CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous Class

- Security in Networks
  - Threats in Networks
    - Threats in Layer Network (IP) Layer

ICMP Attacks

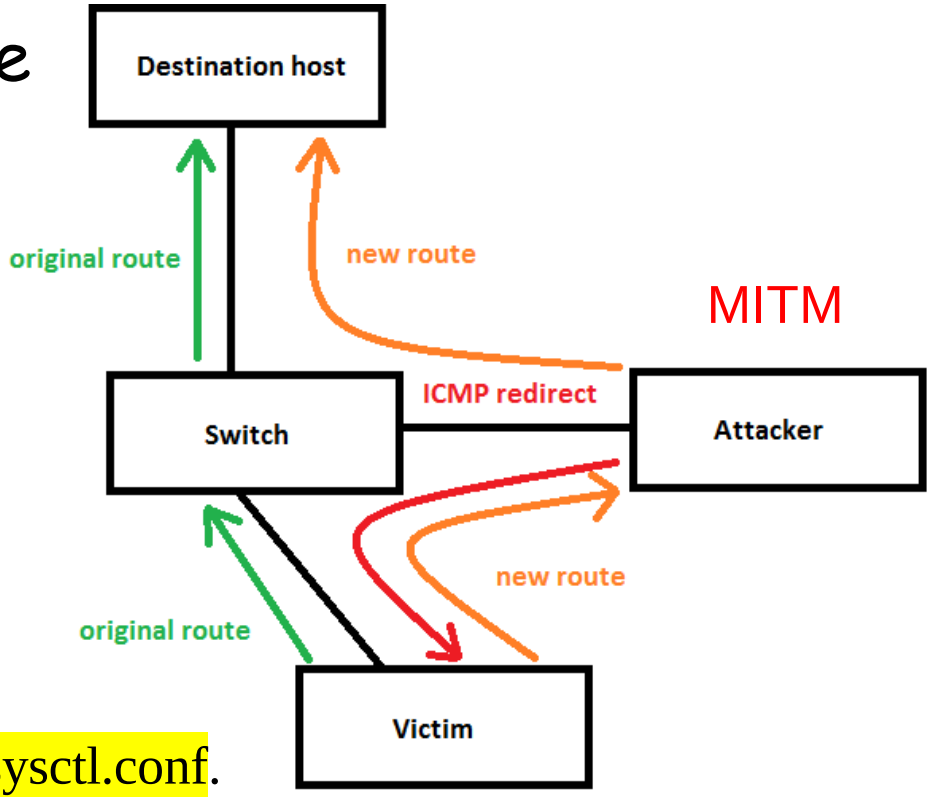
- ICMP is used
  - to *handle errors* and *exchange control messages*.
  - to determine whether a machine is responding.

  - *ICMP Redirect message* is used by gateways when a host has mistakenly assumed the destination is not on the local network.
- If an attacker forges an ICMP "Redirect" message, it can cause another host to send packets for certain connections through the attacker's host.

- There is *no authentication* in ICMP,
  - It can result in a DoS, or
  - allowing the attacker to intercept packets.
- Forge ICMP messages also cause victim overwhelming.

ICMP Redirect Attack

- The attacker simply sends ICMP redirect packets to the victim, to imitate a new optimal gateway.
- The victim re-route the traffic through the attacker and thus allowing the attacker to sniff its communication.
- The attacker can even spoof the source IP and MAC addresses to look as if it is coming from the real gateway.



- Countermeasure:
  - Disable “net.ipv4.conf.all.accept_redirects" in /etc/sysctl.conf.

Ping Flood (ICMP Flood)

- ping command is used by network administrators to test connectivity between two computers.
- In the ping flood attack, it is used to flood large amounts of data packets to the victim repeatedly in an attempt to overload it.

Normal Ping packets

```
ubuntu@VM-GW:~$ ping 172.24.55.6 -c 5
PING 172.24.55.6 (172.24.55.6) 56(84) bytes of data.
64 bytes from 172.24.55.6: icmp_req=1 ttl=64 time=0.991 ms
64 bytes from 172.24.55.6: icmp_req=2 ttl=64 time=1.16 ms
64 bytes from 172.24.55.6: icmp_req=3 ttl=64 time=1.03 ms
64 bytes from 172.24.55.6: icmp_req=4 ttl=64 time=0.926 ms
64 bytes from 172.24.55.6: icmp_req=5 ttl=64 time=1.05 ms

--- 172.24.55.6 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.926/1.032/1.163/0.088 ms
```

Large Size of Ping packets

```
ubuntu@VM-GW:~$ ping 172.24.55.6 -c 5 -s 65500
PING 172.24.55.6 (172.24.55.6) 65500(65528) bytes of data.
65508 bytes from 172.24.55.6: icmp_req=1 ttl=64 time=14.5 ms
65508 bytes from 172.24.55.6: icmp_req=2 ttl=64 time=10.3 ms
65508 bytes from 172.24.55.6: icmp_req=3 ttl=64 time=10.0 ms
65508 bytes from 172.24.55.6: icmp_req=4 ttl=64 time=9.99 ms
65508 bytes from 172.24.55.6: icmp_req=5 ttl=64 time=10.2 ms

--- 172.24.55.6 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 9.994/11.025/14.528/1.756 ms
```

This type of attack is generally useless on larger networks or websites, but it could be a threat if it becomes a *DDoS attack*.

