

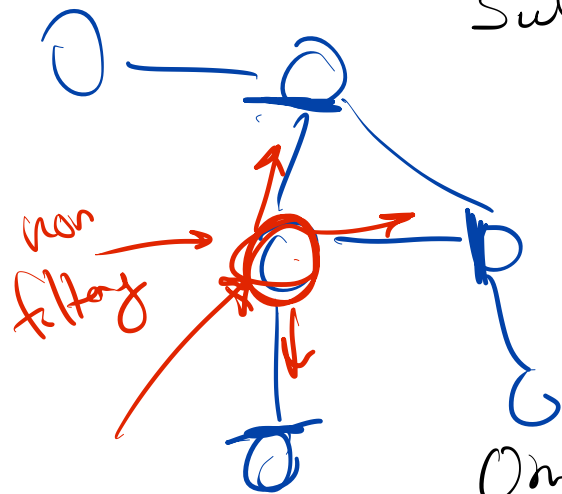
CS558 Network Security

Lecture 8: DoS and DDoS

Julio

Review BGPsec:

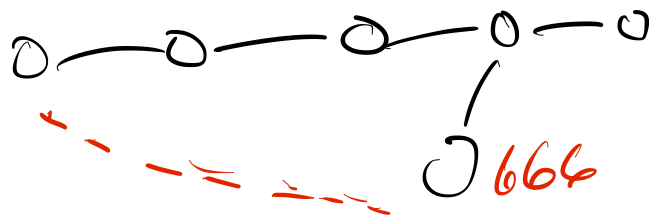
Sub prefix x hijacks → ^{malicious} announcement was more specific than actual announcement



