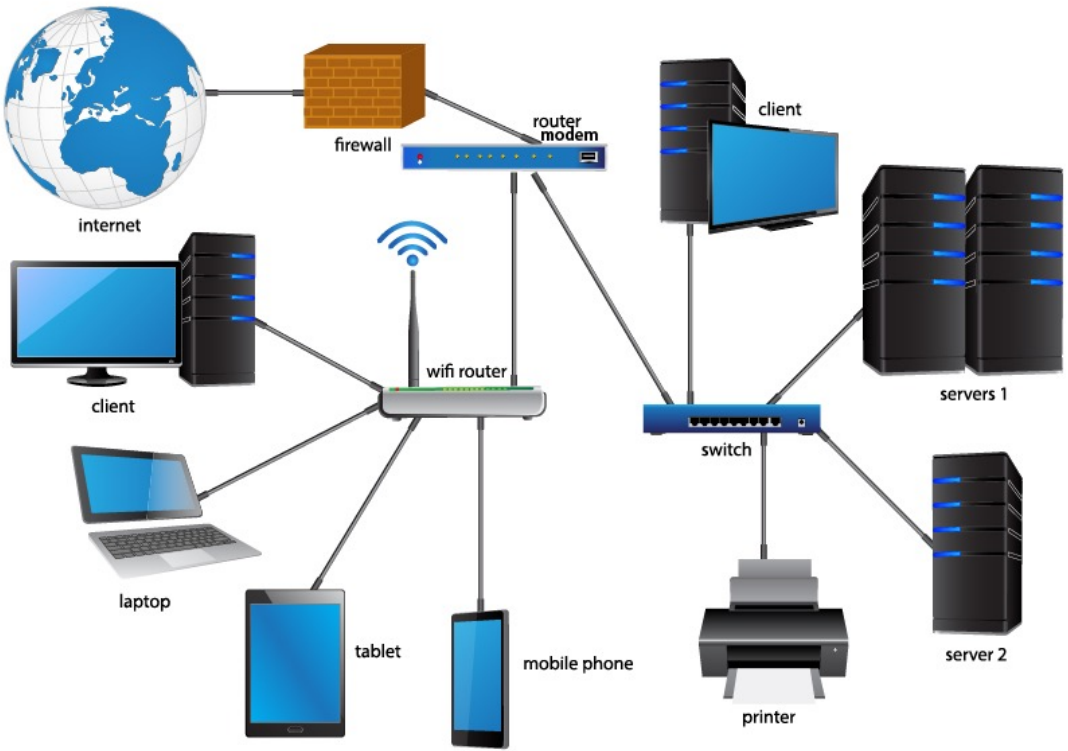
CS 4910: Intro to Computer Security

Network Security II: Network Attacks

Instructor: Xi Tan

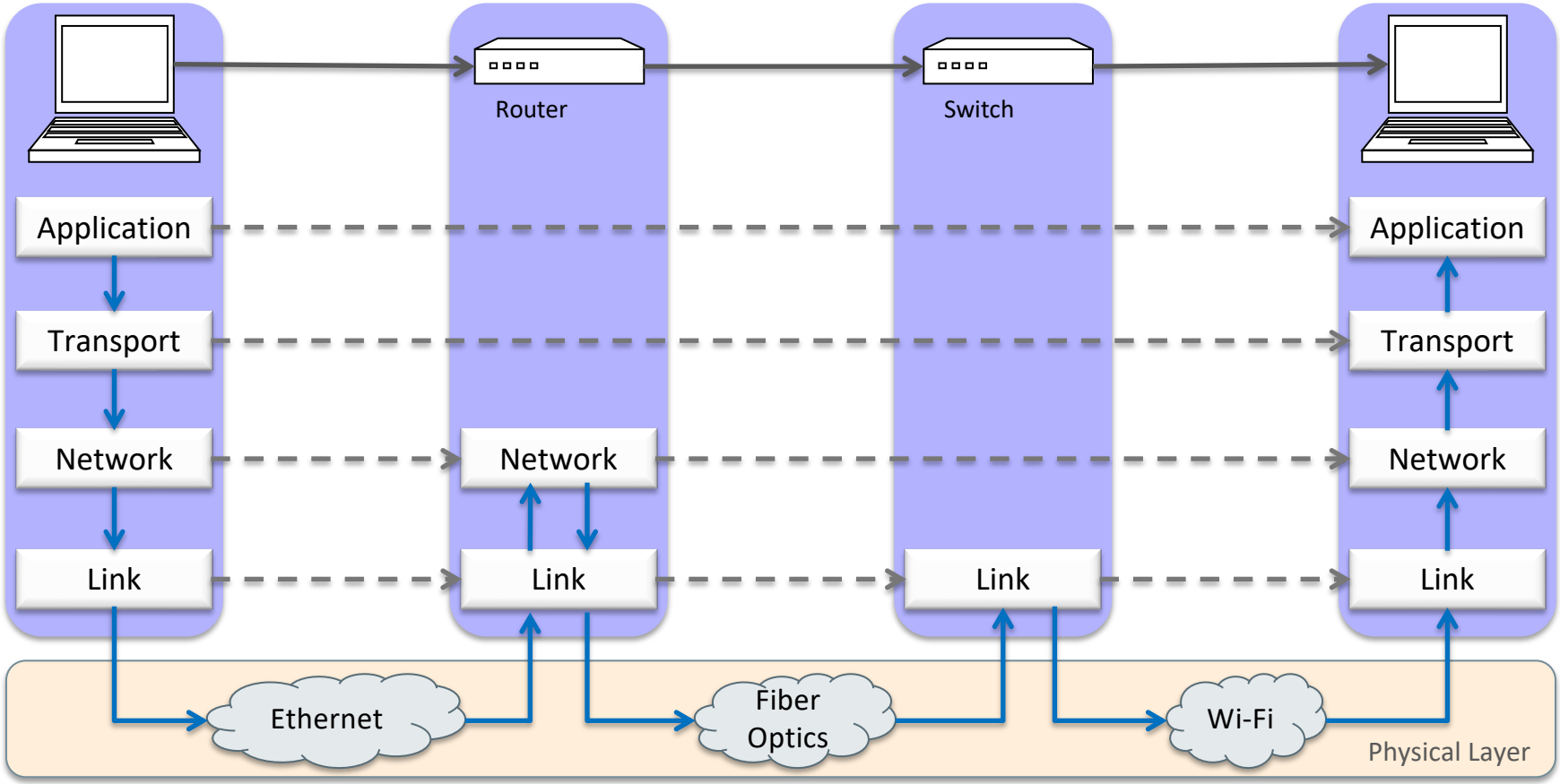
Recall: What is A Computer Network?



