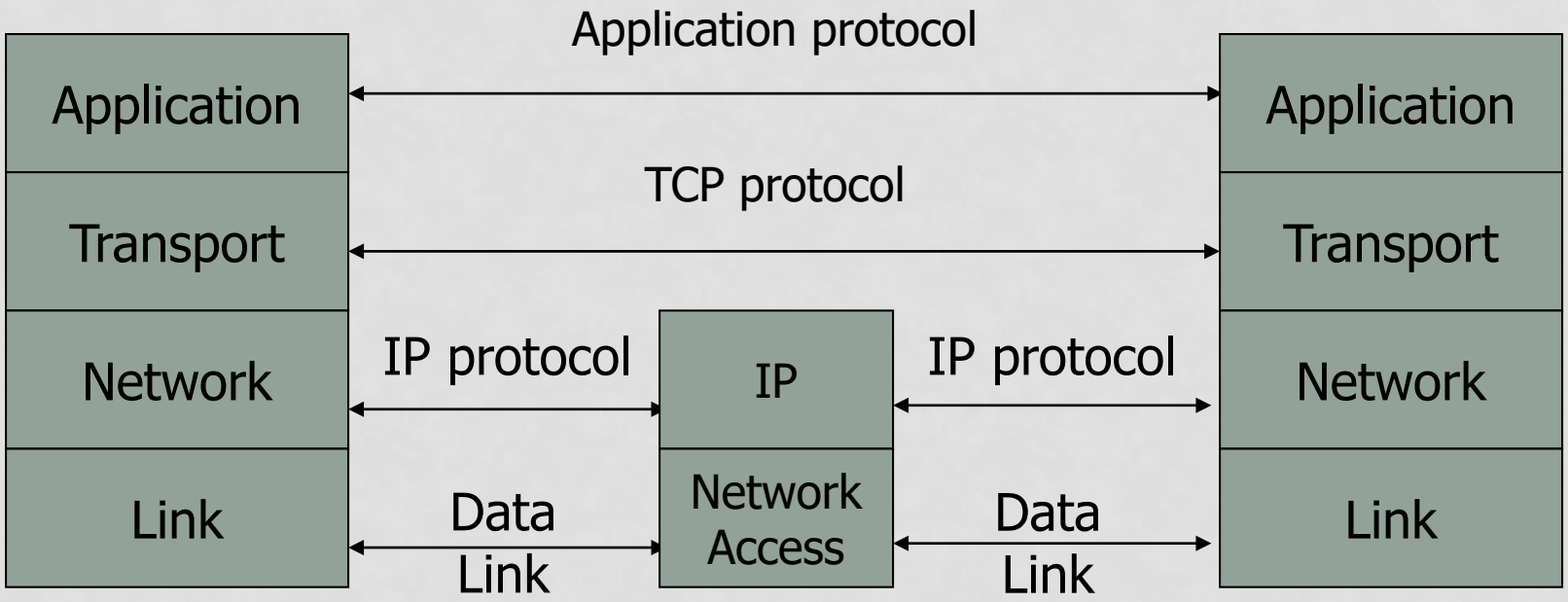
CSC429 – Computer Security

LECTURE 12
NETWORK SECURITY

Mohammed H. Almeshekah, PhD
meshekah@ksu.edu.sa

Network Protocol Stack



Types of Addresses in Internet

- Media Access Control (MAC) addresses in the network access layer
  - Associated w/ network interface card (NIC)
  - 48 bits or 64 bits
- IP addresses for the network layer
  - 32 bits for IPv4, and 128 bits for IPv6
  - E.g., 128.3.23.3
- IP addresses + ports for the transport layer
  - E.g., 128.3.23.3:80
- Domain names for the application/human layer
  - E.g., www.purdue.edu

Routing and Translation of Addresses

- Translation between IP addresses and MAC addresses
  - Address Resolution Protocol (ARP) for IPv4
  - Neighbor Discovery Protocol (NDP) for IPv6
- Routing with IP addresses
  - TCP, UDP, IP for routing packets, connections
  - Border Gateway Protocol for routing table updates
- Translation between IP addresses and domain names
  - Domain Name System (DNS)

Threats in Networking

- Confidentiality
  - E.g. Packet sniffing
- Integrity
  - E.g. Session hijacking
- Availability
  - E.g. Denial of service attacks
- Combinations/Other
  - Address translation poisoning attacks.
  - Routing attacks.