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

One hop attack

BGP Sec
authenticate the path an announcement took



PK_{12}, SK_{12}

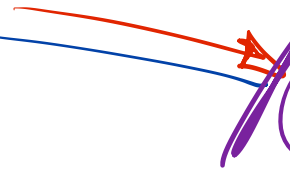
AS12



AS32



PK_{32}, SK_{32}



$$\text{Sign}_{SK_{32}}(\boxed{V} || AS14) = \sigma_{32}$$



AS14



AS463

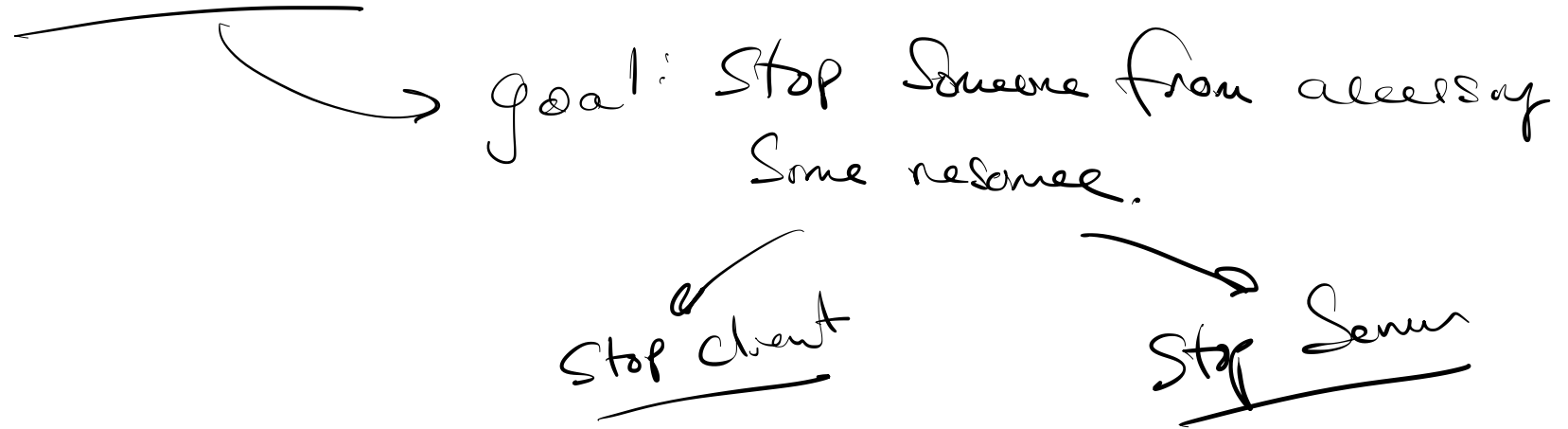


$$\text{Sign}_{SK_{12}}(\text{Announcement} || AS32) = \sigma_{12}$$

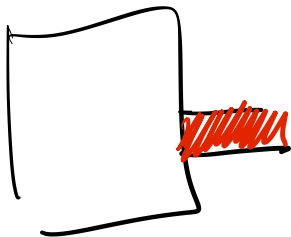


$$\text{Sign}_{SK_{14}}(\boxed{V} || AS463) = \sigma_{14}$$

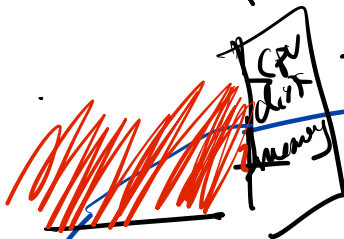
Denial of Service



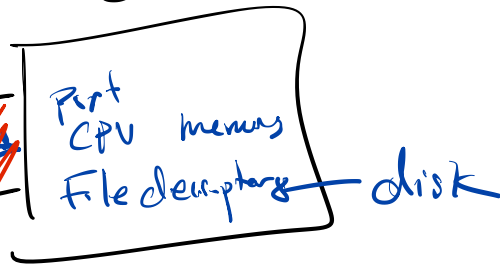
Attacker



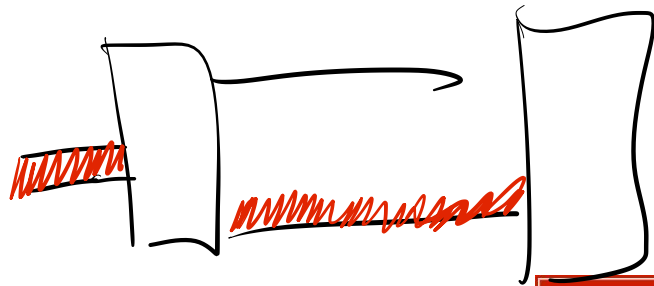
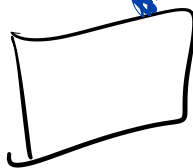
Router