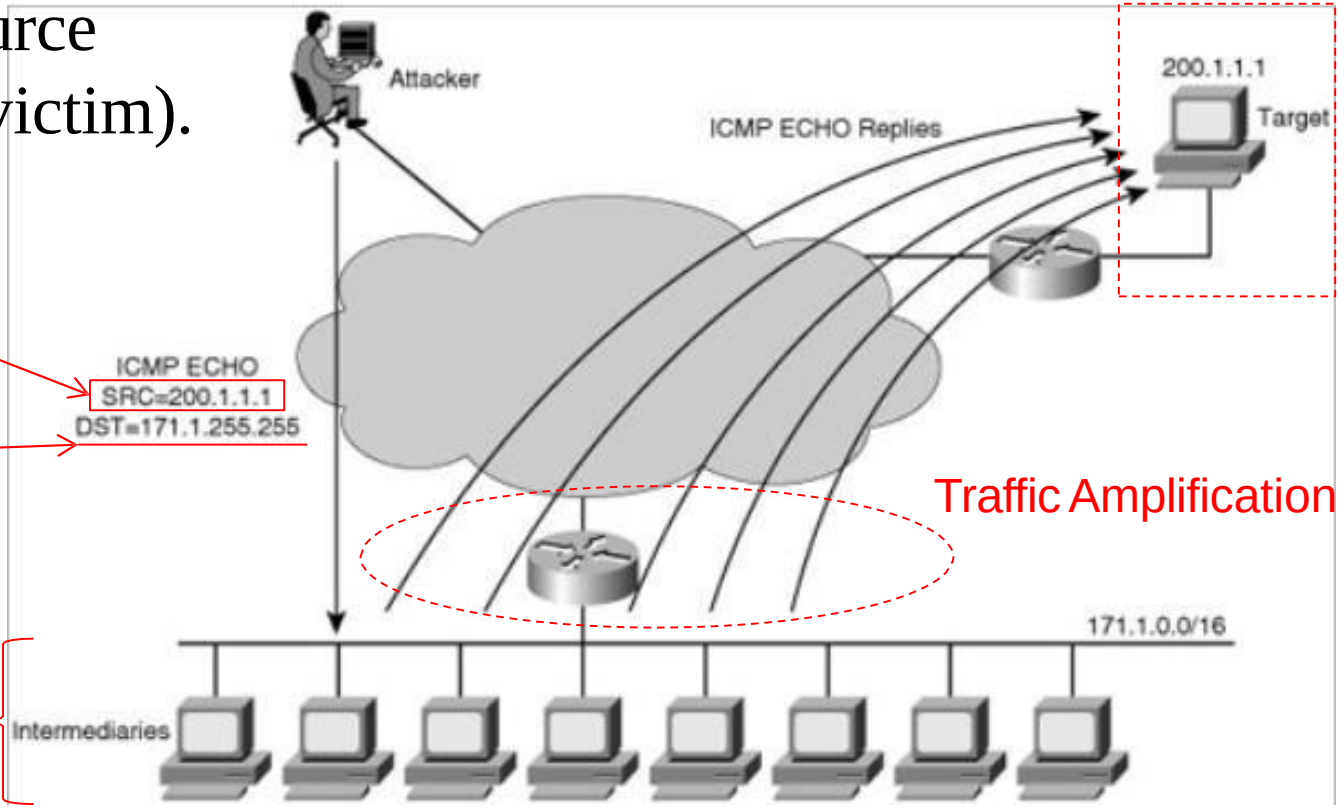
Ping of Death

- ICMP echo with fragmented packets
- Maximum legal size of an ICMP echo packet: 65535 - 20 - 8 = 65507

- IP Fragmentation allows bypassing the maximum size:
- (offset + size) > 65535 (64KB)
- OS cannot reassembled a packet larger than 64KB
- It causes OS crash, reboot or hang
- Most of modern OS or devices are immune to this kind of attack.
- IDS signature: for any fragment offset + length > 64KB
- alert icmp any any -> any any (**dsize:>65507**; msg:"Ping of Death Detected"; sid:7777);

Smurf Attack

- Smurf attack is a type of DoS attack where attacker spoofs *ICMP Echo Request* to a network *broadcast address*.
- All hosts that receive the Echo Requests will response to the spoofed source address (a victim).



Forged IP

Broadcast IP

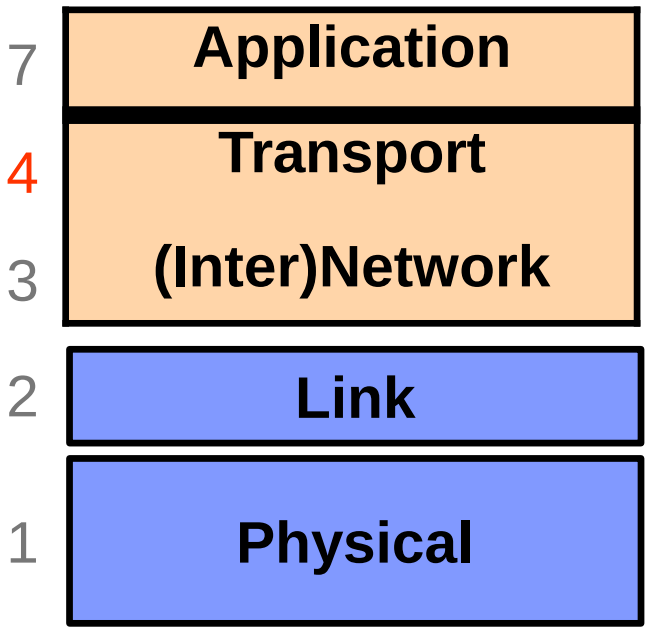
If they do not filter ICMP traffic directed to IP broadcast address