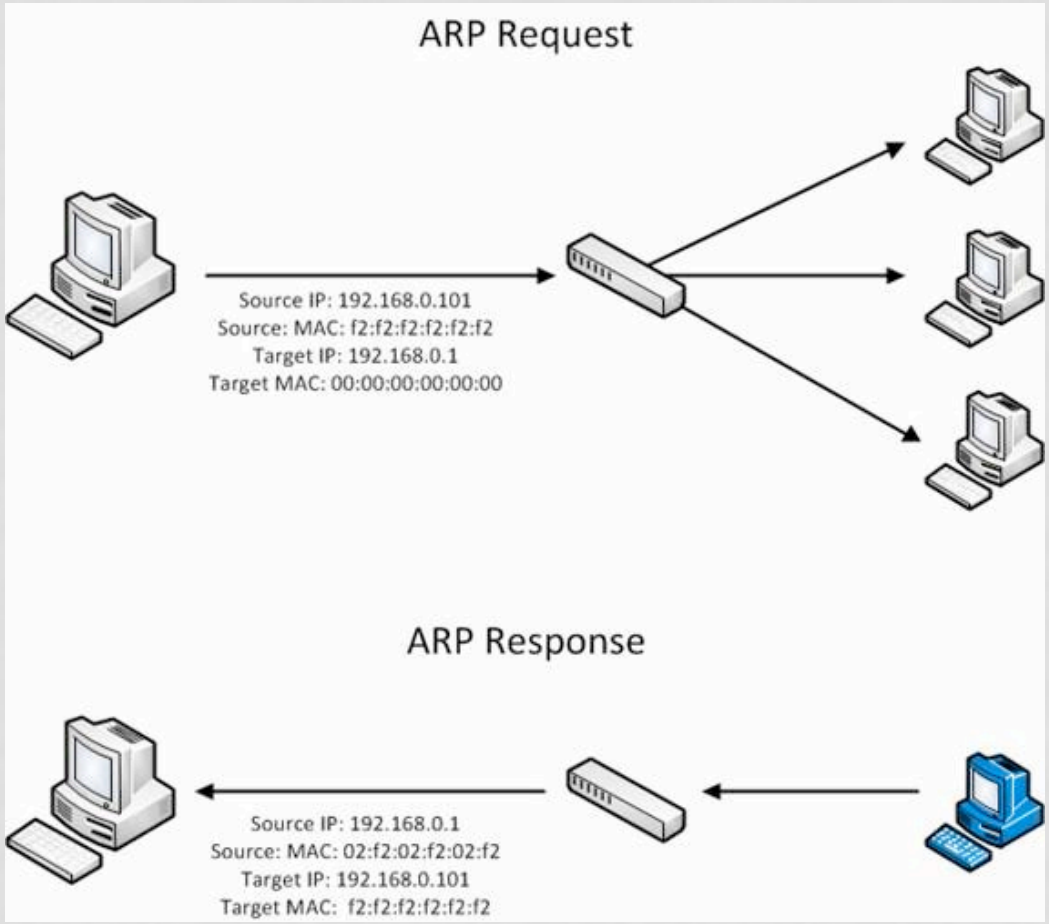
Network Security

Link Layer

Address Resolution Protocol (ARP)

- Primarily used to translate IP addresses to Ethernet MAC addresses
  - The device drive for Ethernet NIC needs to do this to send a packet
- Also used for IP over other LAN technologies, e.g. IEEE 802.11
- Each host maintains a table of IP to MAC addresses mapping.
- Message types:
  - ARP request
  - ARP reply
  - ARP announcement.

