Network Security II - IP and TCP

CSE 565 - Fall 2025
Computer Security

Hongxin Hu (hongxinh@buffalo.edu)

Updates

- **Project 2 SQL Injection Attack**
  - Deadline: Thursday, October 7
- **Assignment 2**
  - Deadline: Tuesday, October 9
- **Midterm Exam**
  - Thursday, October 16

Midterm Exam

- **Question 1: True/False questions. (10 points)**
- **Question 2: Multiple-choice questions. (20 points)**
- **Question 3: Short Answer questions. (50 points)**
- **Question 4: Lab 1 question. (10 points)**
- **Question 5: Lab 2 questions. (10 points)**

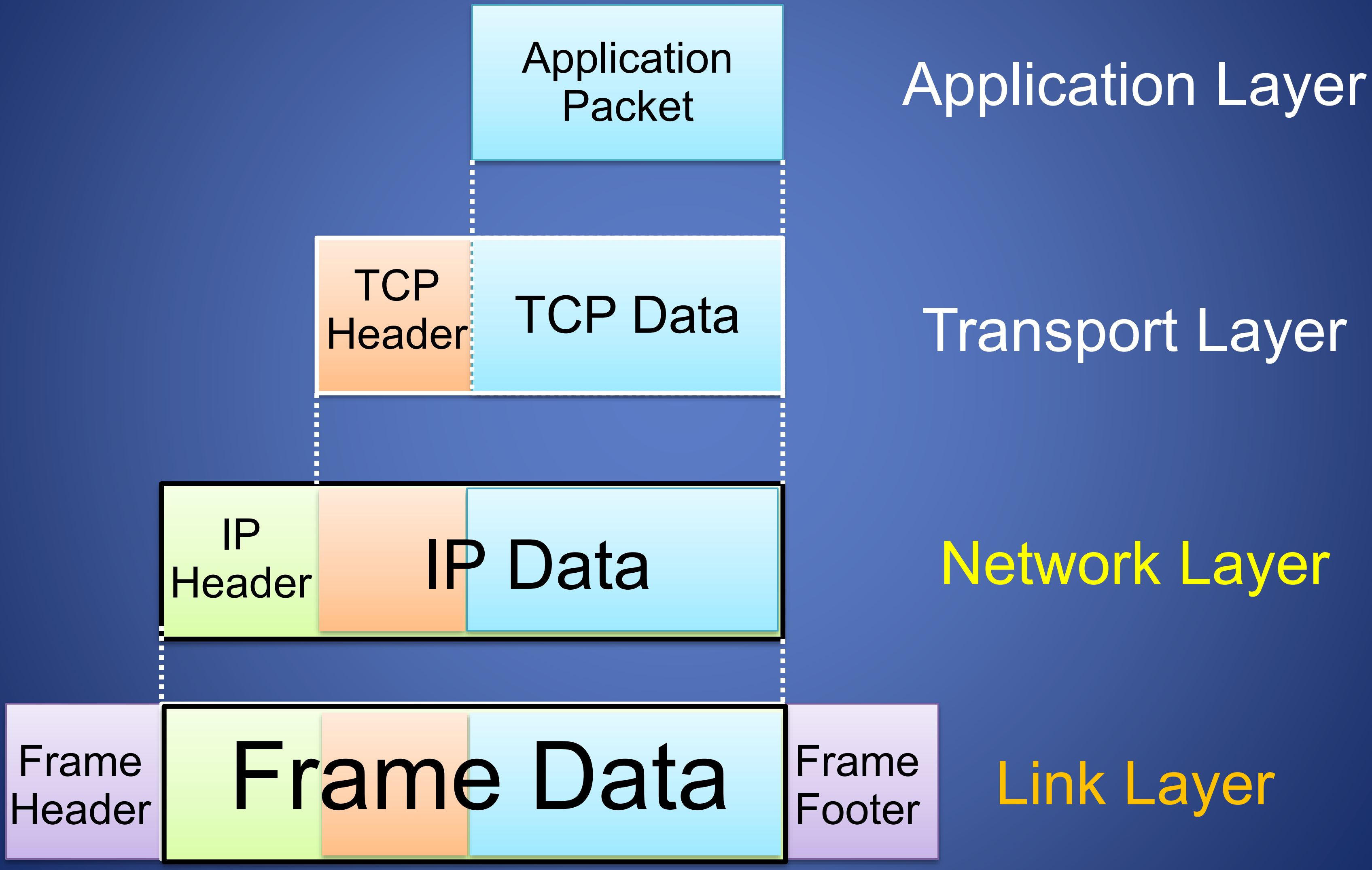
Updates

- Survey 1 Large Language Model Security
  - Deadline:
    - Thursday, October 23, 2024

Updates

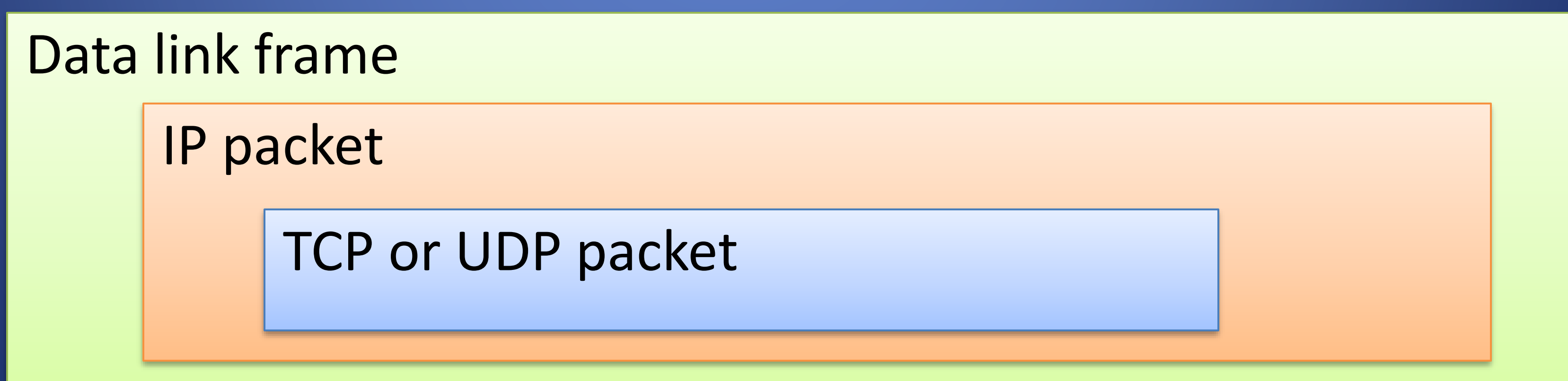
- Survey Papers
  - Structure
    - Title
    - Abstract
    - Introduction
    - Main Techniques
    - Issues and Problems
    - Future Trends
    - Reference (less than 10)
  - Page limit
    - 3-4 pages excluding references
  - Please use the following IEEE paper template to prepare your survey paper:
    - https://www.ieee.org/conferences/publishing/templates.html

Internet Communication



Internet Protocol (IP)