severe network congestion

Homework

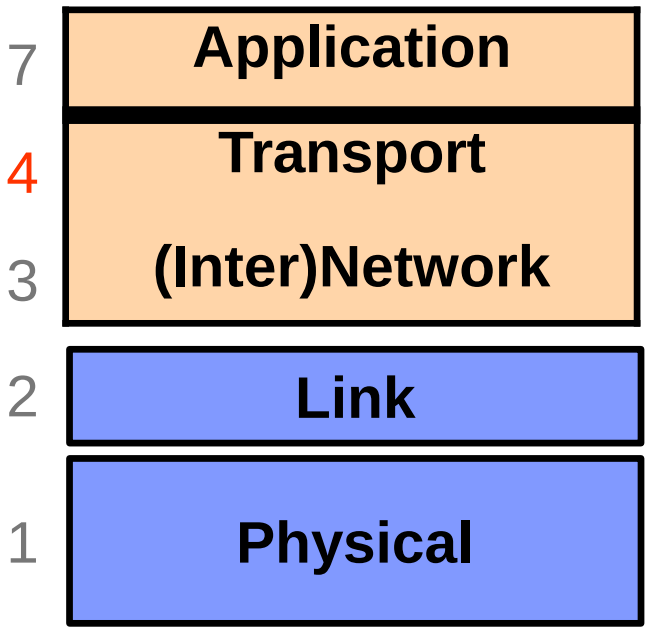
- Work/ Exercise with tcpdump/ wireshark
  - Capture packets and
  - Understand the fields
  - Realize the protocols

TCP



Source port			Destination port
Sequence number			
Acknowledgment			
HdrLen	0	Flags	Advertised window
Checksum			Urgent pointer
Options (variable)			
Data			