A computer network is a collection of computers and other devices connected together to communicate and share resources.

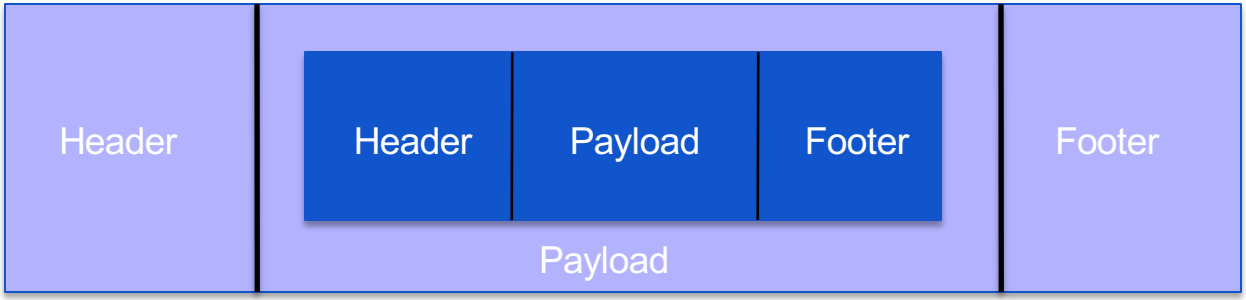
Figure is from: https://integrinetit.com/what-is-a-computer-network/