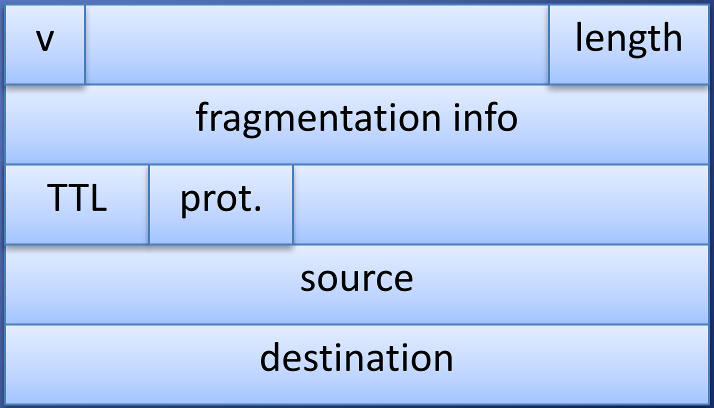
- Connectionless
  - Each packet is transported independently from other packets
- Unreliable
  - Delivery on a best effort basis
  - No acknowledgments
  - Packets may be lost, reordered, corrupted, or duplicated
- IP packets
  - Encapsulate TCP and UDP packets
  - Encapsulated into link-layer frames



IP Addresses and Packets

- IP addresses
  - IPv4: 32-bit addresses
  - IPv6: 128-bit addresses
- Address subdivided into network, subnet, and host
  - E.g., 128.148.32.110
- Broadcast addresses
  - E.g., 128.148.32.255
- Private networks
  - not routed outside of a LAN
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16

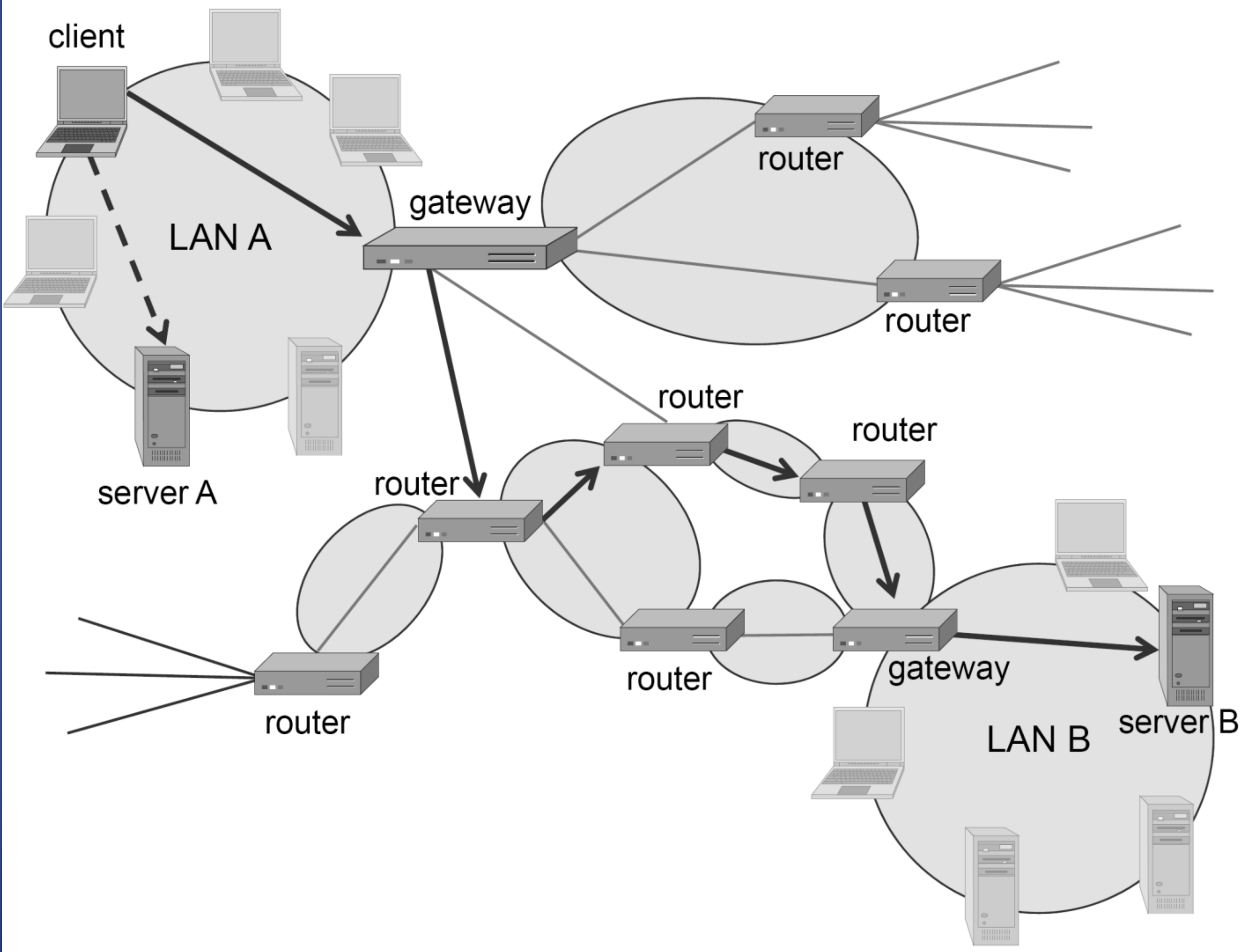
- IP header includes
  - Source address
  - Destination address
  - Packet length (up to 64KB)
  - Time to live (up to 255)
    - Hop limit
  - IP protocol version
  - Fragmentation information
  - Transport layer protocol information (e.g., TCP)



IP Routing

- A router bridges two or more networks
  - Operates at the network layer
    - Drop: if the packet is expired
    - Deliver: on one of the LANs connected
    - Forward: on different LANs
  - Maintains tables to forward packets to the appropriate network
  - Forwarding decisions based solely on the destination address
- Routing table
  - Maps ranges of addresses to LANs or other gateway routers