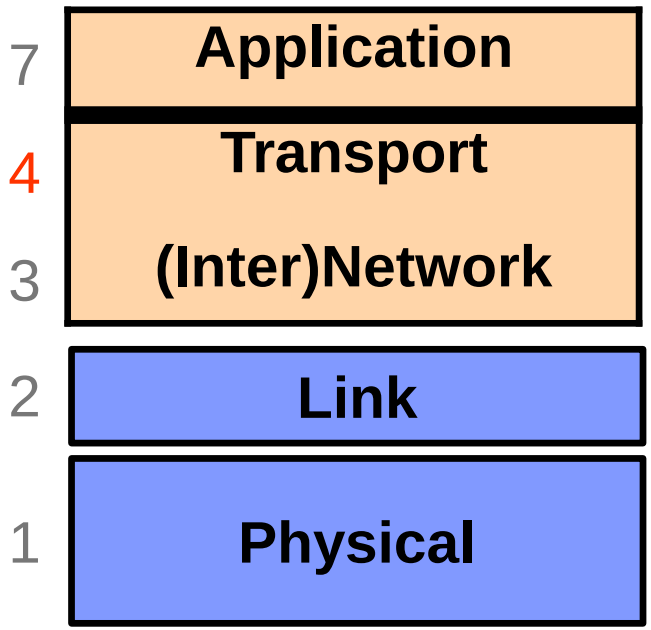
TCP



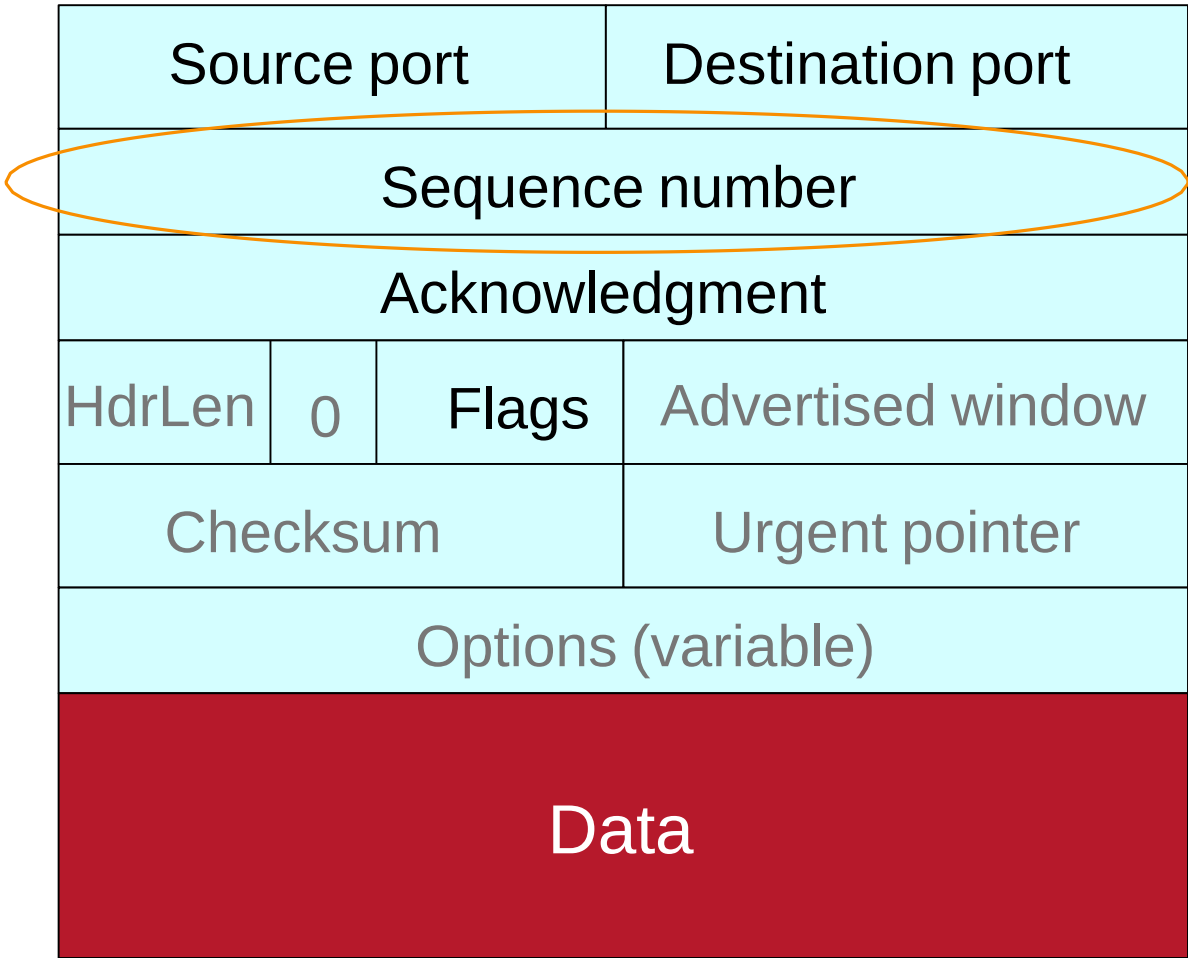
These plus IP addresses define a given connection

Source port			Destination port
Sequence number			
Acknowledgment			
HdrLen	0	Flags	Advertised window
Checksum			Urgent pointer
Options (variable)			
Data			

