Classic Network Attacks

UT CS361S – Network Security and Privacy

Spring 2021

Lecture Notes

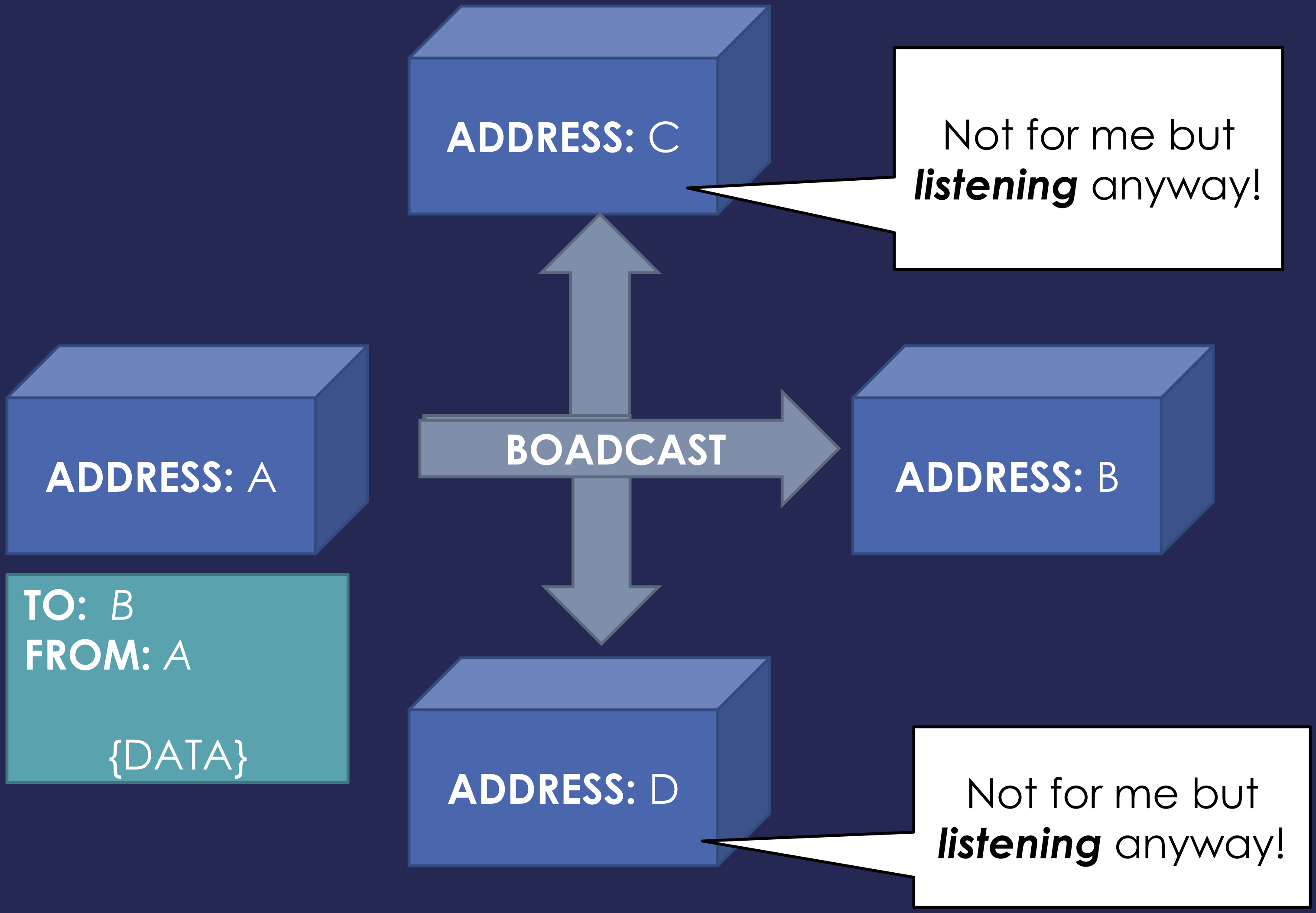
What is an “Attack”?