Routing on the Internet



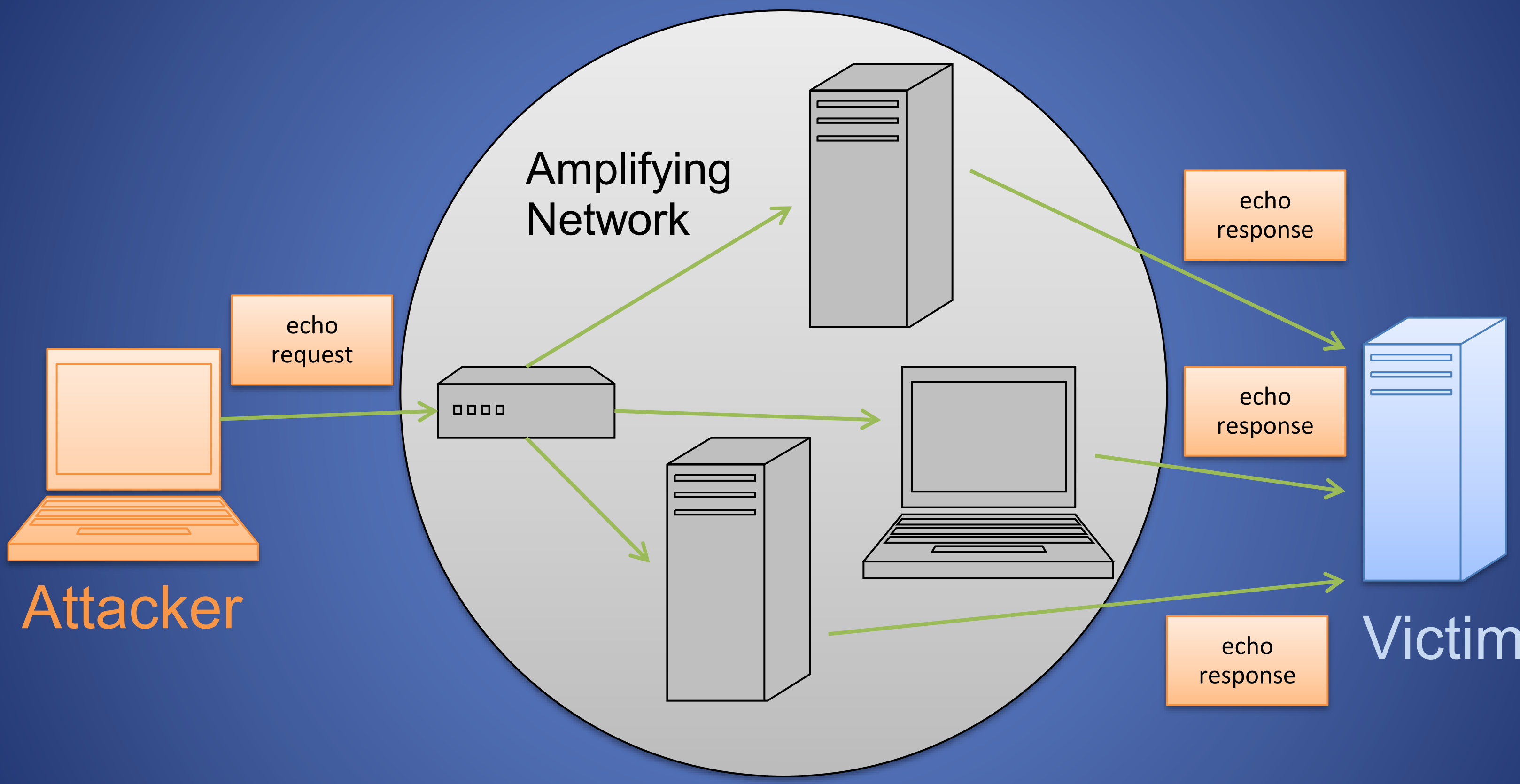
Internet Routes

- Internet Control Message Protocol (ICMP)
  - Used for network testing and debugging
  - Simple messages encapsulated in single IP packets
    - Echo request (sender); echo response (reciever)
  - Considered a network layer protocol
- Tools based on ICMP
  - Ping: sends series of echo request messages and provides statistics on roundtrip times and packet loss
  - Traceroute: sends series ICMP packets with increasing TTL value to discover routes

ICMP Attacks

- Ping of death
  - ICMP specifies messages must fit a single IP packet (64KB)
  - Send a ping packet that exceeds maximum size using IP fragmentation
  - Reassembled packet caused several operating systems to crash due to a buffer overflow
- Ping Flood
  - Send a massive amounts of echo requests to a single victim server
- Smurf
  - Ping a broadcast address using a spoofed source address

Smurf Attack



- Use a misconfigured network to amplify traffic intended to overwhelm the bandwidth of a target

IP Vulnerabilities

- Unencrypted transmission
  - Eavesdropping possible at any intermediate host during routing
- No source authentication
  - Sender can spoof source address, making it difficult to trace packet back to attacker
- No integrity checking
  - Entire packet, header and payload, can be modified while route to destination, enabling content forgeries, redirections, and man-in-the-middle attacks
- No bandwidth constraints
  - Large number of packets can be injected into network to launch a denial-of-service attack
  - Broadcast addresses provide additional leverage

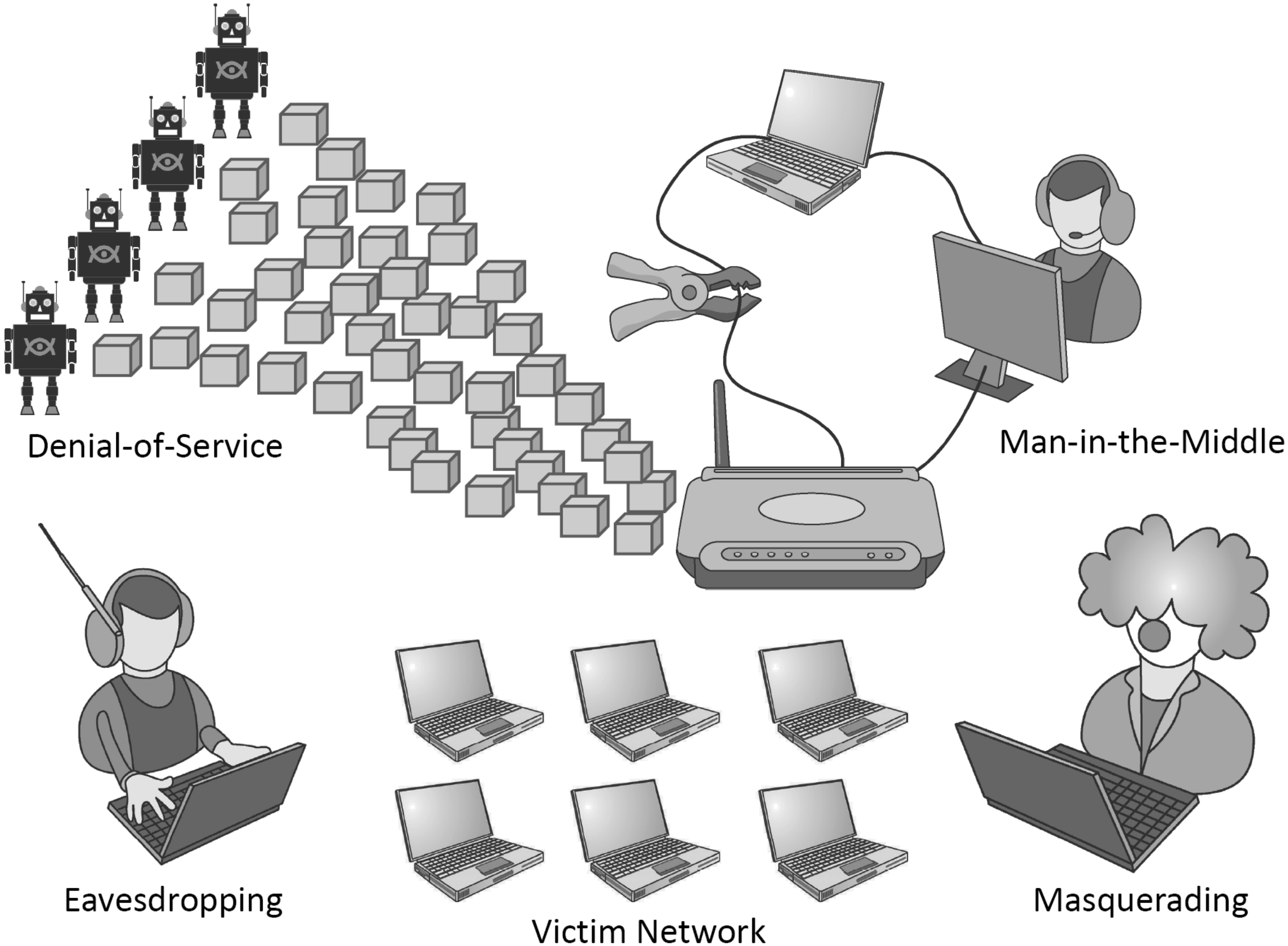
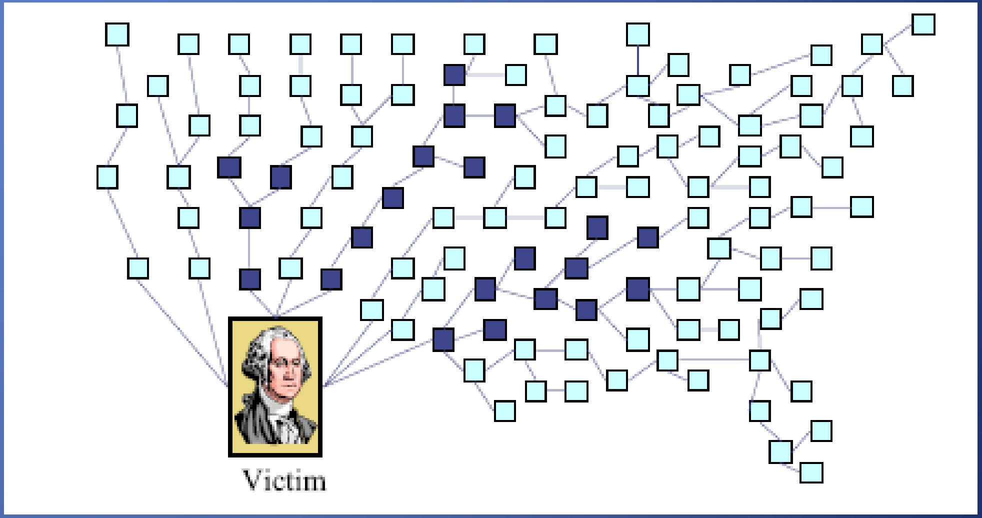