Recall: Network Layers

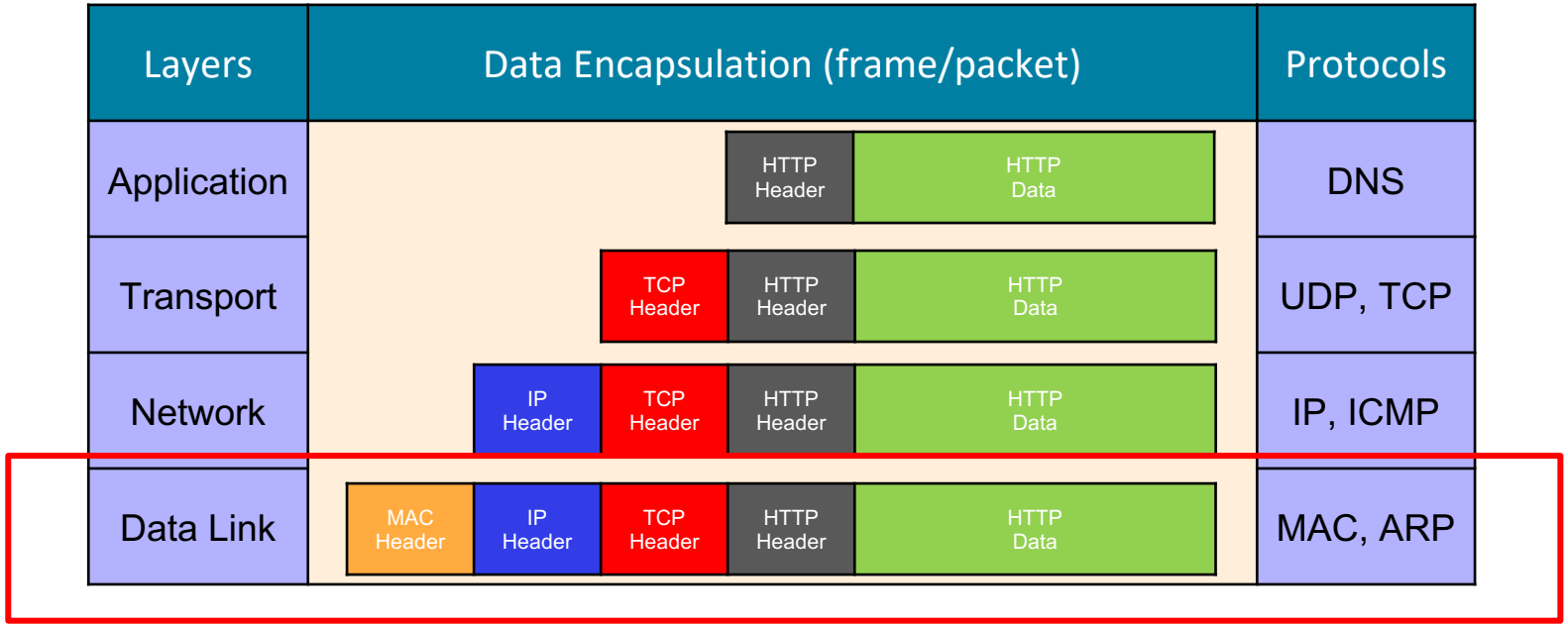


Recall: Encapsulation

- A packet typically consists of
  - Control information for addressing the packet: header and footer
  - Data: payload
- A network protocol N1 can use the services of another network protocol N2
  - A packet p1 of N1 is encapsulated into a packet p2 of N2
  - The payload of p2 is p1
  - The control information of p2 is derived from that of p1



Recall: Internet Communication



MAC spoofing, ARP spoofing

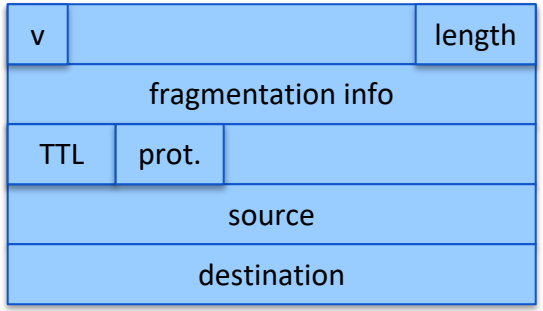
Today

- MAC Spoofing, ARP Spoofing
- IP Spoofing
- Denial of Service
- DNS Cache Poisoning