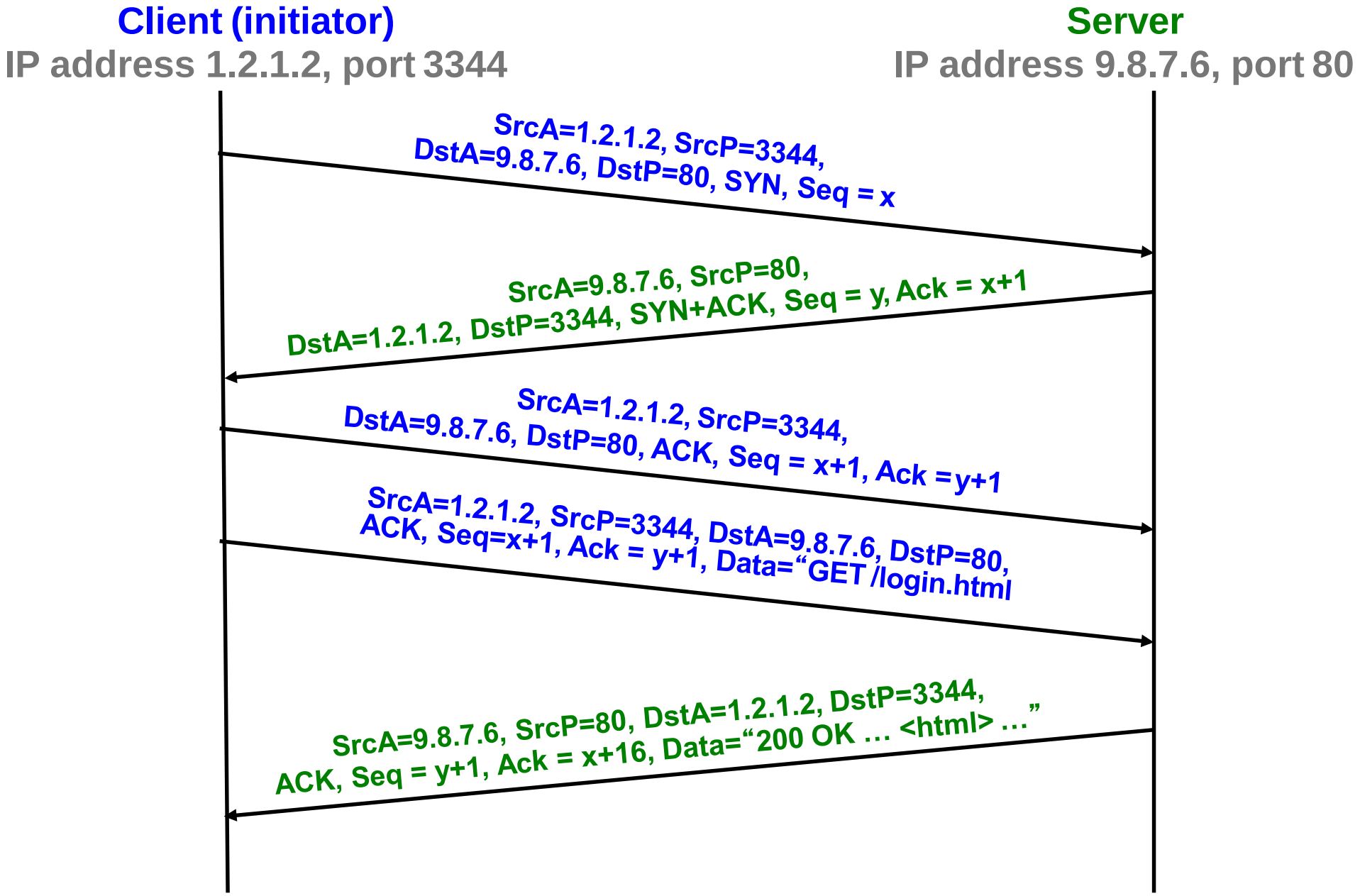
TCP



Defines where this packet fits within the sender's bytestream

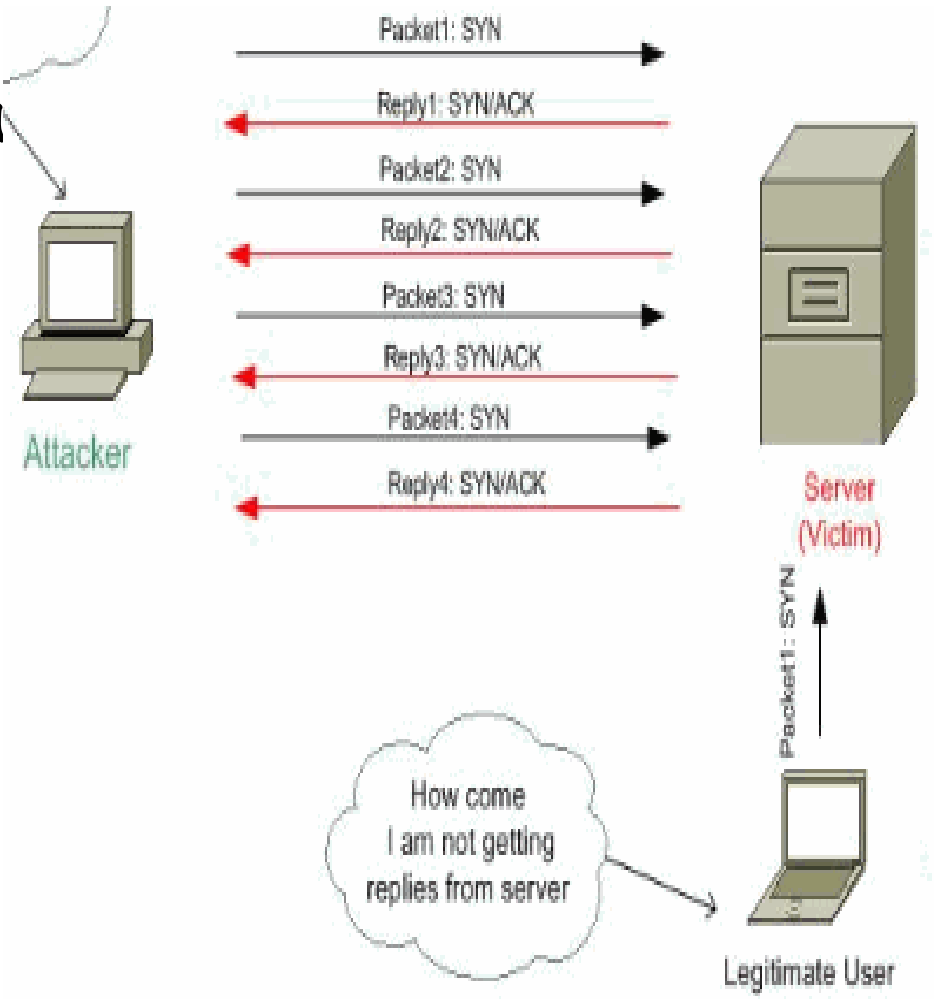


TCP Conn. Setup & Data Exchange



TCP Layer Attacks

- TCP SYN Flooding
  - Exploit state allocated a server after initial SYN packet
  - Send a SYN and don't reply with ACK
  - Server will wait for 511 seconds for ACK
  - Finite queue size for incomplete connections (1024)
  - Once the queue is full it doesn't accept requests