- Any activity designed to disrupt/violate authorized system goals
- Usually one of “Confidentiality”, “Integrity”, or “Availability”
- Violate Confidentiality – Read Data
- Violate Integrity – Change Data
- Violate Availability – Make Data Unavailable

Eavesdropping

- ***Our entire Internet designed for a <u>TRUSTED WORLD</u>***
- There is no protection for any of CIA by default
- Eavesdropping is super trivial

Eavesdropping in the Old Days



ADDRESS: C

Not for me but ***listening*** anyway!

ADDRESS: A

BOADCAST

ADDRESS: B

TO: *B*
FROM: *A*

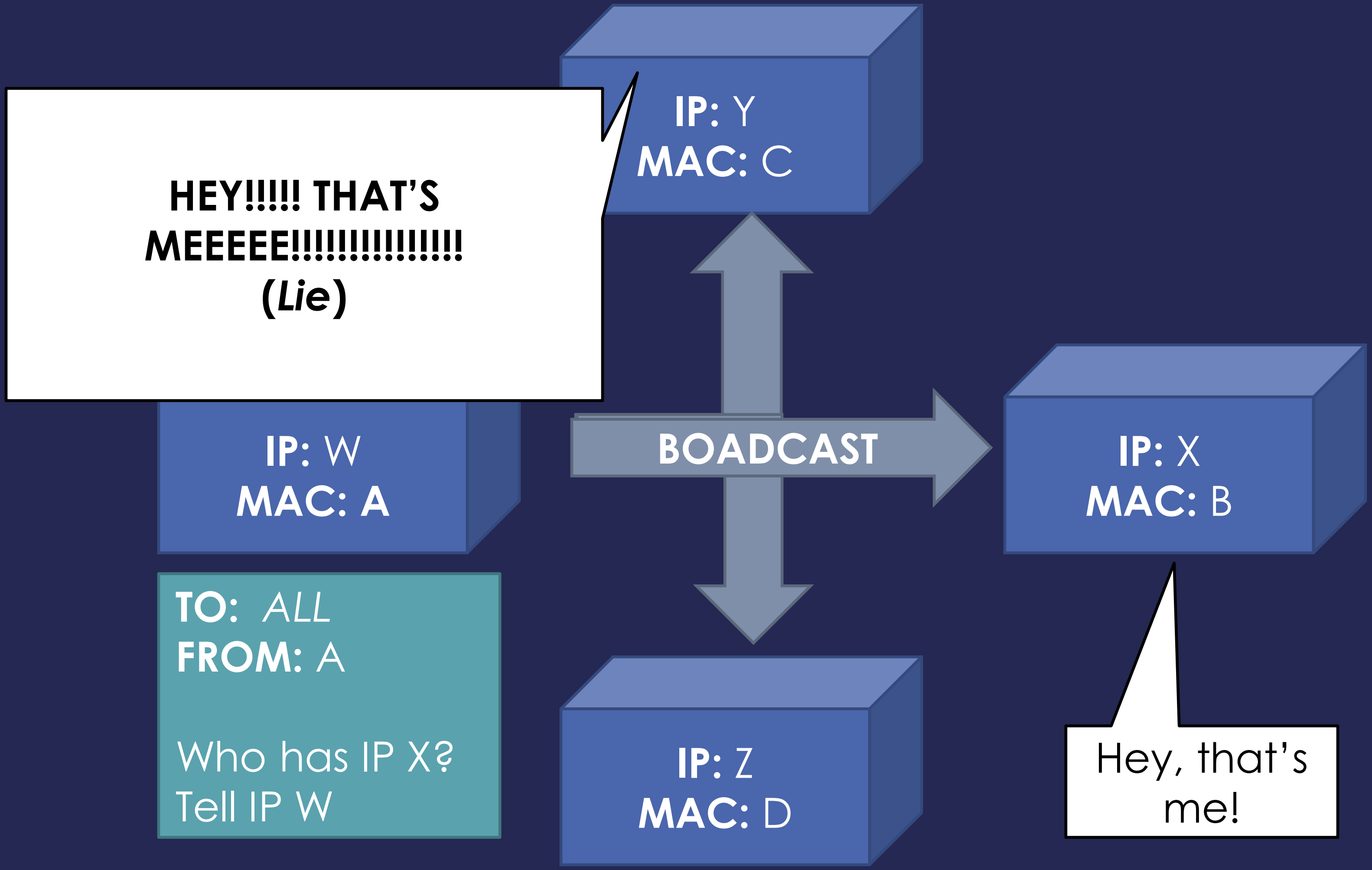
{DATA}

ADDRESS: D

Not for me but ***listening*** anyway!