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

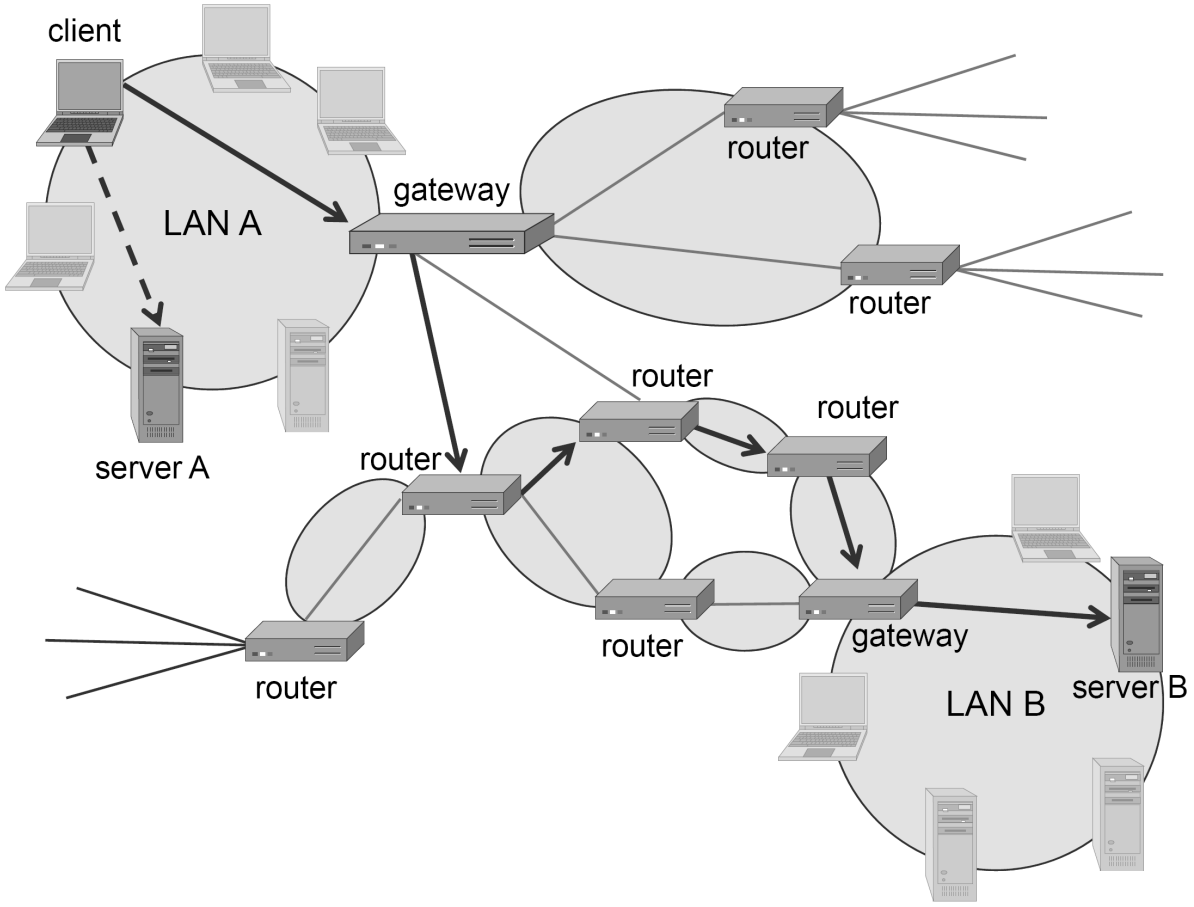
- IP header includes
  - Source address
  - Destination address
  - Packet length (up to 64KB)
  - Time to live (up to 255)
    - Hop limit
  - IP protocol version
  - Fragmentation information
  - Transport layer protocol information (e.g., TCP)



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

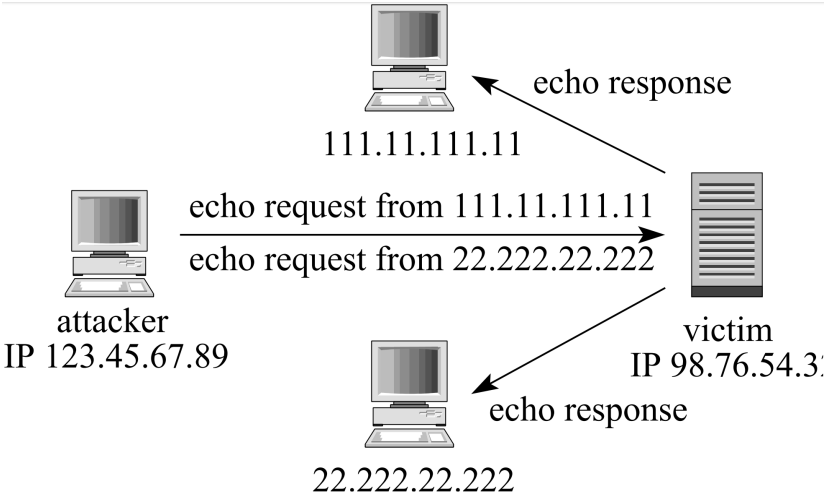


IP Vulnerabilities

- 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

IP Spoofing

- With sufficient privileges to a machine, the source address in IP packets can be set to anything
- The source address is set to a randomly chosen address
- Replies from the victim machine are scattered across the internet



IP Spoofing Prevention

- Ingress and Egress Filtering
  - Ingress Filtering: Configure routers or firewalls to block packets with source IP addresses that are outside the range of valid IP addresses for incoming traffic.
  - Egress Filtering: Prevent outgoing packets from leaving the network with a spoofed source IP address.

- Reverse Path Forwarding (uRPF)
  - Enables routers to verify the reachability of the source IP address by checking the routing table.

Denial of Service (DoS) Attacks

- Denial of service attacks target at denying availability of some service or resource, including
  - Network bandwidth
    - relates to the capacity of the network links connecting a server to the Internet
    - for most organizations, this is their connection to their Internet Service Provider (ISP)
  - System resources
    - aims to overload or crash the network handling software
  - Application resources
    - typically involves a number of valid requests, each of which consumes significant resources and thus limiting the ability of the server to respond to requests from other users

DoS Attacks

- Types of DoS attacks

	stopping services	exhausting resources
local	process crashing process killing system reconfiguration	spawning processes to fill process table filling up file system saturating bandwidth
remote	malformed packets to crash buggy services	packet floods

DoS Attacks

- Basic form of DoS
  - Attacker sends a large number of packets through a link or to a particular service
  - The goal is to saturate the network or overload the server
  - Most requests from legitimate users will be dropped