TCP Layer Attacks

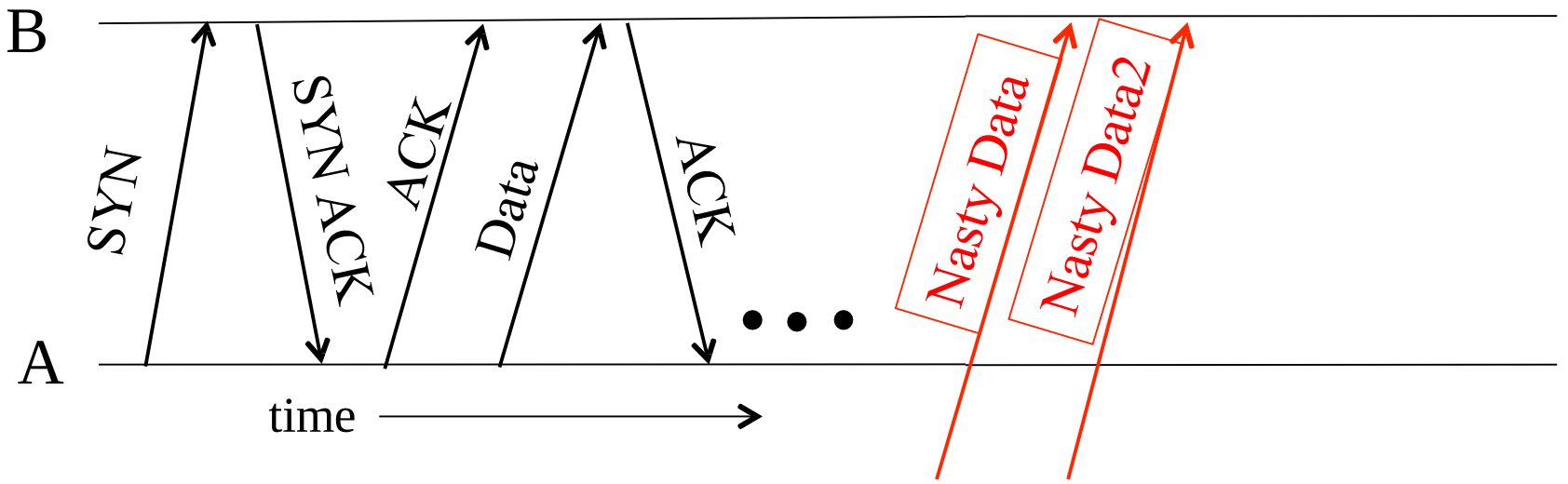
- TCP Session Hijack:
  - Hacker takes over a **TCP** session between two machines.
  - Also called active sniffing

  - Involves the attacker gaining access to a host in the network and disconnecting it
  - Attacker then inserts another machine with the same IP address, which will allow the attacker access to all information on the original system
  - UDP and TCP don't check the validity of an IP address which is why this attack is possible

Categories of **TCP** Session Hijacking

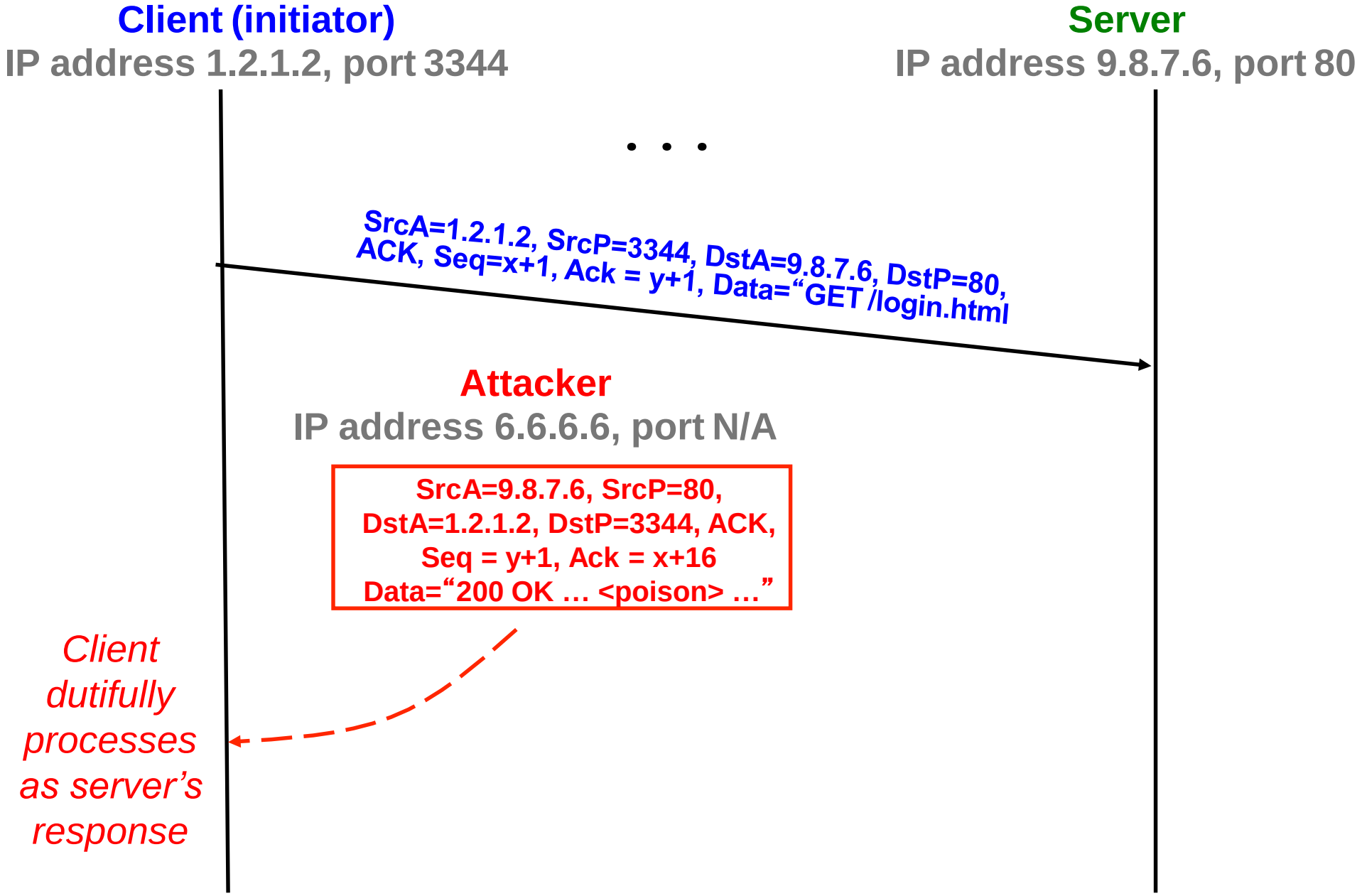
- Based on the anticipation of sequence numbers there are two types of TCP hijacking:
  - Man-in-the-middle (**MITM**):
    - A hacker can be "inline" between **B** and **C** using a sniffing program (passively or actively) to watch the sequence numbers and acknowledge numbers in the IP packets transmitted between **B** and **C**. And then hijack the connection. This is known as a "man-in-the-middle attack".
  - Blind Hijack
    - to brute force all combinations of sequence number
      - which will be an unreliable task (32 bit seq no.).