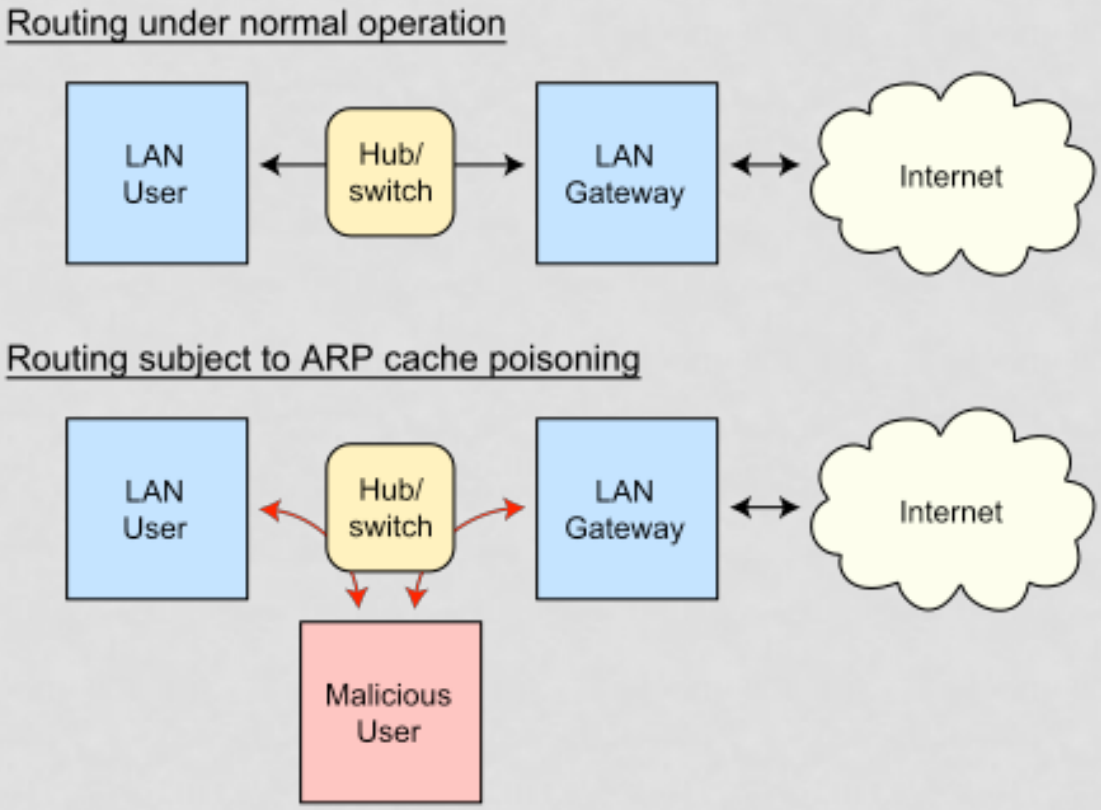
ARP Example


ARP Request
Source IP: 192.168.0.101
Source: MAC: f2:f2:f2:f2:f2:f2
Target IP: 192.168.0.1
Target MAC: 00:00:00:00:00:00
ARP Response
Source IP: 192.168.0.1
Source: MAC: 02:f2:02:f2:02:f2
Target IP: 192.168.0.101
Target MAC: f2:f2:f2:f2:f2:f2

ARP Spoofing/Poisoning

- Send fake or 'spoofed', ARP messages to an Ethernet LAN.
  - To have other machines associate IP addresses with the attacker's MAC.
  - Solution: just disable it.
- Legitimate use
  - redirect a user to a registration page before allow usage of the network.
  - Implementing redundancy and fault tolerance