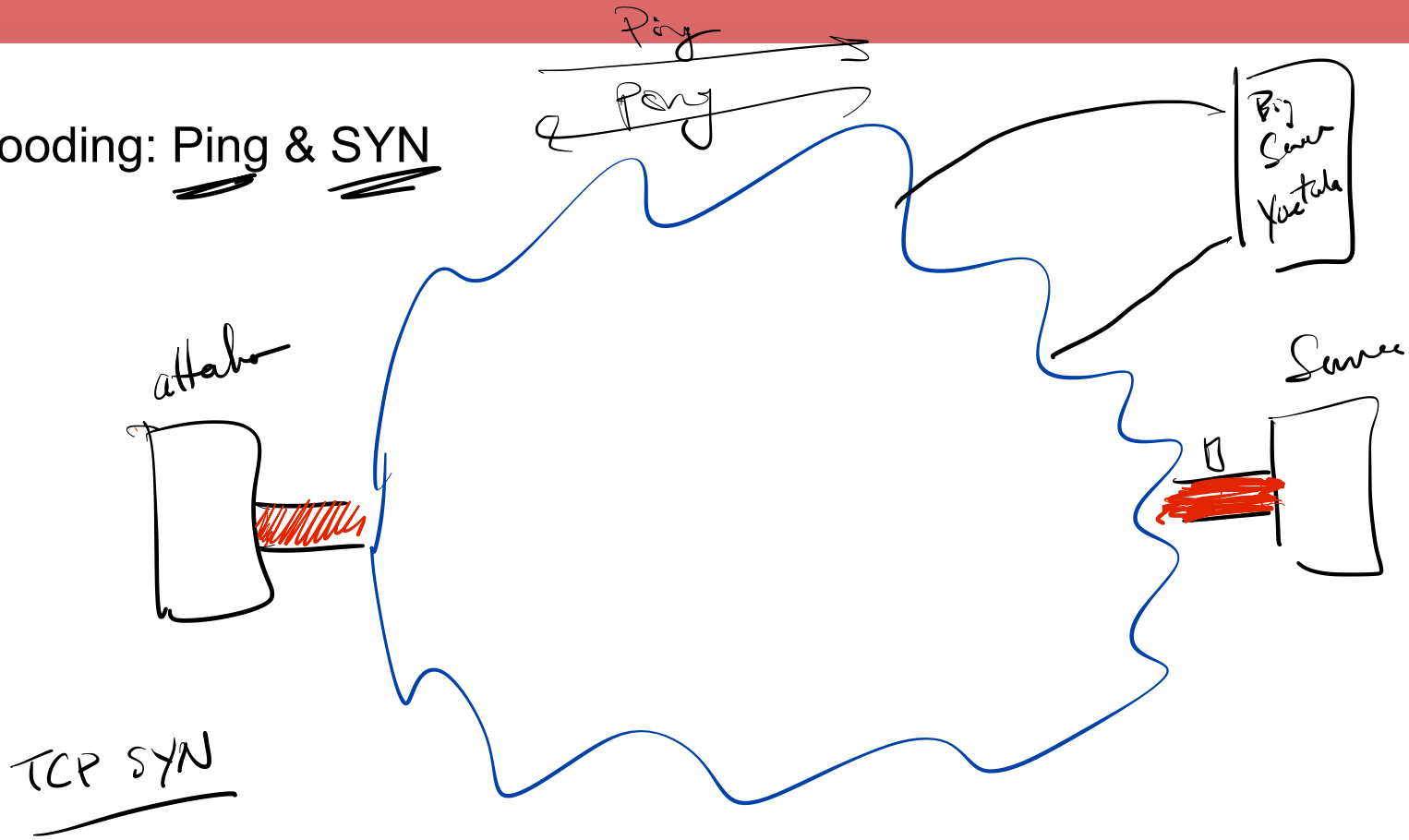
Server



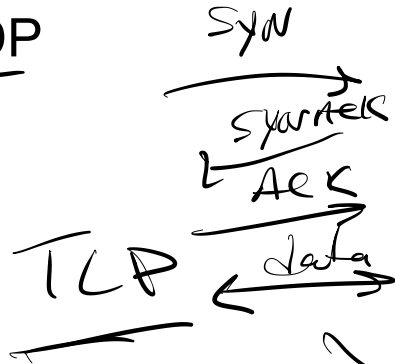
Client



Flooding: Ping & SYN