TCP Threat: Data Injection

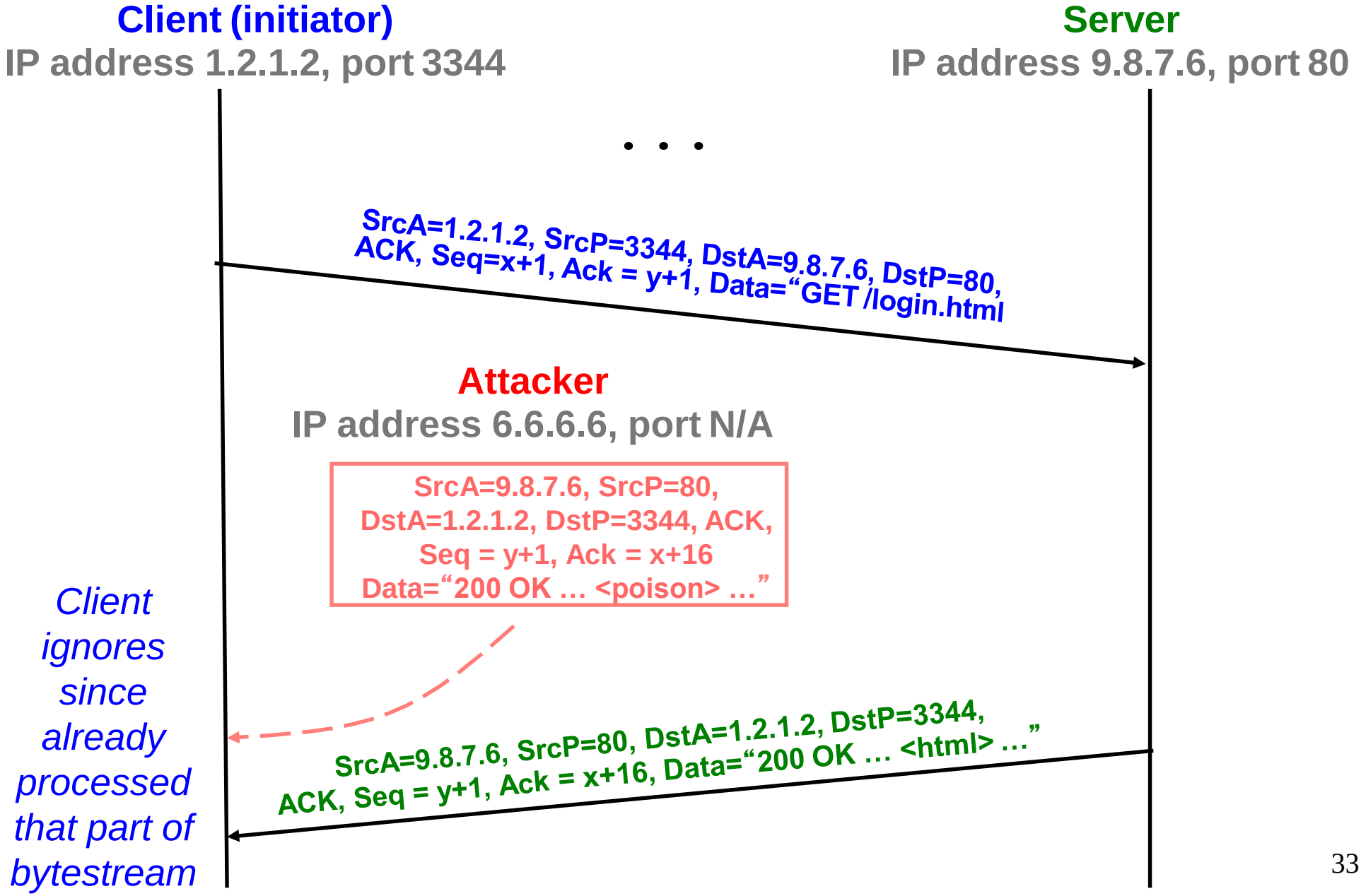


- If attacker knows ports & sequence numbers (e.g., on-path attacker), attacker can inject data into any TCP connection
- Termed TCP connection hijacking (or "*session hijacking*")
  - A general means to take over an already-established connection!
- We are toast if an attacker can see our TCP traffic!
  - Because then they immediately know the port & sequence numbers