ARP Spoofing/Poisoning



ARP Spoofing/Poisoning Defenses

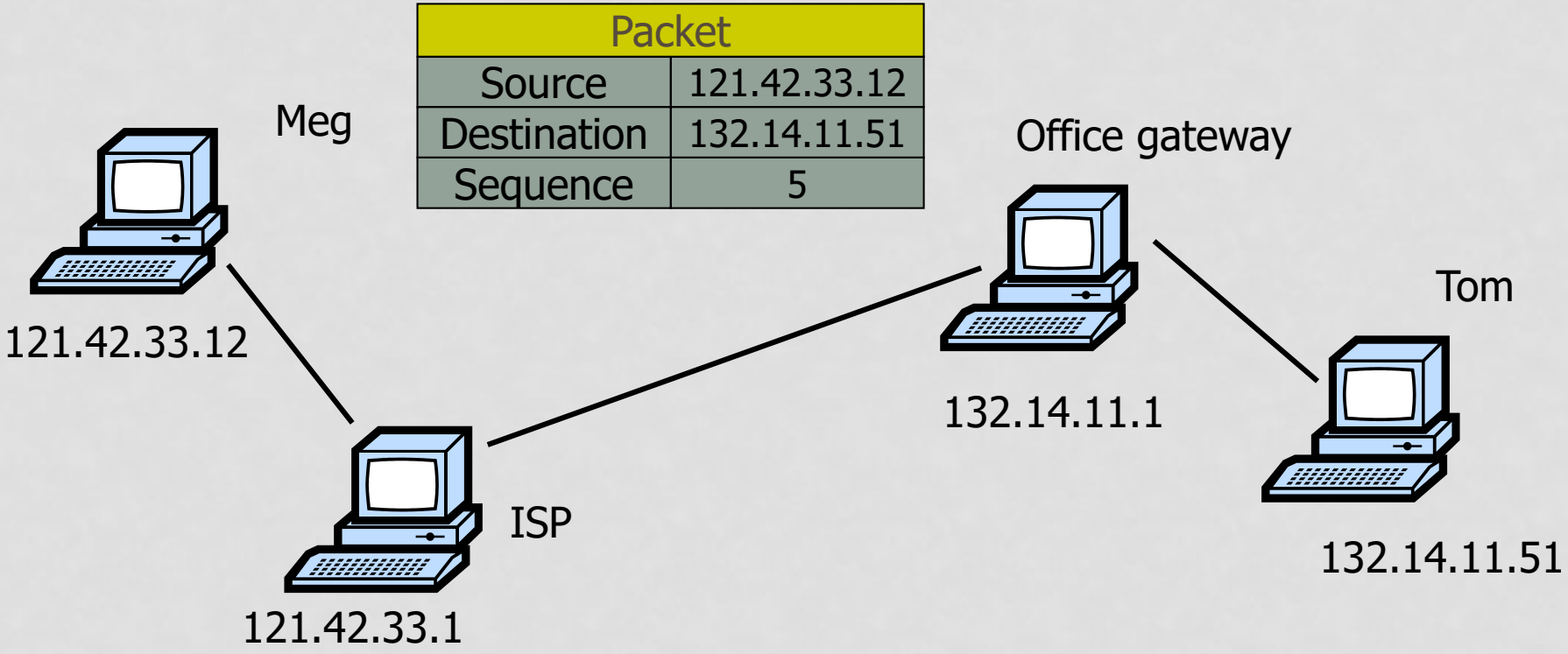
- Static ARP table
- DHCP Certification (use access control to ensure that hosts only use the IP addresses assigned to them, and that only authorized DHCP servers are accessible).
- Detection:
  - Arpwatch (sending email when updates occur),