Passive Adversary

- A “Passive” Adversary cannot ***change/insert*** packets
- Can only intercept packets
- In the old Ethernet days, could passively intercept local data
- Can still be done on WiFi if the encryption is defeated



HEY!!!!! THAT'S MEEEEEE!!!!!!!!!!!!!!!! (*Lie*)

IP: Y
MAC: C

IP: W
MAC: A

BOADCAST

IP: X
MAC: B

IP: Z
MAC: D

TO: *ALL*
FROM: A

Who has IP X?
Tell IP W

Hey, that's me!

Active Adversary

- A "Active" Adversary ***can*** ***change/insert*** packets
- With ARP, can flood other nodes with fake arp responses
- Can convinces other nodes it is the default gateway
- Can now eavesdrop/change data in/out of network

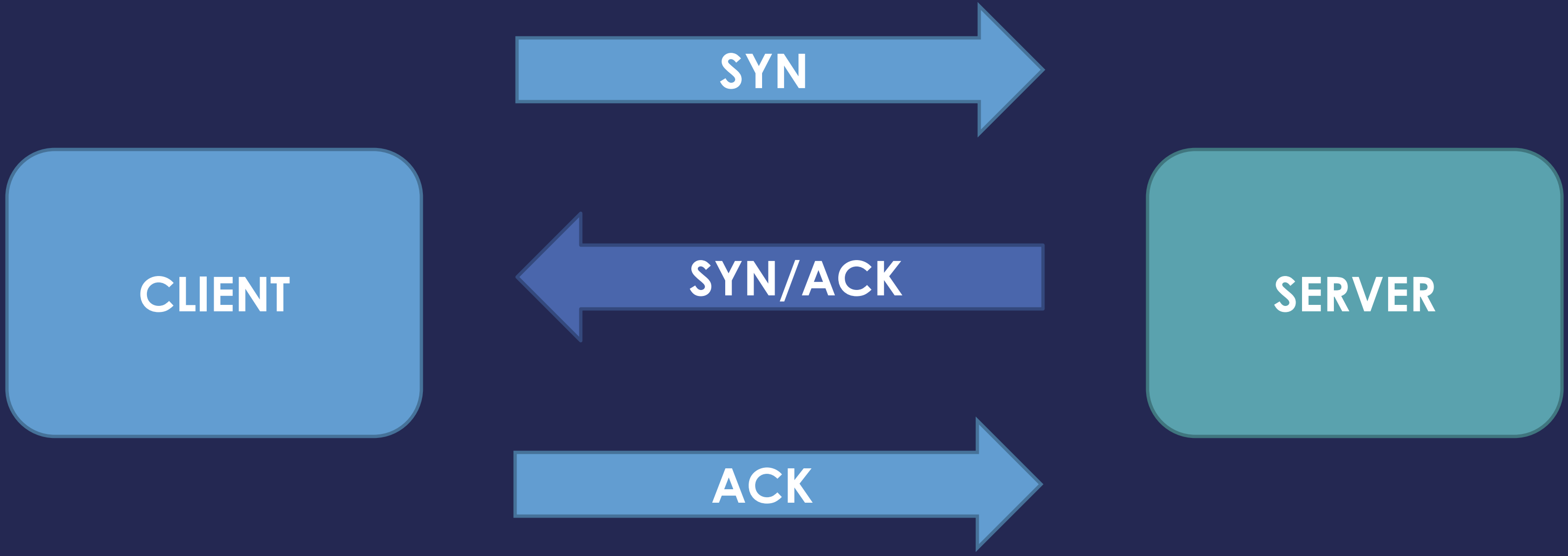
ARP Spoofing Still Works!