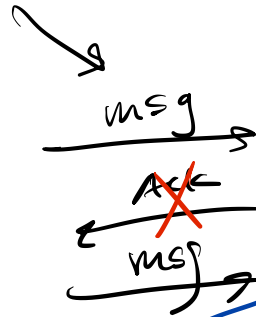
TCP vs UDP



Reliable

Slow

Complicated



UDP

Stateless

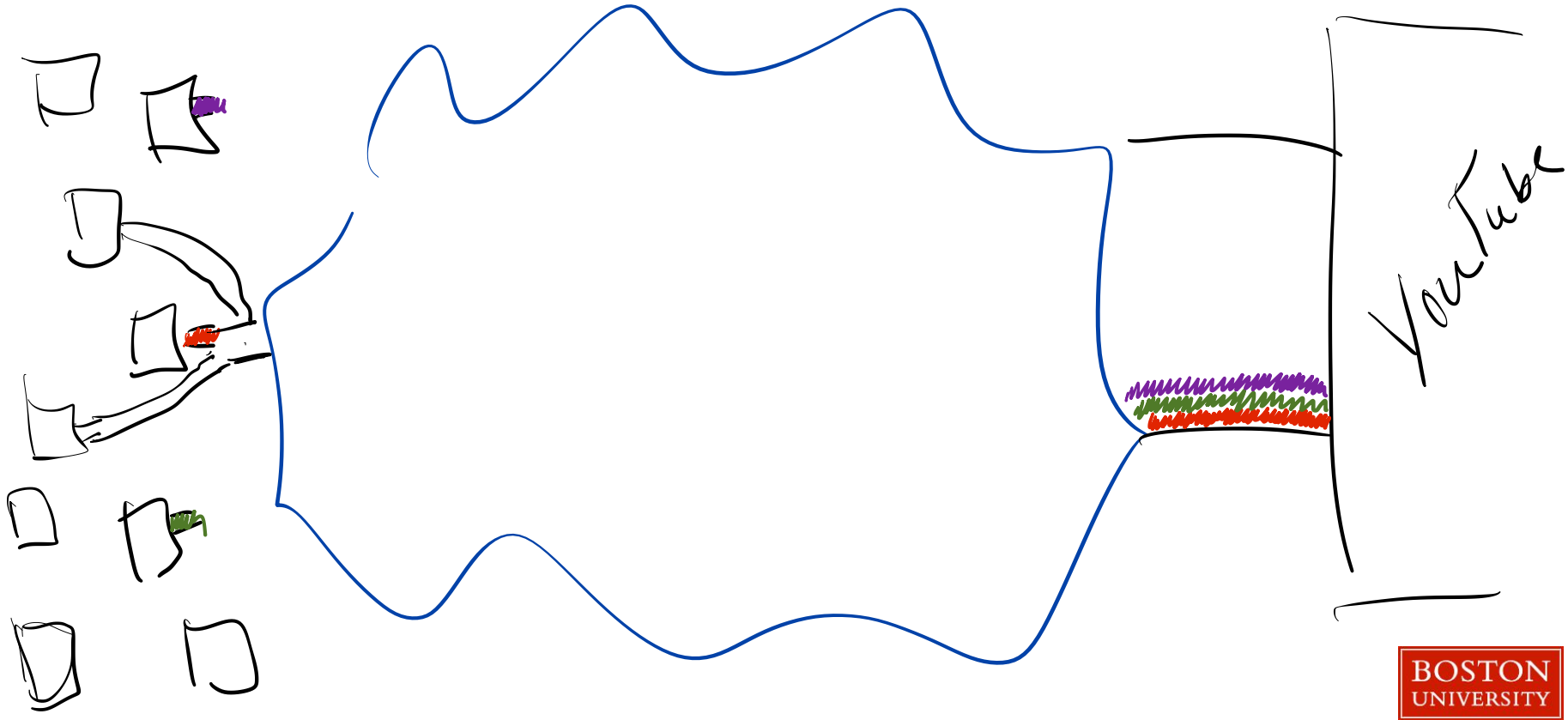
Fast