- Example:
  - Flooding attack: ICMP Flood, SYN Flood, etc.
  - Distributed DoS (DDoS)
  - Other DoS Attacks

DoS Attacks – Flooding Attack

- Flooding attack: attackers send **a very high volume of traffic** to a system so that it cannot examine and allow permitted network traffic

- Flooding attacks in general can use any type of packets
  - e.g., ICMP flood, TCP SYN flood, UDP flood
- In any attack with spoofed addresses, it is hard to find attacker

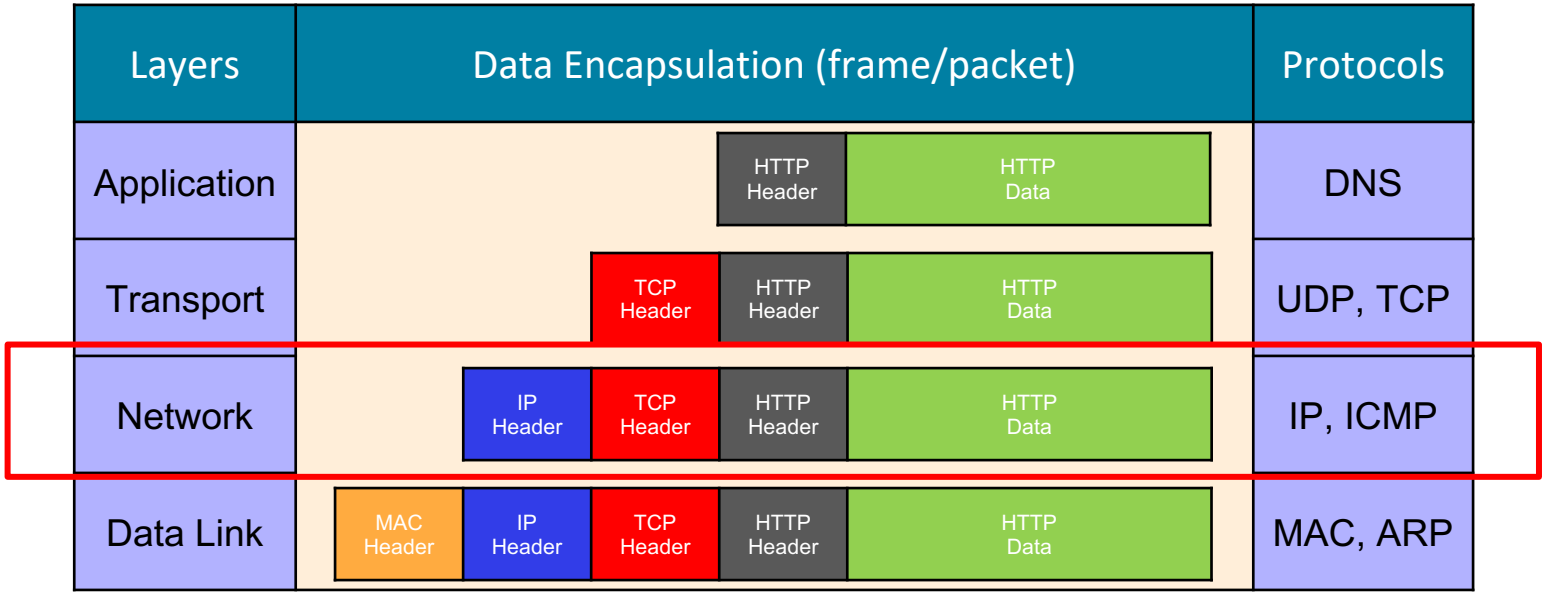
Internet Routes

- 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

DoS Attacks – ICMP Flood

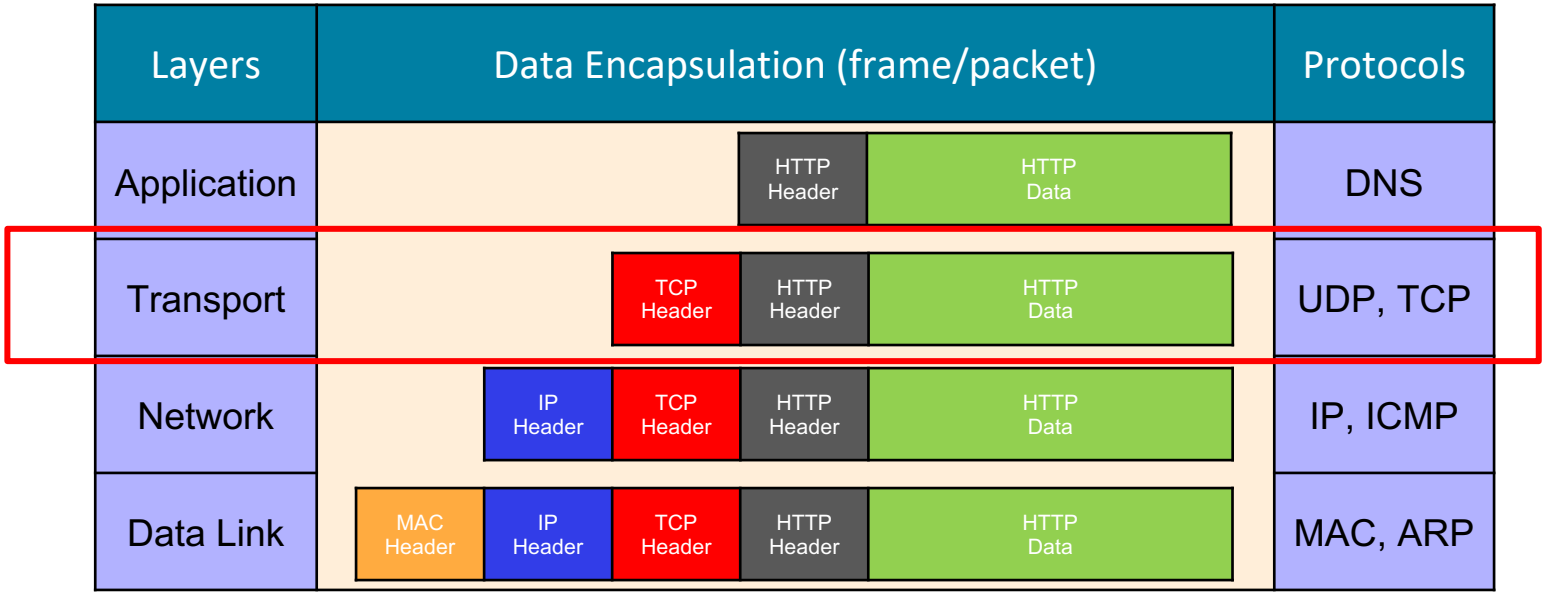
- Ping of death
  - ICMP specifies messages must fit a single IP packet (64KB)
  - Send a ping packet that exceeds maximum size using IP fragmentation
  - Reassembled packet caused several operating systems to crash due to a buffer overflow
- Ping Flood
  - Send a massive amounts of echo requests to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

So far …



IP spoofing, ICMP flood

Next


Layers
Data Encapsulation (frame/packet)
Protocols
Application
HTTP Header
HTTP Data
DNS
Transport
TCP Header
HTTP Header
HTTP Data
UDP, TCP
Network
IP Header
TCP Header
HTTP Header
HTTP Data
IP, ICMP
Data Link
MAC Header
IP Header
TCP Header
HTTP Header
HTTP Data
MAC, ARP

UDP and TCP

- UDP: User Datagram Protocol
  - transport protocol with minimal guarantees
    - no acknowledgment, no flow control, no message continuation
  - traffic is separated by port number
- TCP: Transmission Control Protocol
  - connection-oriented transport protocol
  - partitions data into packets and reassembles them in correct order at the destination
  - transmission is reliable
    - packets are acknowledged and retransmitted if necessary
  - port numbers are used for different services as well

UDP

- UDP is a stateless, unreliable datagram protocol built on top of IP
- It does not provide delivery guarantees, or acknowledgments, but is significantly faster
- Distinguish data for multiple concurrent applications on a single host via ports