Figure 5.4: Some network-based attacks.

Denial of Service Attack

- Send large number of packets to host providing service
  - Slows down or crashes host
  - Often executed by botnet
- Attack propagation
  - Starts at zombies
  - Travels through tree of internet routers rooted
  - Ends at victim
- IP source spoofing
  - Hides attacker
  - Scatters return traffic from victim

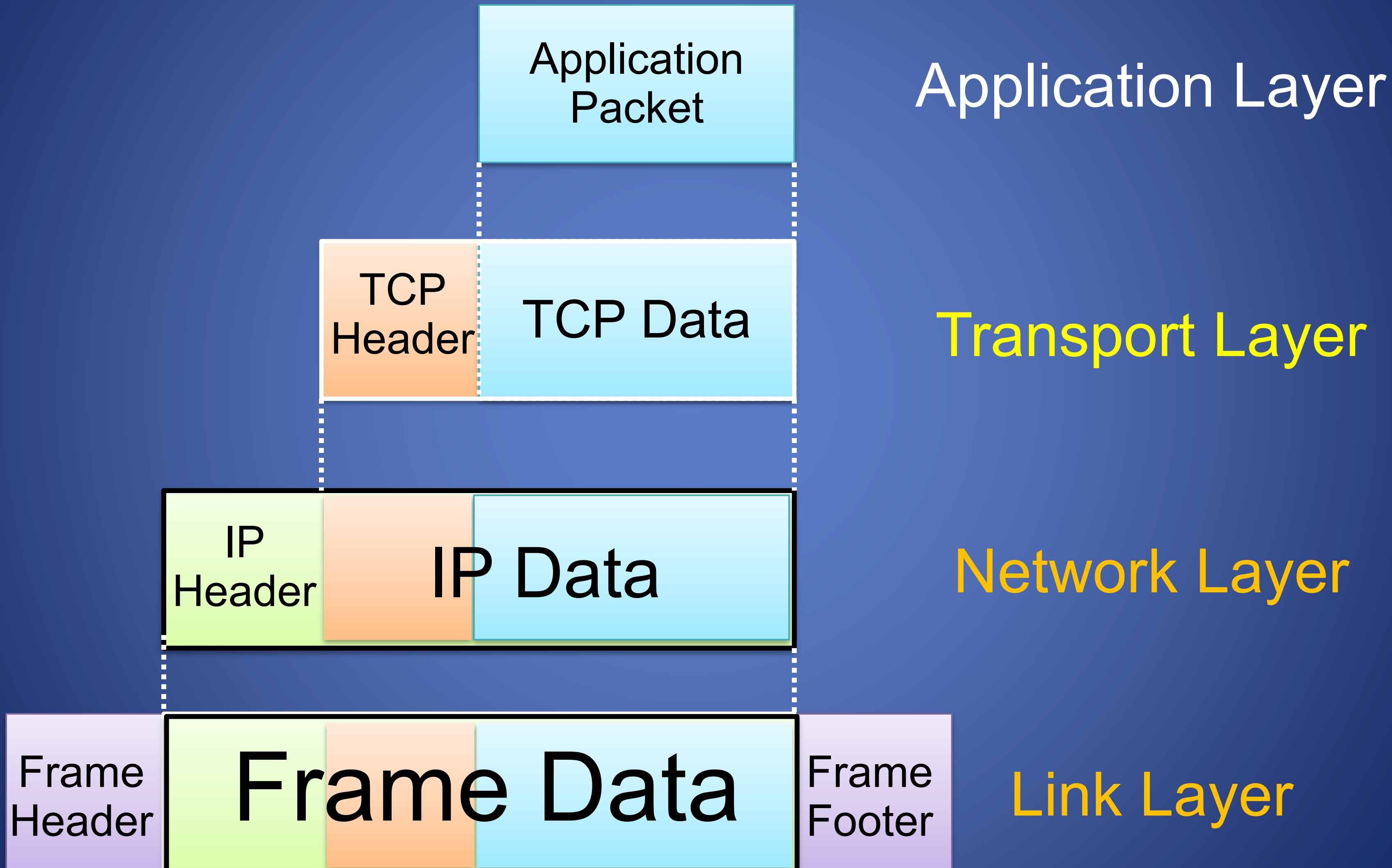
Source:
M.T. Goodrich, Probabalistic Packet Marking for Large-Scale IP Traceback, IEEE/ACM Transactions on Networking 16:1, 2008.



IP Traceback

- Problem
  - How to identify leaves of DoS propagation tree
- Issues
  - There are more than 2M internet routers
  - Attacker can spoof source address
  - Attacker knows that traceback is being performed
- Approaches
  - Filtering and tracing (immediate reaction)
  - Messaging (additional traffic)
  - Logging (additional storage)
  - Probabilistic marking

Internet Communication



Transmission Control Protocol

- TCP is a transport layer protocol guaranteeing reliable data transfer, in-order delivery of messages and the ability to distinguish data for multiple concurrent applications on the same host
  - Most popular application protocols, including WWW, FTP and SSH are built on top of TCP

- TCP takes a stream of 8-bit byte data, packages it into appropriately sized segment and calls on IP to transmit these packets
- Delivery order is maintained by marking each packet with a sequence number
- Every time TCP receives a packet, it sends out an ACK to indicate successful receipt of the packet.
- TCP generally checks data transmitted by comparing a checksum of the data with a checksum encoded in the packet