Network Security

IP Layer

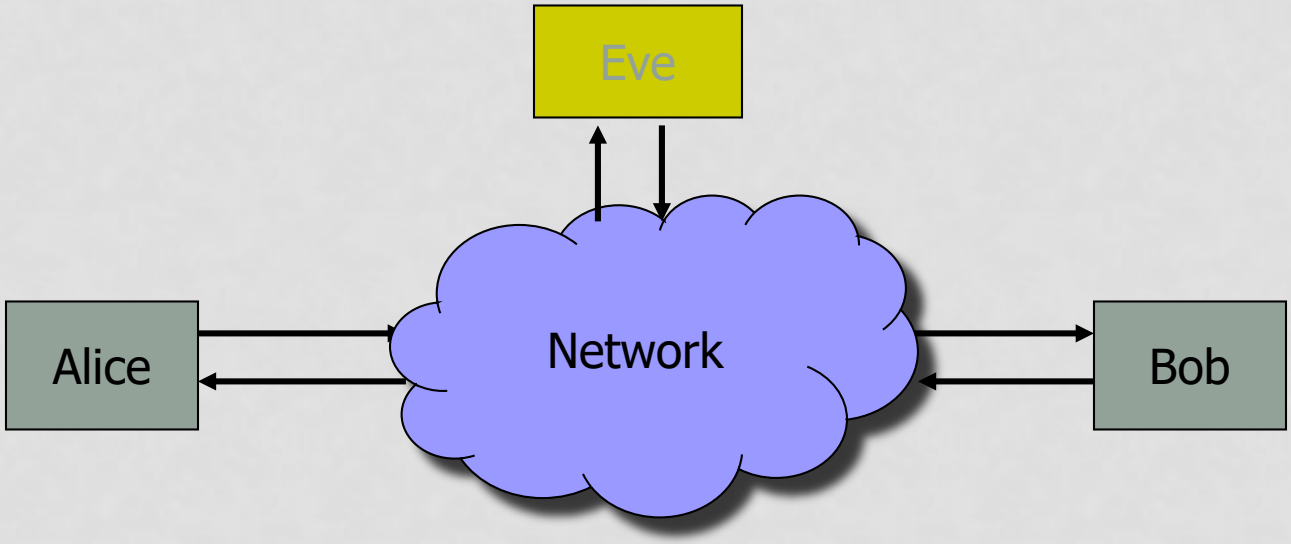
IP Routing

- Internet routing uses numeric IP address
- Typical route uses several hops



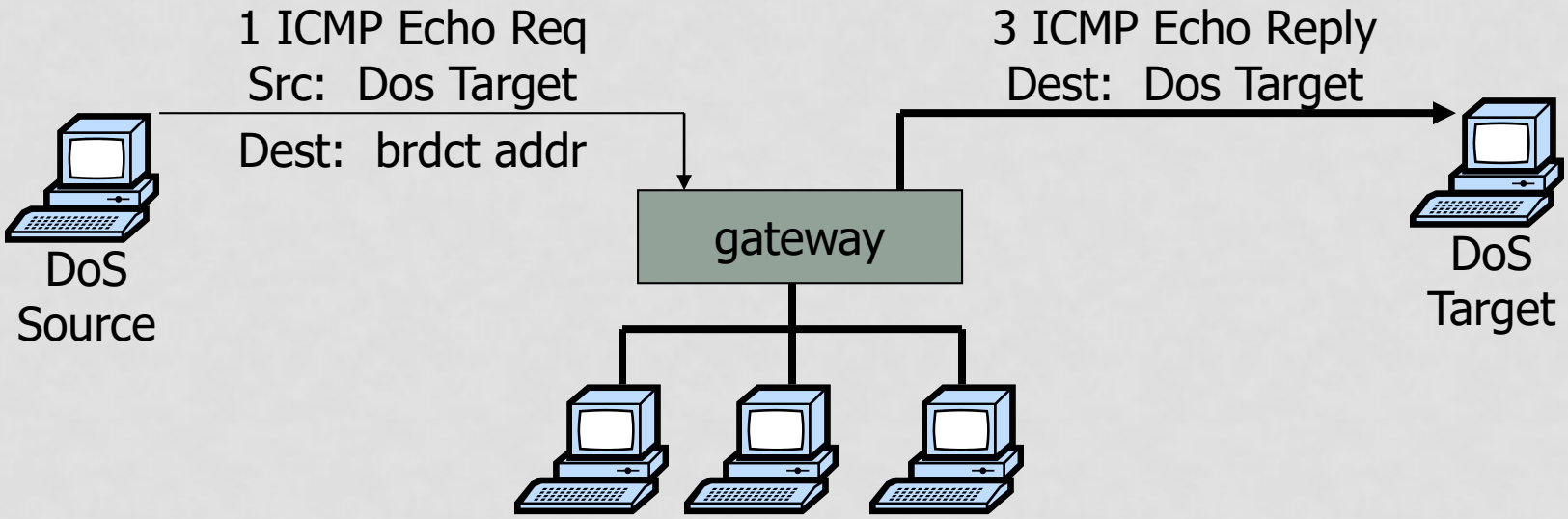
Packet Sniffing

- Promiscuous Network Interface Card reads all packets
  - Read all unencrypted data (e.g., "ngrep")
  - ftp, telnet send passwords in clear!



ICMP – Smurf DoS Attack

- Send ping request to broadcast address (ICMP Echo Req).
- Lots of responses:
  - Every host on target network generates a ping reply (ICMP Echo Reply) to victim
  - Ping reply stream can overload victim