- Can still happen today with WiFi (e.g., Coffee Shop)
- Convince other devices before “register”/”connect”

IP Attack: Source Routing

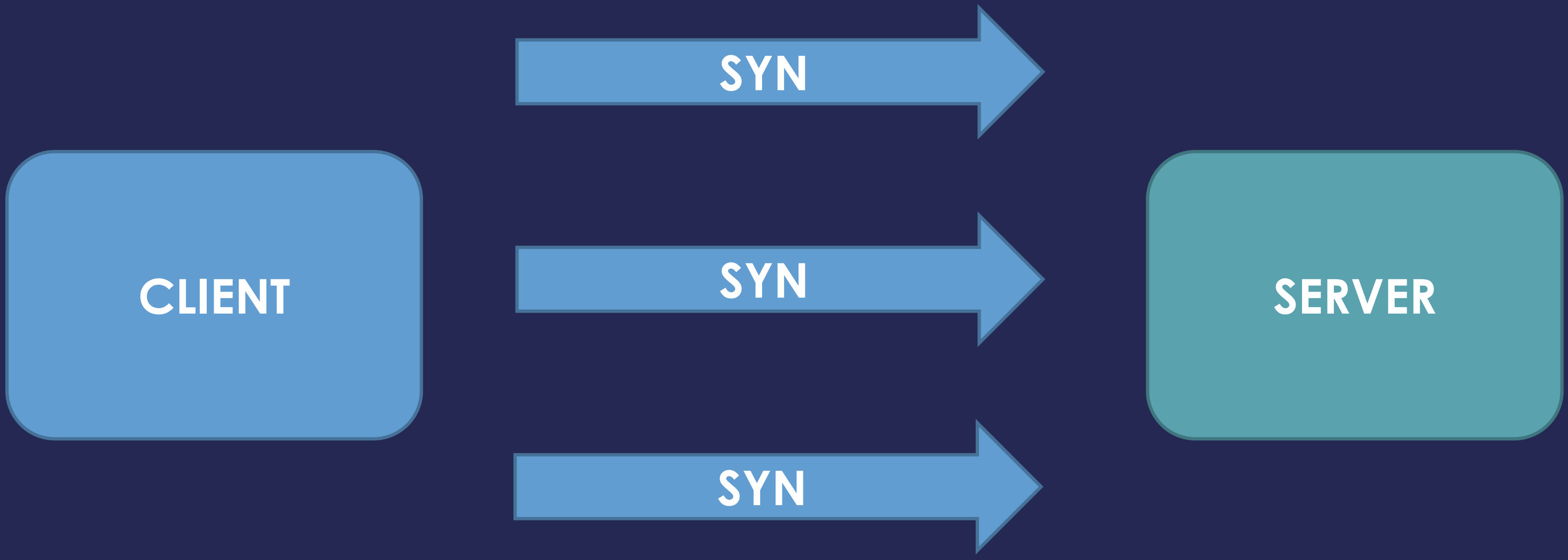
- IP protocol permits specifying an ***explicit route***
- Most modern firewalls block this because of the danger
- Permits an attacker to redirect traffic, bypass firewall, etc