Ports

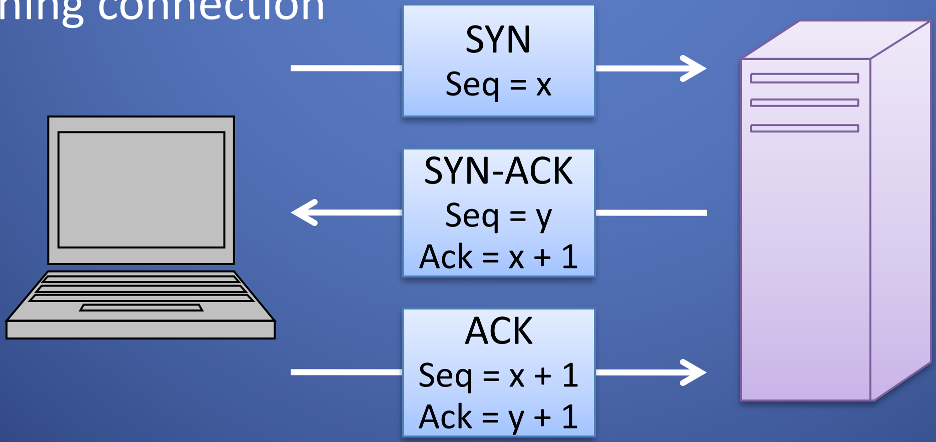
- TCP supports multiple concurrent applications on the same server
- Accomplishes this by having ports, 16 bit numbers identifying where data is directed
  - The TCP header includes space for both a source and a destination port, thus allowing TCP to route all data
  - In most cases, both TCP and UDP use the same port numbers for the same applications
    - Ports 0 through 1023 are reserved for use by known protocols.
    - Ports 1024 through 49151 are known as user ports, and should be used by most user programs for listening to connections and the like
    - Ports 49152 through 65535 are private ports used for dynamic allocation by socket libraries

TCP Packet Format

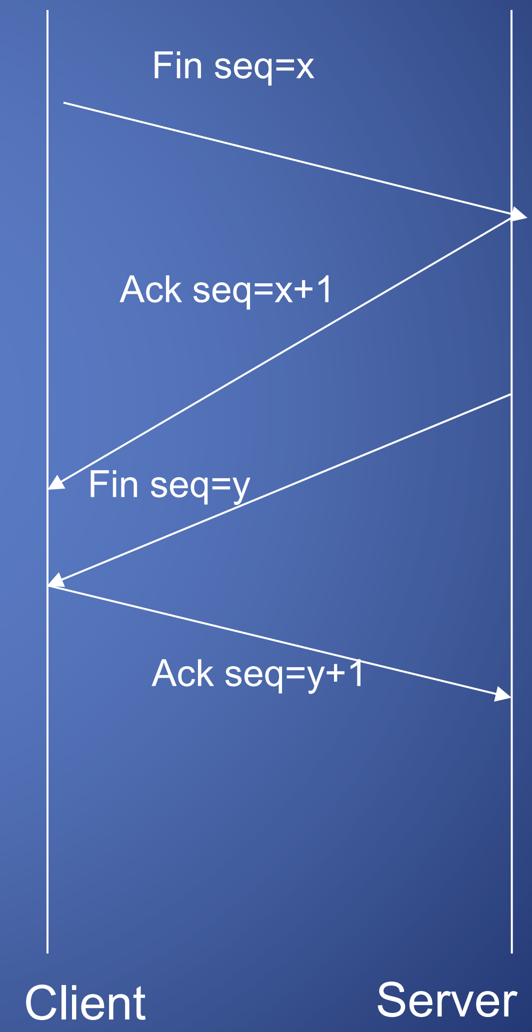
Bit Offset	0-3	4-7	8-15	16-18	19-31
0	**Source Port**			**Destination Port**	
32	**Sequence Number**				
64	**Acknowledgment Number**				
96	Offset	Reserved	Flags	**Window Size**	
128	Checksum			Urgent Pointer	
160	Options				
>= 160	Payload				

Establishing TCP Connections

- TCP connections are established through a three way handshake.
  - The server generally has a passive listener, waiting for a connection request
  - The client requests a connection by sending out a SYN (synchronization) packet
  - The server responds by sending a SYN/ACK packet, indicating an acknowledgment for the connection
  - The client responds by sending a **concluding** ACK to the server thus establishing connection



TCP Data Transfer and Teardown

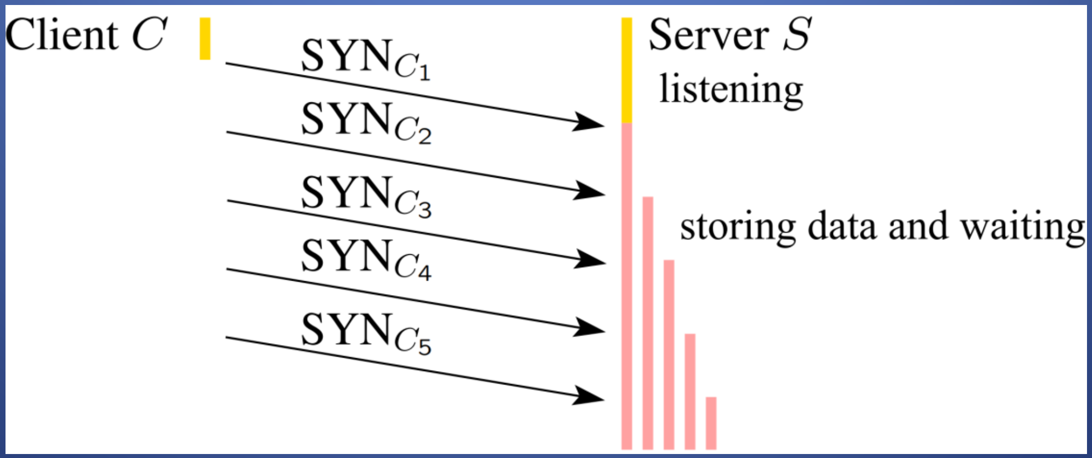


DoS Attack: SYN Flood

- Typically DOS attack can be combined with other attack such as TCP hijacking
- Rely on sending TCP connection requests faster than the server can process them
  - Attacker creates a large number of packets with spoofed source addresses and setting the SYN flag on these
  - The server responds with a SYN/ACK for which it never gets a response (waits for about 3 minutes each)
  - Eventually the server stops accepting connection requests (full memory), thus triggering a denial of service.
    - Can be solved in multiple ways
    - One of the common way to do this is to use SYN cookies

DoS Attack: SYN Flood

- TCP SYN flooding attack exploits the fact that server waits for ACKs
  - attacker sends many SYN requests with spoofed source addresses
  - victim allocates resources for each request
    - connection requests exist until timeout
    - there is a fixed bound on half-open connections