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

DoS Attack – UDP Flood

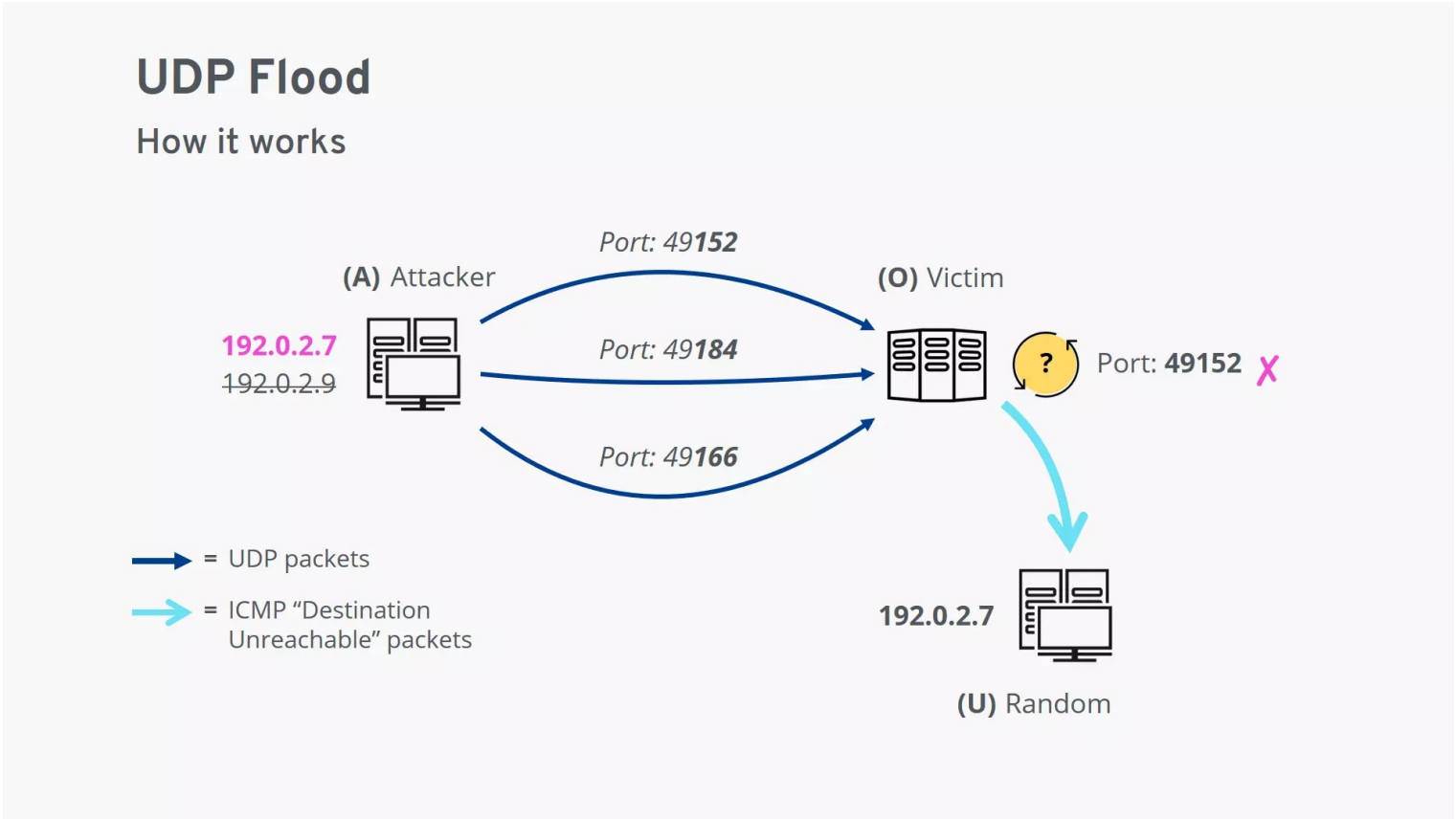


Figure from: https://www.ionos.com/digitalguide/server/security/udp-flood/

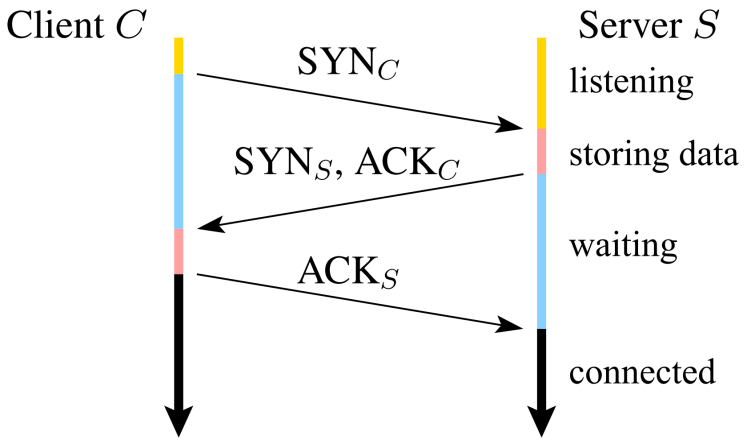
TCP

- 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

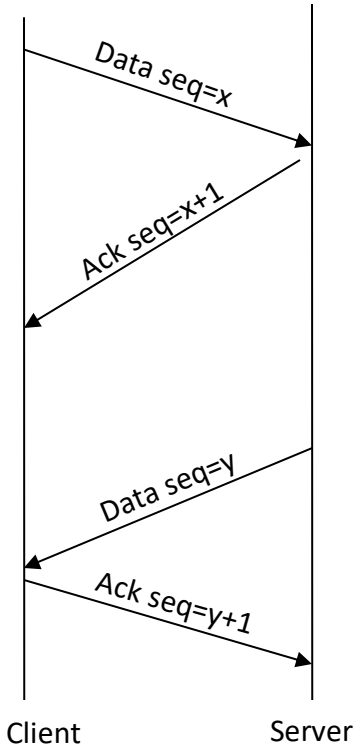
- TCP takes a stream of 8-bit byte data, packages it into appropriately sized segment and calls on IP to transmit these packets
- Delivery order is maintained by marking each packet with a sequence number
- Every time TCP receives a packet, it sends out an ACK to indicate successful receipt of the packet.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