TCP Handshake



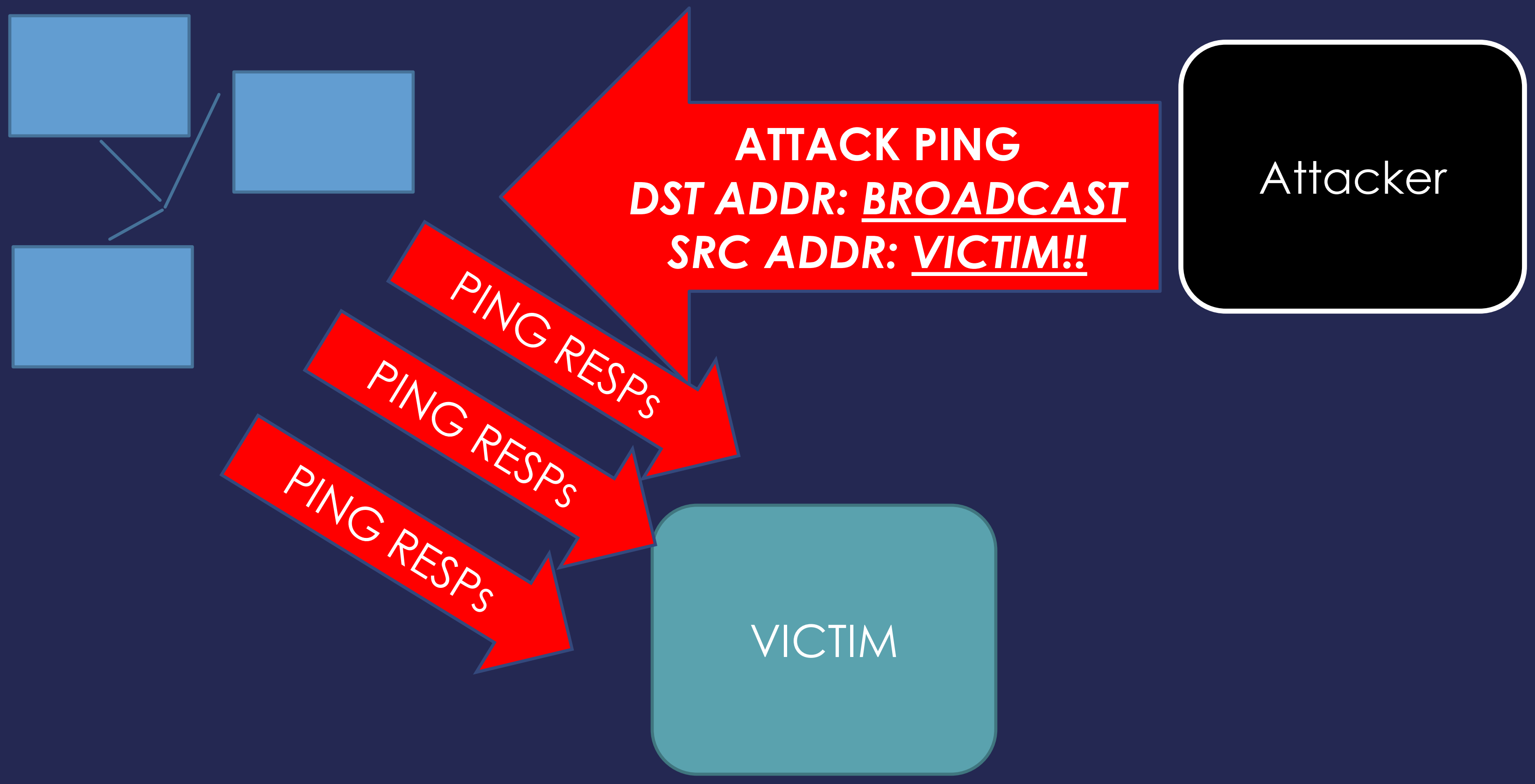
TCP is ***STATEFUL***. Upon SYN, hold state, waits for ACK