DoS Attack: SYN Flood

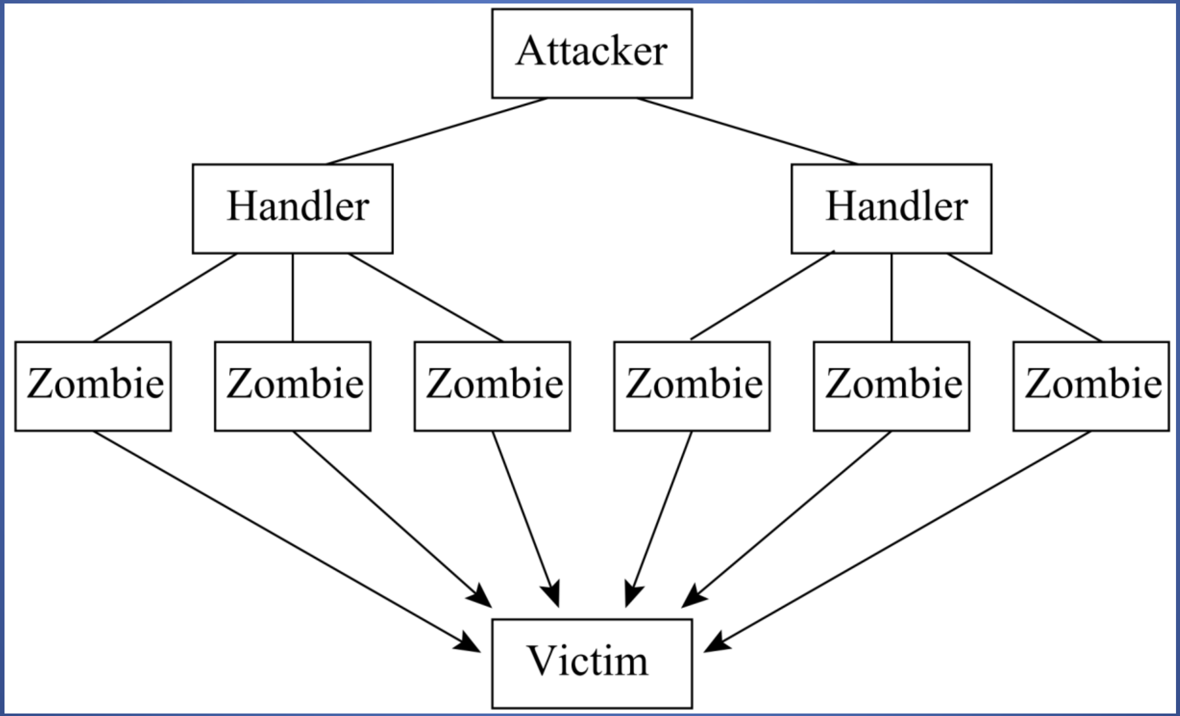
- TCP SYN flooding attack (cont.)
  - resources exhausted ⇒ legitimate requests rejected
  - the attack relies on the fact that many SYN-ACK packets will be unanswered
    - an existing host replies to a SYN-ACK packet with RST
    - many IP addresses are not in use
  - the attacker needs to keep sending new SYN packets to keep the table full
- Flooding attacks in general can use any type of packets
  - e.g., ICMP flood, UDP flood, TCP SYN flood
- In any attack with spoofed addresses, it is hard to find attacker

DDoS Attacks

- In all of the above attacks, attacker needs to have substantial resources
  - thus attacks are more effective if carried out from many sources
  - they are called distributed DoS (DDoS) attacks
- DDoS attacks often use compromised computers (zombies)
  - attacker compromised machines and builds a botnet
  - attacker instructs the bots to attack the target machine
  - all communication is often encrypted, can be authenticated
  - zombie machines flood the victim
  - spoofing IP addresses is not necessary since it is hard to trace the attacker from the zombie machines

DDoS Attacks

- DDoS attack illustrated



Defenses Against DoS Attacks

- A significant challenge in defending against DoS attacks is that spoofed addresses are used
- What can be done
  - ingress filtering
    - basic recommendation to check that packets coming from a network have source address within the network's range
    - ISPs are best suited to perform such filtering
    - despite its simplicity and effectiveness, this recommendation is not implemented by many ISPs

Defenses Against DoS Attacks

- DoS defenses (cont.)
  - SYN cookies
    - this technique is used to defend against TCP SYN floods
    - after receiving a SYN, information about it is not stored the server
    - instead it is encoded in the SYN-ACK packet
    - upon receiving ACK, server can reconstruct all information
    - disadvantages: increased server computation
  - blocking certain packets
    - many systems block ICMP echo requests from outside of network
    - often IP broadcasts are also blocked from outside

Defenses Against DoS Attacks

- DoS defenses (cont.)
  - limiting packet rates
    - certain types of packets such as ICMP are rather rare in normal network operation
    - limiting their rate can help mitigate attacks
  - packet marking
    - a router marks a small number of packets with its ID
    - for high volume traffic, packets will be marked by most servers on their path to the victim
    - path to the attacker can be reconstructed
    - effectiveness of this technique depends on its wide usage
  - general good security practices

TCP Session Hijacking

- A security attack over a protected network
- Attempt to take control of a network session
  - Sessions are server keeping state of a client’s connection
  - Servers need to keep track of messages sent between client and the server and their respective actions

- Most networks follow the TCP/IP protocol
- IP Spoofing is one type of hijacking on large network

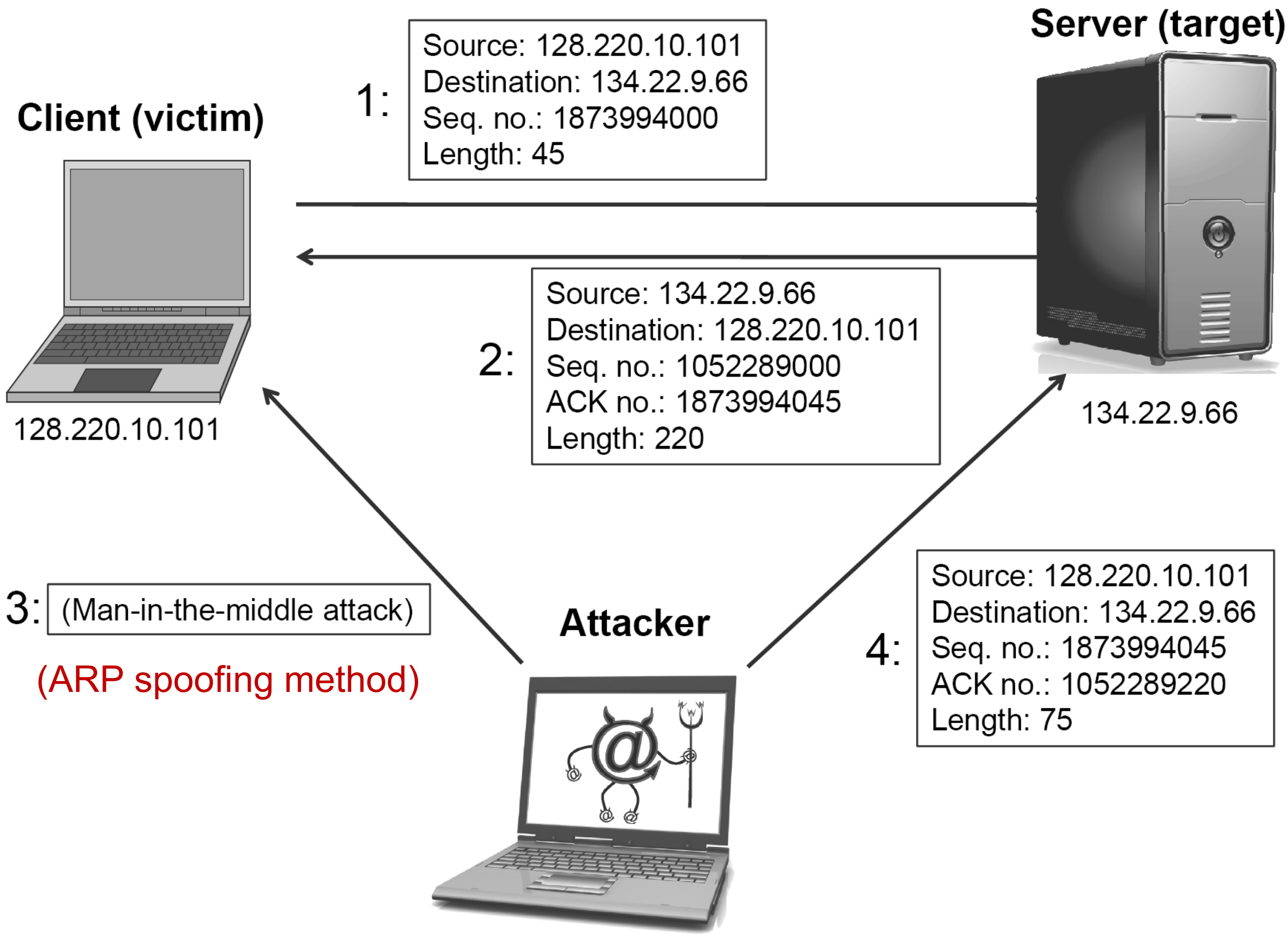


Figure 5.18: A TCP session hijacking attack.