Not reliable

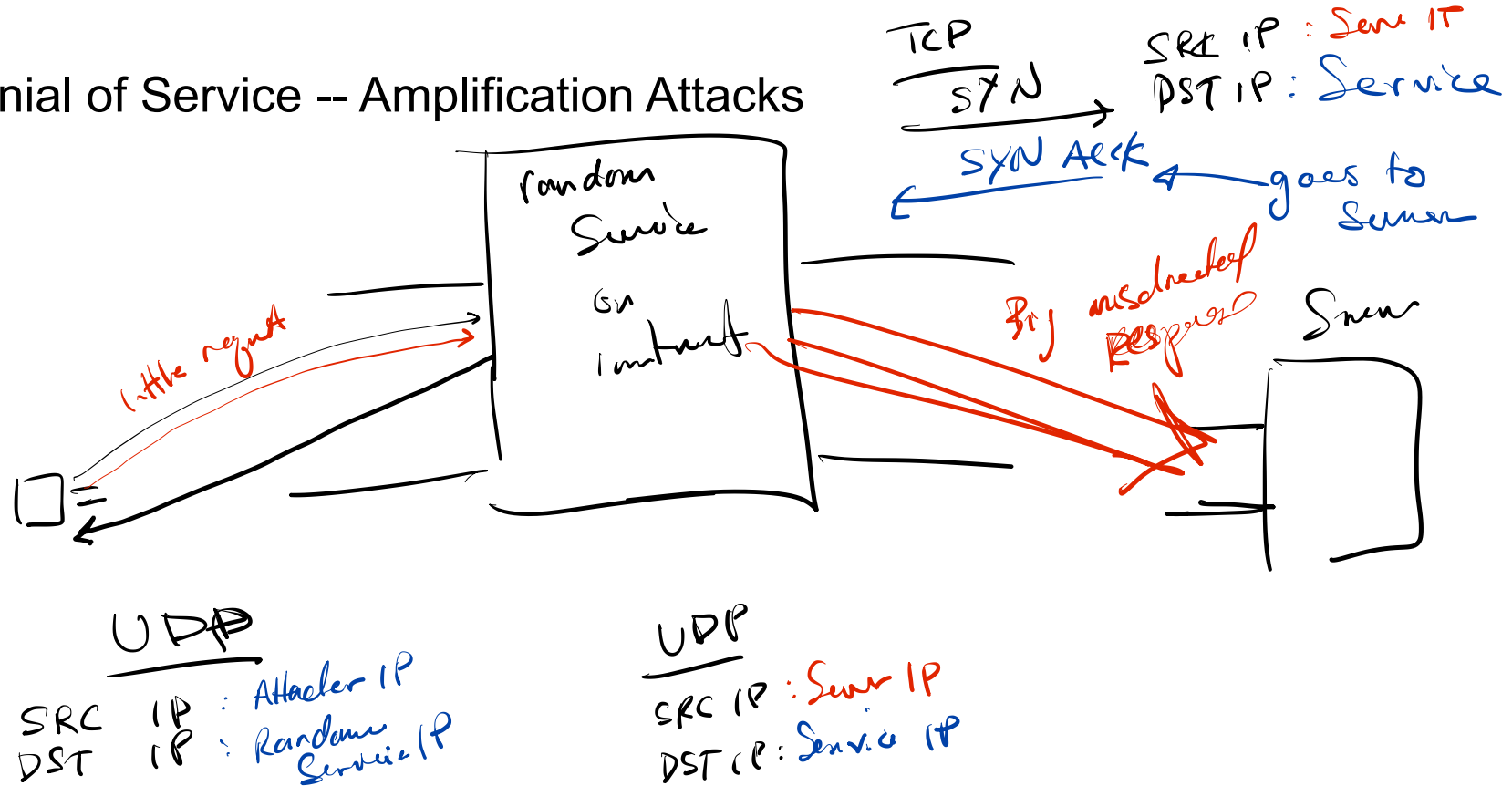
SRC IP: Client IP
DST IP: Server IP
SRC Port: Client port
DST Port: Server port
8080