SYN Flood



If Server is overloaded with SYN,
will stop accepting new connections

Smurf Attack



ATTACK PING

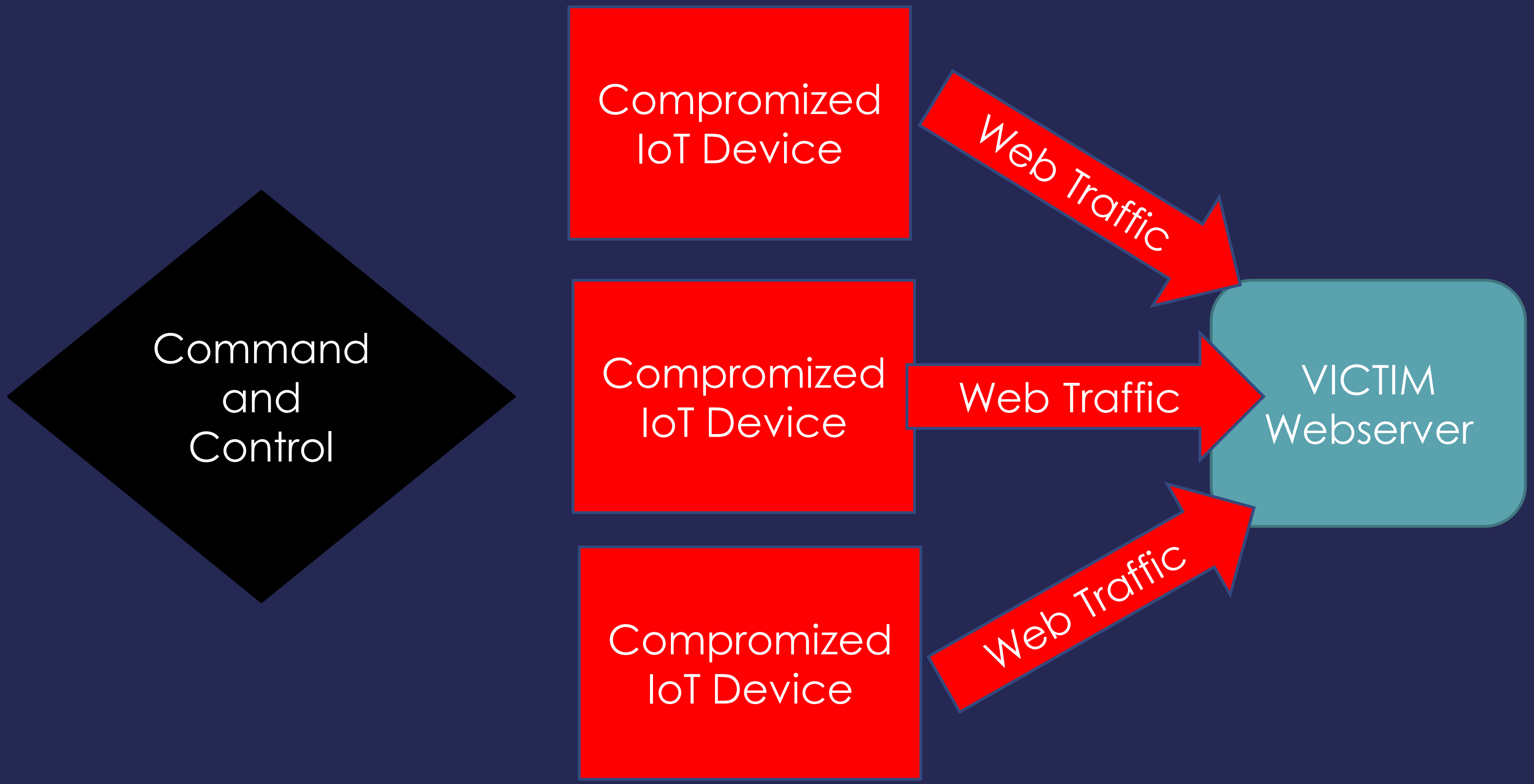
DST ADDR: BROADCAST

SRC ADDR: VICTIM!!

DOS and DDOS

- DOS – Denial of Service; Any reduction in Availability
- DDOS – Distributed Denial of Service; Use ***many*** machines
- Syn Flood from single host, DOS
- Smurf, DDOS
- Syn Flood from many hosts, DDOS

Mirai Botnet Attack, Modern DDOS



TCP Session RST

- TCP-based DOS
- TCP sessions can terminate with an RST packet
- Easy to forge. Easy to guess or flood sequence number

MITM Impersonation

- Of course, attackers like to change data too
- MITM – Man-in-the-middle typically intercepts and alters
- Sometimes just shuts down the original and sends alternate
- One approach: TCP Hijack

TCP Session

- TCP sends session data including a ***sequence number***
- For attacker to "hijack" session, must get correct seq num
- Not as hard as it sounds… flood with multiple copies/nums
- Typically a small enough range to easily hijack

DNS Poisoning

- DNS not all from one server
- Hierarchy of DNS servers requesting from other DNS servers
- Results are cached
- By flooding DNS, can cache wrong results
- This points name to false IP addr
- Kind of like ARP Spoofing