IP Spoofing

- IP Spoofing is an attempt by an intruder to send packets from one IP address that appear to originate at another
- If the server thinks it is receiving messages from the real source after authenticating a session, it could inadvertently behave maliciously
- There are two basic forms of IP Spoofing
    - Blind Spoofing
        – Attack from any source
    - Non-Blind Spoofing
        – Attack from the same subnet

Packet Sniffers

- Packet sniffers "read" information traversing a network
  - Packet sniffers intercept network packets, possibly using ARP cache poisoning
  - Can be used as legitimate tools to analyze a network
    - Monitor network usage
    - Filter network traffic
    - Analyze network problems
  - Can also be used maliciously
    - Steal information (i.e. passwords, conversations, etc.)
    - Analyze network information to prepare an attack
- Packet sniffers can be either software or hardware based
  - Sniffers are dependent on network setup

Packet Sniffers - Wireshark

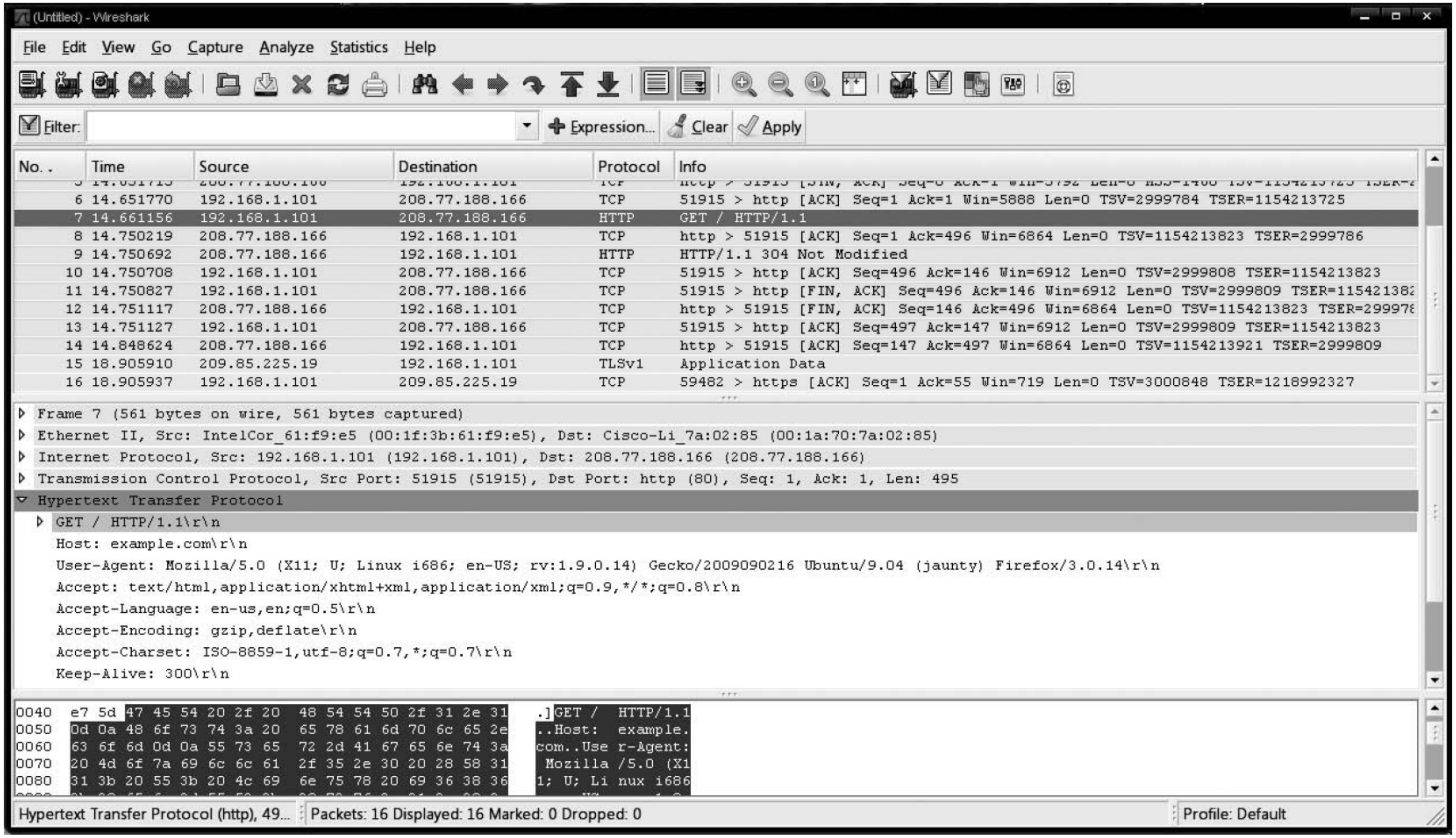


Figure 5.13: An example use of the Wireshark packet-sniffing tool. Here, the packet associated with an HTTP request to www.example.com has been captured and analyzed.

Detecting Sniffers

- Sniffers are almost always passive
  - They simply collect data
  - They do not attempt “entry” to “steal” data
- This can make them extremely hard to detect
  - Most detection methods require suspicion that sniffing is occurring
    - Then some sort of “ping” of the sniffer is necessary
    - It should be a broadcast that will cause a response only from a sniffer
  - Another solution on switched hubs is ARP watch
    - An ARP watch monitors the ARP cache for duplicate entries of a machine
    - If such duplicates appear, raise an alarm
    - Problem: false alarms
      - Specifically, DHCP networks can have multiple entires for a single machine

- To reduce the impact of packet sniffing, encryption mechanisms should be utilized in higher-level protocols to prevent attackers from recovering sensitive data

Stopping Packet Sniffing

- The best way is to encrypt packets securely
  - Sniffers can capture the packets, but they are meaningless
    - Capturing a packet is useless if it just reads as garbage
  - SSH is also a much more secure method of connection
    - Private/Public key pairs makes sniffing virtually useless

- On switched networks, almost all attacks will be via ARP spoofing
  - Add machines to a permanent store in the cache
  - This store cannot be modified via a broadcast reply
  - Thus, a sniffer cannot redirect an address to itself

- The best security is to not let them in the first place
  - Sniffers need to be on your subnet in a switched hub in the first place
  - Any solution for wireless networks?

User Datagram Protocol

- UDP is a stateless, unreliable datagram protocol built on top of IP, that is it lies on level 4
- It does not provide delivery guarantees, or acknowledgments, but is significantly faster
- Can however distinguish data for multiple concurrent applications on a single host.

- A lack of reliability implies applications using UDP must be ready to accept a fair amount of error packages and data loss. Some application level protocols such as TFTP build reliability on top of UDP.
  - Most applications used on UDP will suffer if they have reliability. VoIP, Streaming Video and Streaming Audio all use UDP.