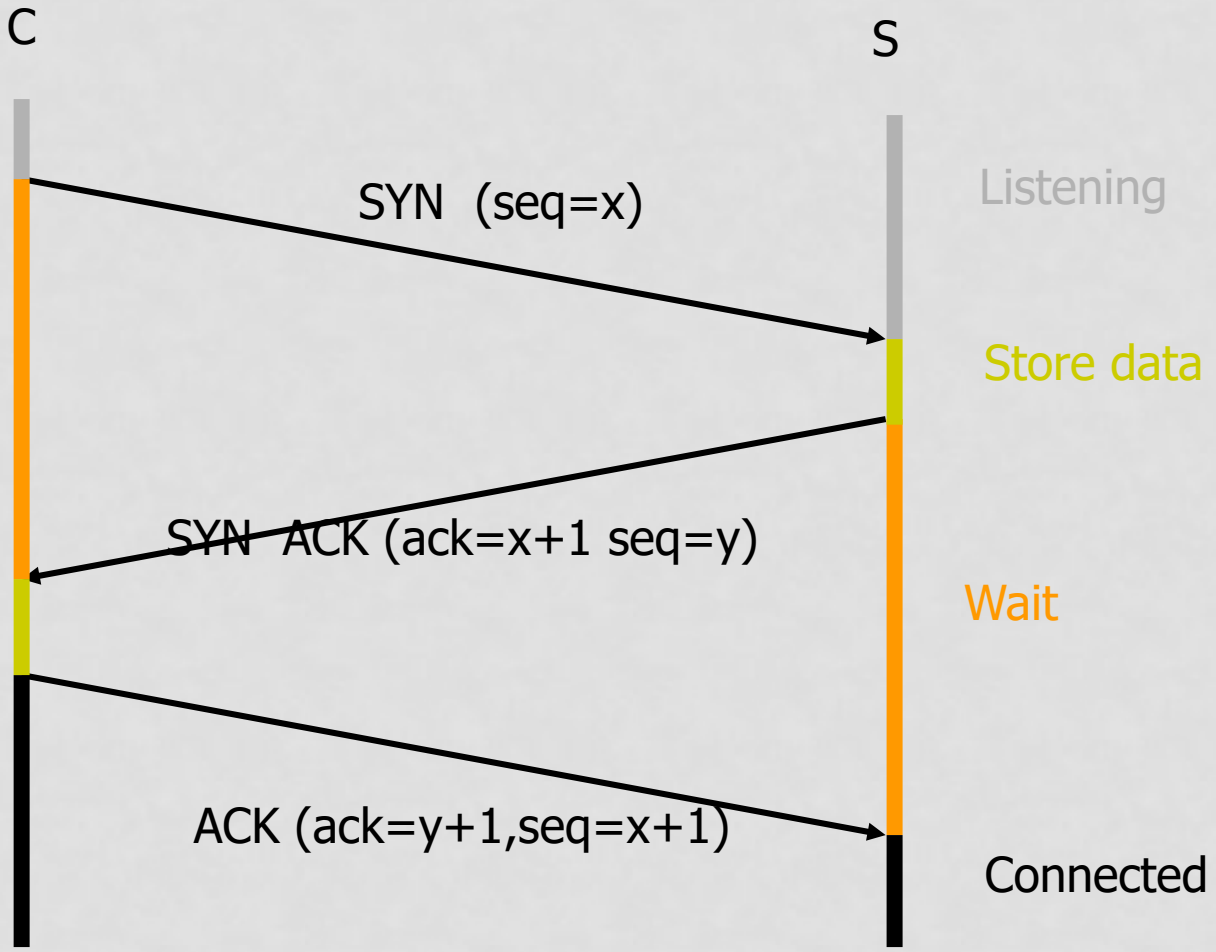
Network Security

Transport Layer

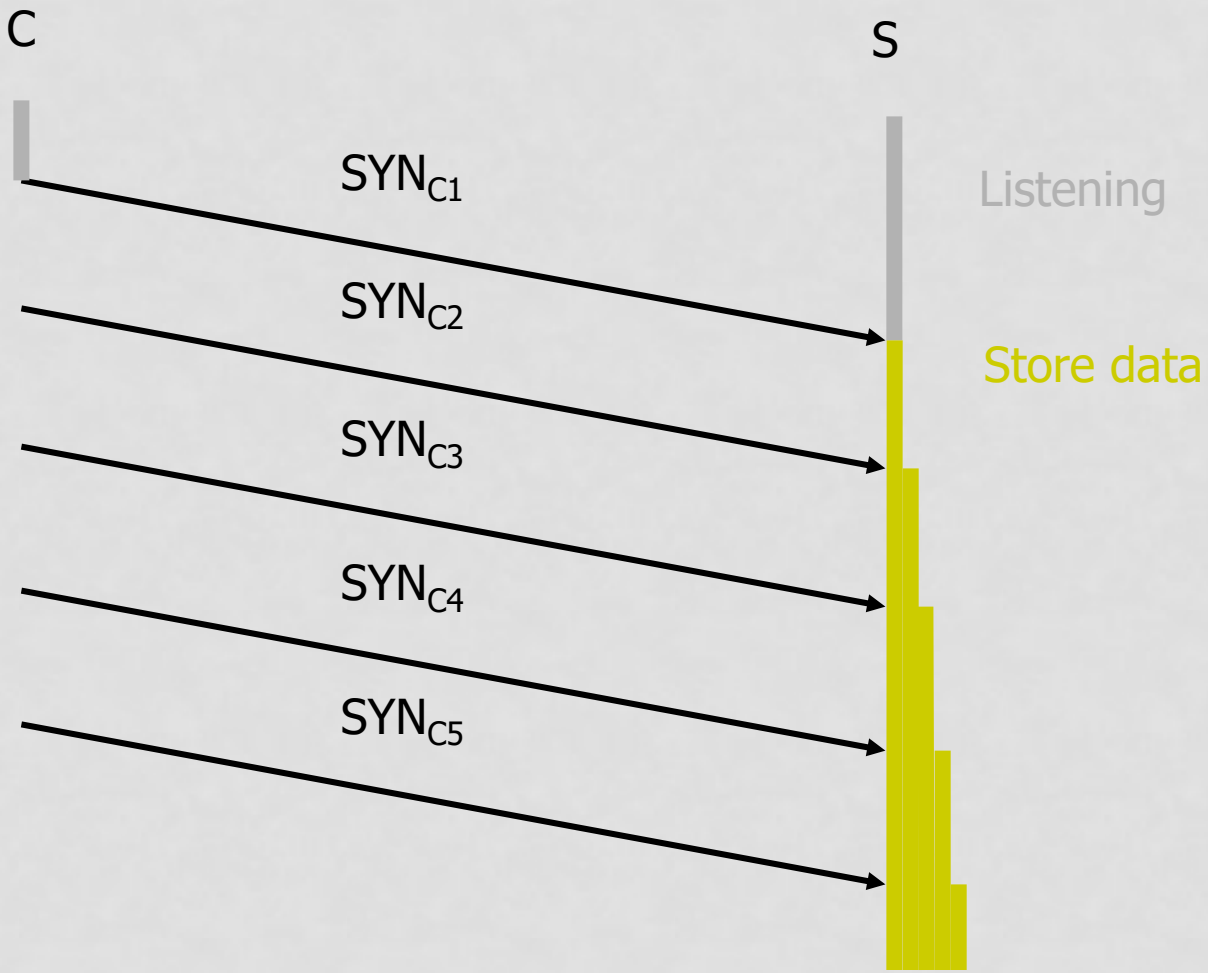
TCP vs. UDP

- Each protocol provides different guarantees.
- TCP uses 32-bits numbers.
- Sequence number has a multiple roles:
  - If the SYN flag is set,
    - then this is the initial sequence number
    - the seq. num of the actual first data byte is this seq. num + 1)
  - If the SYN flag is clear,
    - then this is the seq. number of the first data byte of this packet.
  - If the ACK flag is set,
    - then this the next sequence number that the receiver is expecting.
    - This acknowledges receipt of all prior bytes.

TCP Handshake



SYN Flooding Attack



SYN Flooding Attack

- Attacker sends many connection requests
  - Spoofed source addresses
- Victim allocates resources for each request
  - Connection requests exist until timeout
  - Old implementations have a small and fixed bound on half-open connections
- Resources exhausted ⇒ new requests rejected
- No more effective than other channel capacity-based attack today

TCP Prediction

- Attacker can predict the sequence number used in a TCP connection,
  - then counterfeit packets.
  - Blind Session Hijacking.
- Adversary do not have full control over the network (cannot read the packets), but can inject packets with fake source IP addresses.
- TCP sequence numbers are used for authenticating packets.
- Initial seq# needs high degree of unpredictability
  - If attacker knows initial seq # and amount of traffic sent, can estimate likely current values.
  - Some implementations are vulnerable.

Risks from Session Hijacking

- Inject data into an unencrypted server-to-server traffic
  - E.g. an e-mail exchange, DNS zone transfers, etc.
- Inject data into an unencrypted client-to-server traffic
  - E.g ftp file downloads, http responses.
- Denial of service attacks, such as resetting the connection.