TCP *Data Injection*



TCP *Data Injection*

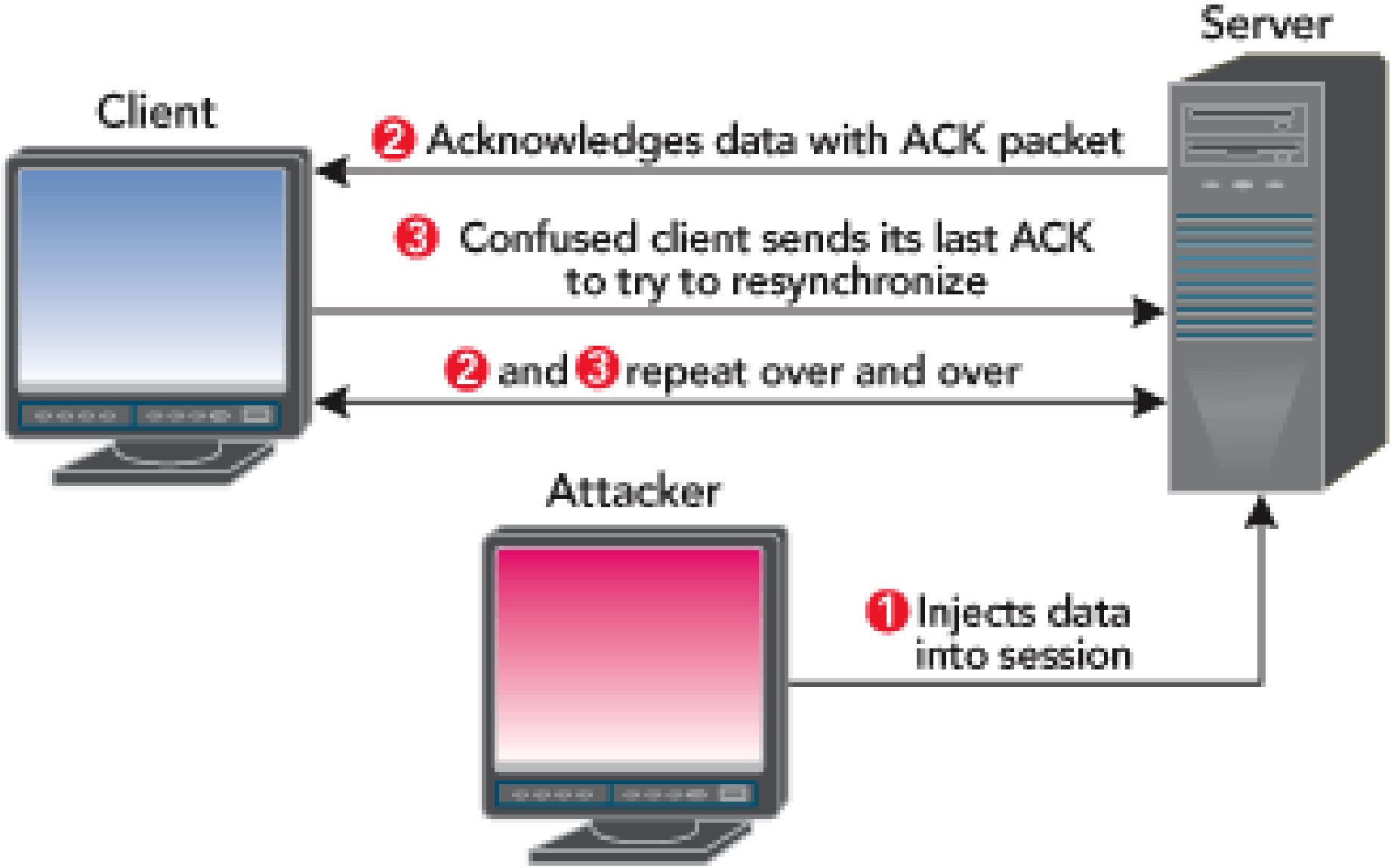


TCP Layer Attacks

- When is a TCP packet valid?
  - Address/Port/Sequence Number in window
  - How to get sequence number?
    - Sniff traffic
    - Guess it
      - Many earlier systems had predictable ISN
  - Inject arbitrary data to the connection

- Do you have to guess the exact sequence number?
  - Anywhere in window is fine
  - For 64k window it takes 64k packets to reset
- It can lead to
  - Desynchronize
  - TCP Ack storm attack

ACK Storm


Server
Client
2 Acknowledges data with ACK packet
3 Confused client sends its last ACK to try to resynchronize
2 and 3 repeat over and over
Attacker
1 Injects data into session

Network security and privacy

- The primary use for cryptography
  - "Separating the security of the medium from the security of the message"

- Entities you can only communicate with over a network are inherently less trustworthy
  - They may not be who they claim to be

What an Attacker Might Do?

- Read communication
- Modify communication
- Forge communication
- Inhibit communication

Network security and privacy

- Cryptography is used at every layer of the network stack for both security and privacy applications:
  - Link layer Security
  - Network
    - VPN, IPSec
  - Transport
    - TLS / SSL, Tor
  - Application
    - PGP, OTR,

- Thanks