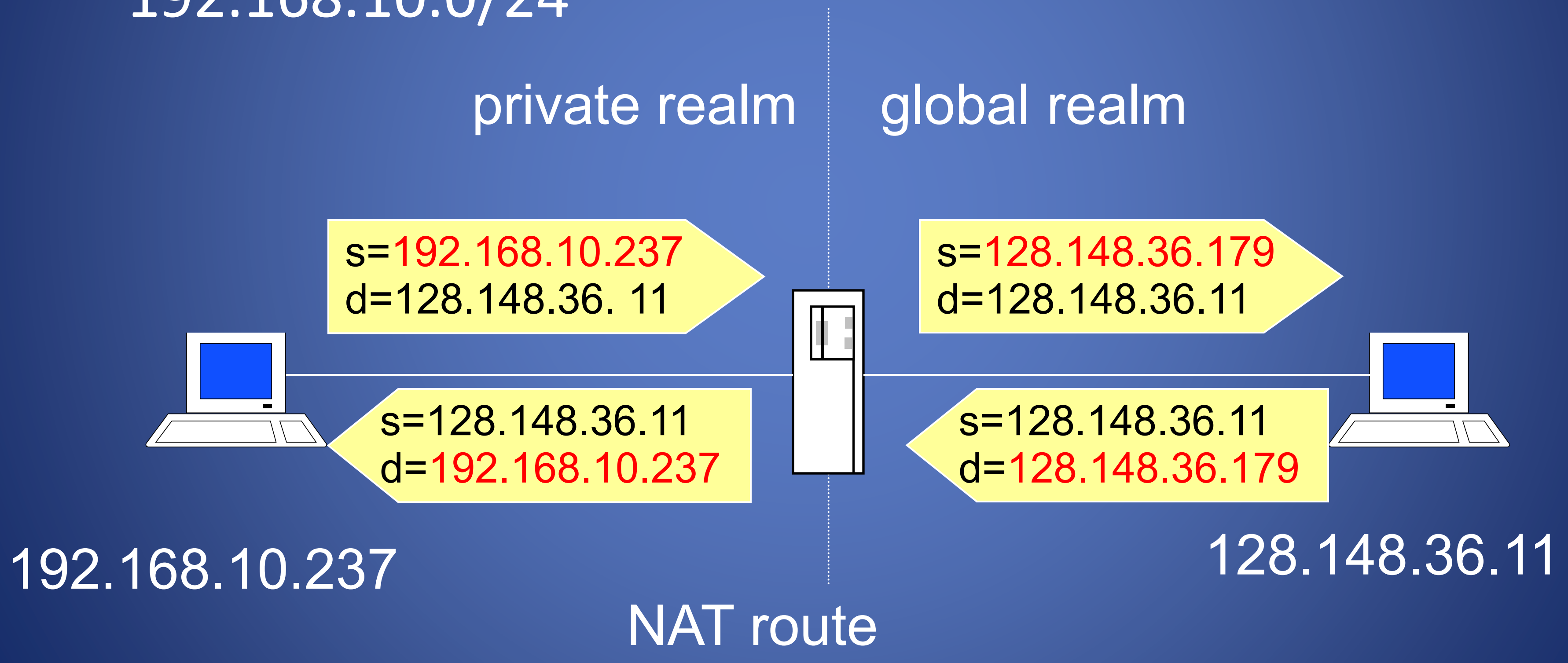
Network Address Translation(NAT)

- Introduced in the early 90s to alleviate IPv4 address space congestion
- Relies on translating addresses in an internal network, to an external address that is used for communication to and from the outside world
  - NAT is usually implemented by placing a router in between the internal *private* network and the *public* network.

- Saves IP address space since not every terminal needs a globally unique IP address, only an organizationally unique one

Translation

- Router has a pool of private addresses 192.168.10.0/24



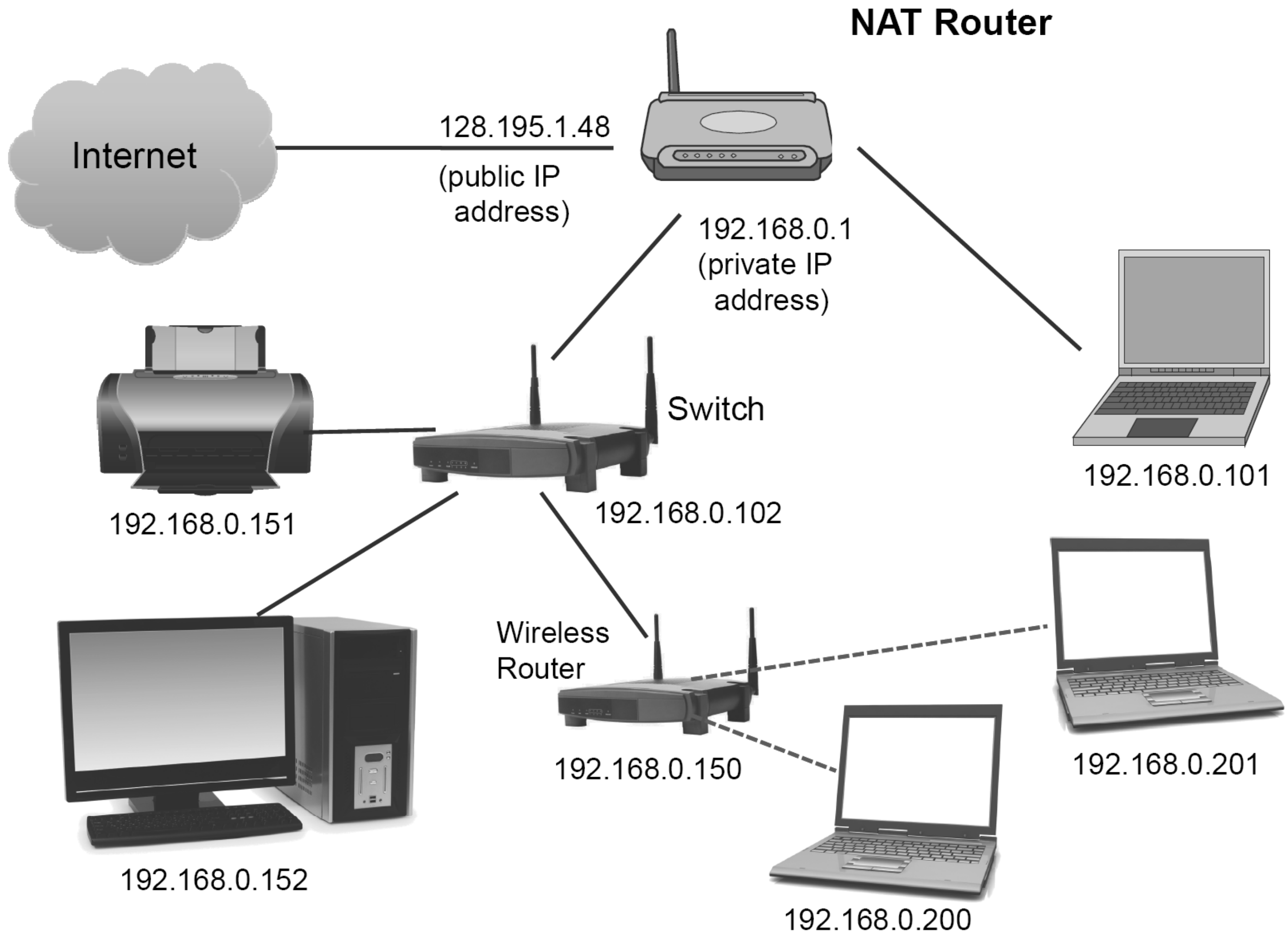


Figure 5.17: An example home network setup using a NAT router.

Questions & Suggestions?