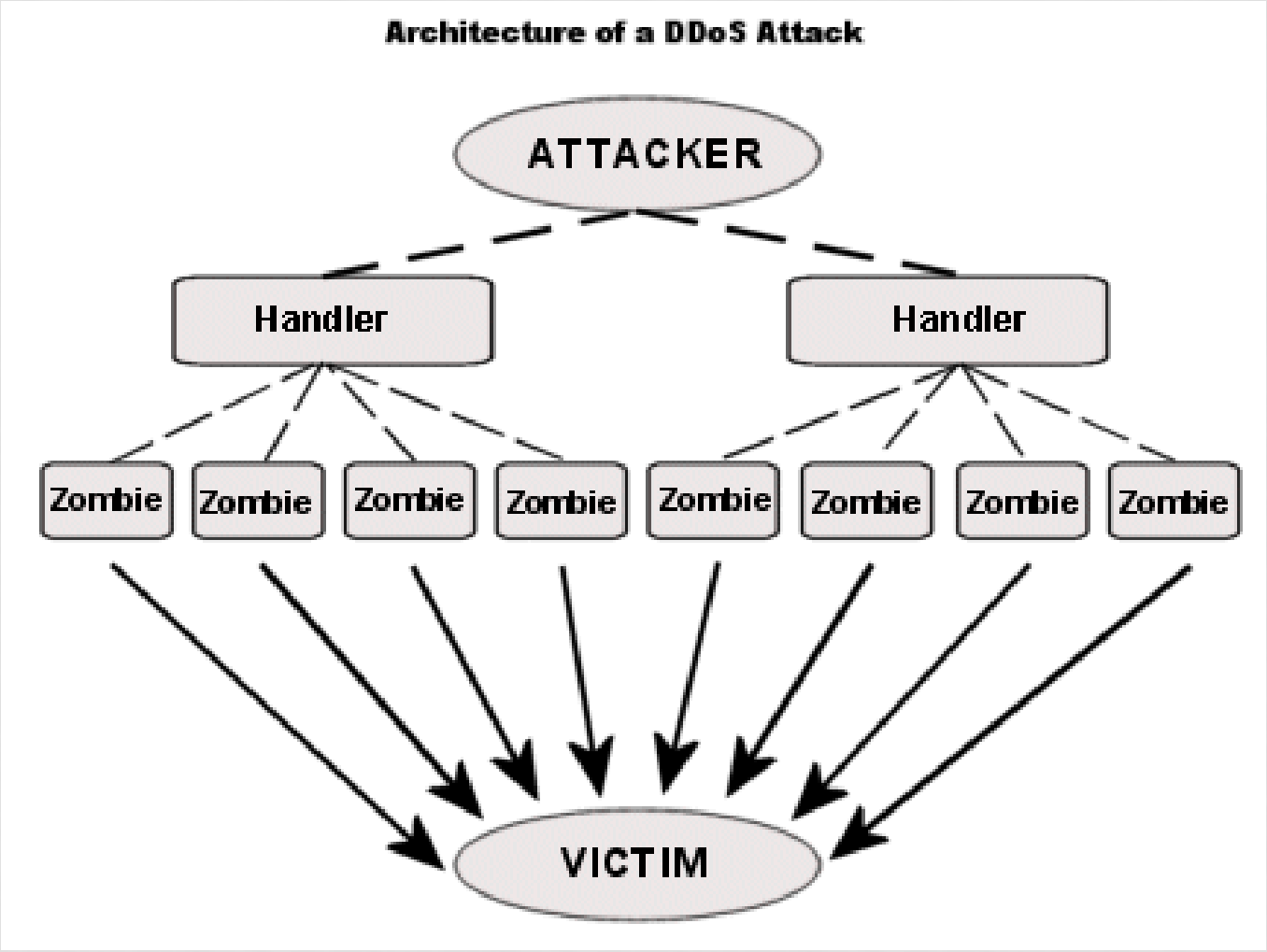
DoS Vulnerability in Session Hijacking

- Suppose attacker cannot guess seq. number for an existing connection.
  - Naively, success prob. is $1/2^{32}$ (32-bit seq. #'s).
  - Most systems allow for a large window of acceptable seq. #:
    - Higher success probability.
- Suppose attacker can guess seq. number for an existing connection:
  - Success Probability becomes significantly higher.
- Attack is most effective against long lived connections, e.g. BGP.

Network Security

Denial of Service Attacks

Distributed DoS (DDoS)



Hiding DDoS Attacks

- Reflection
  - Find big sites with lots of resources, send packets with spoofed source address, response to victim
    - PING => PING response
    - SYN => SYN-ACK
- Pulsing zombie floods
  - each zombie active briefly, then sleeps;
  - zombies taking turns attacking
  - making tracing difficult