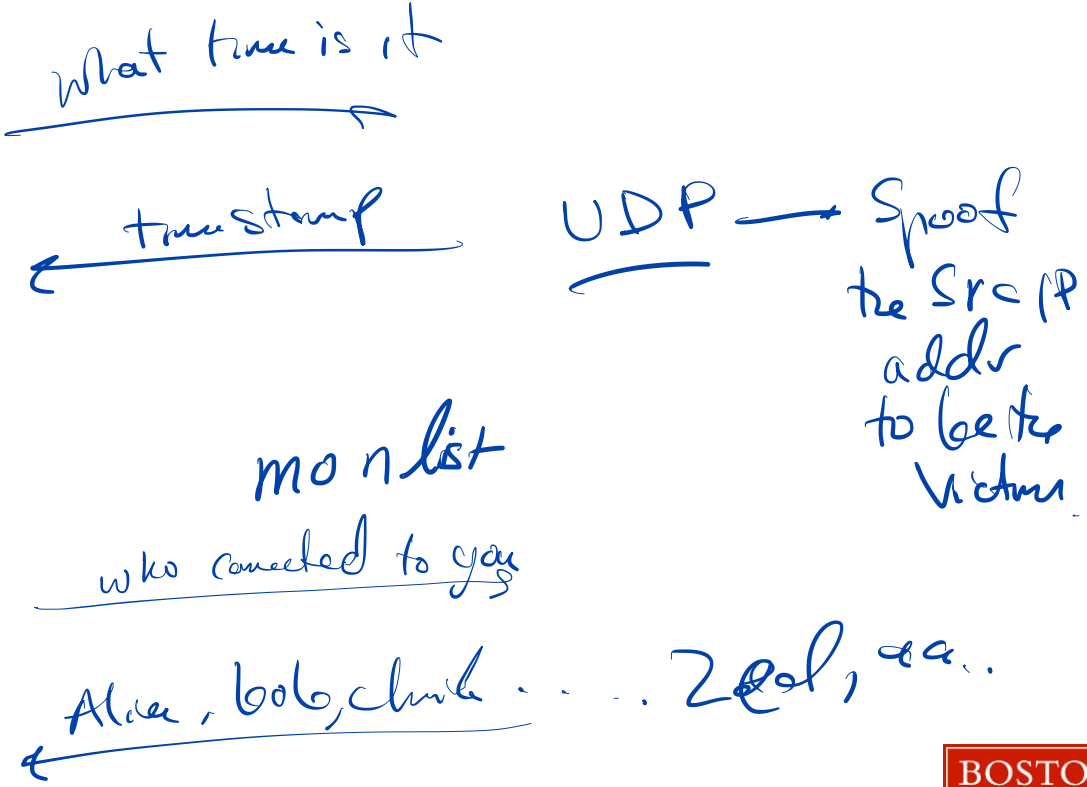


Denial of Service -- Amplification Attacks

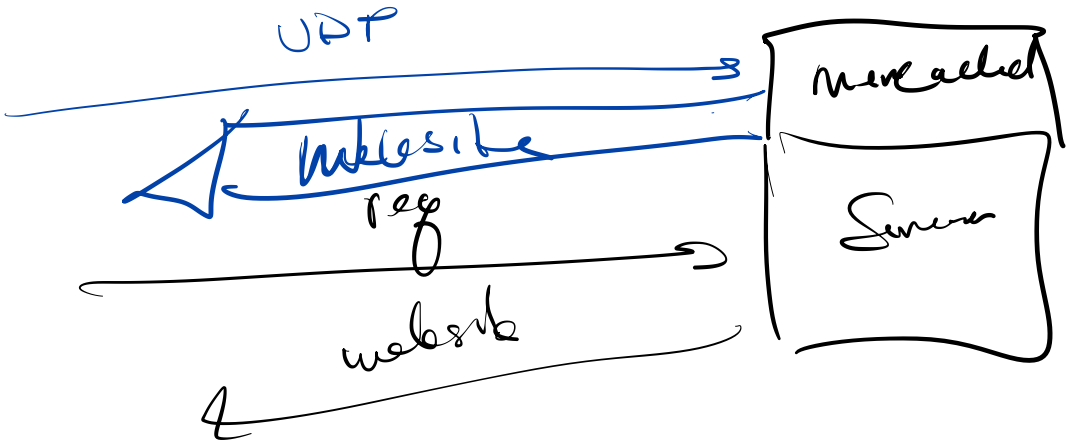


The evolution of DDoS reflection amplification vectors: a chronology

N(etwork) T(ime) P(rotocol)



Memcached (eg. Feb 2018 Against Github @1.3TBPS)



TCP