SRC IP: Server
DST IP: Client
SRC Port: Port # on Server
DST Port: Client port

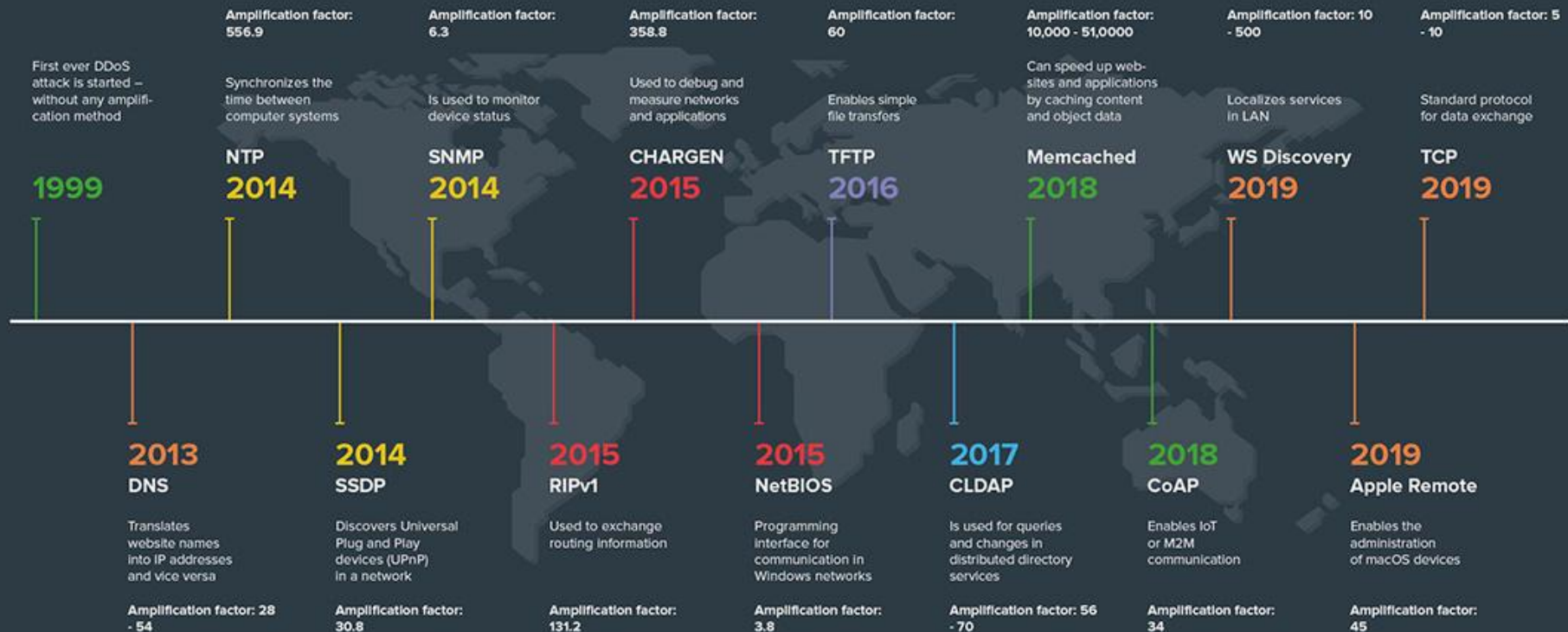
Distributed Denial of Service



Denial of Service -- Amplification Attacks



The evolution of DDoS reflection amplification vectors: a chronology



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

what time is it

timestamp

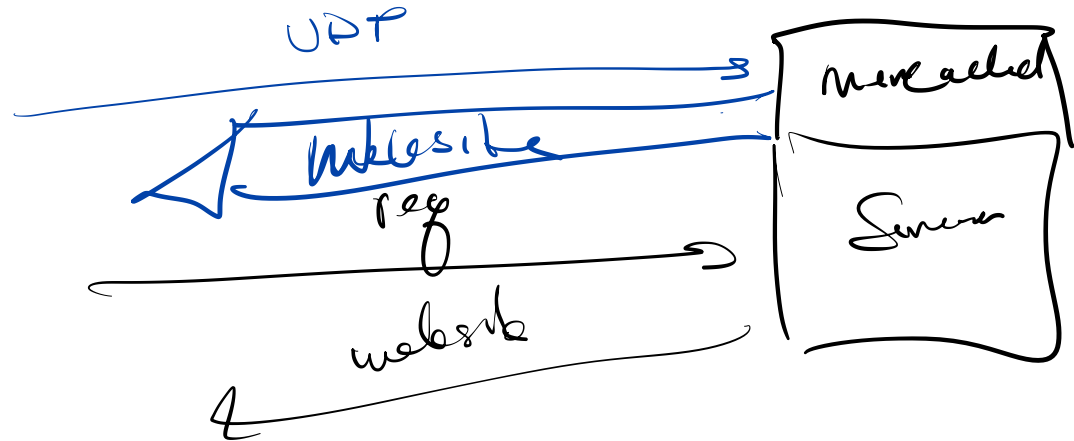
UDP → Spoof
the Src IP
addr
to be the
Victim.

mon list

who connected to you

Alice, bob, chuck . . . Zeol, ea..

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



TCP

(IP, IP, Port, Port)