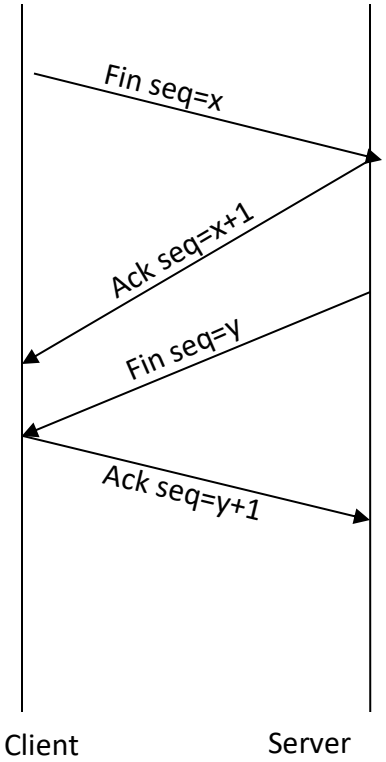
Establishing TCP Connections

- 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



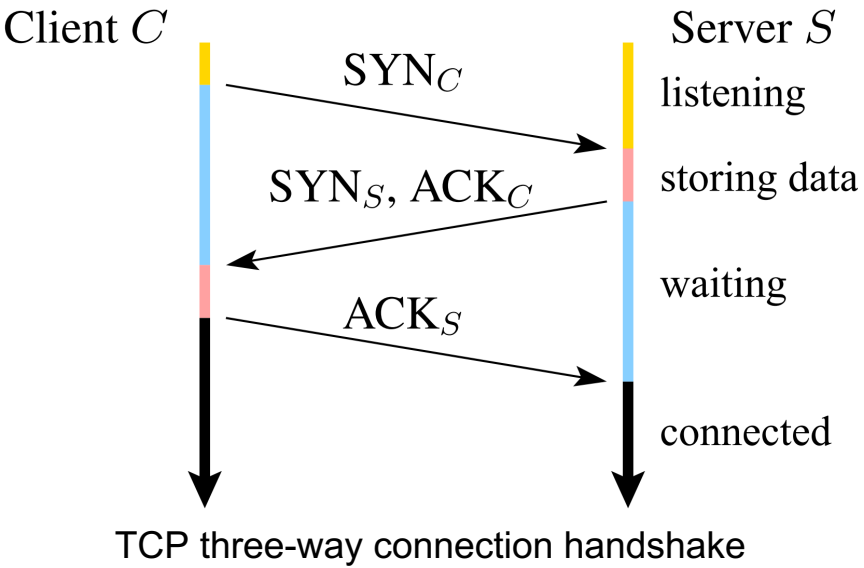


Ports

- Identify multiple concurrent applications on the same server
- 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
      - 20/21: file transfer protocol (FTP)
      - 22: SSH secure login
      - 23: telnet remote login
      - 80: http used in WWW
      - …
    - 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

DoS Attacks – SYN Flood

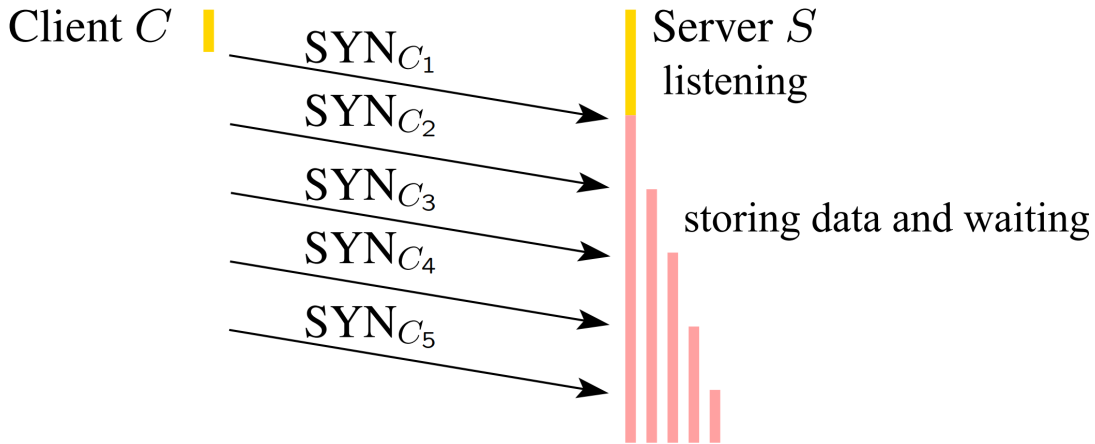
- TCP SYN flooding
  - uses the fact that a machine has a limit on the number of open connections
  - allows attacker to deny availability with much less traffic



TCP three-way connection handshake

DoS Attacks – 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 Attacks – SYN Flood

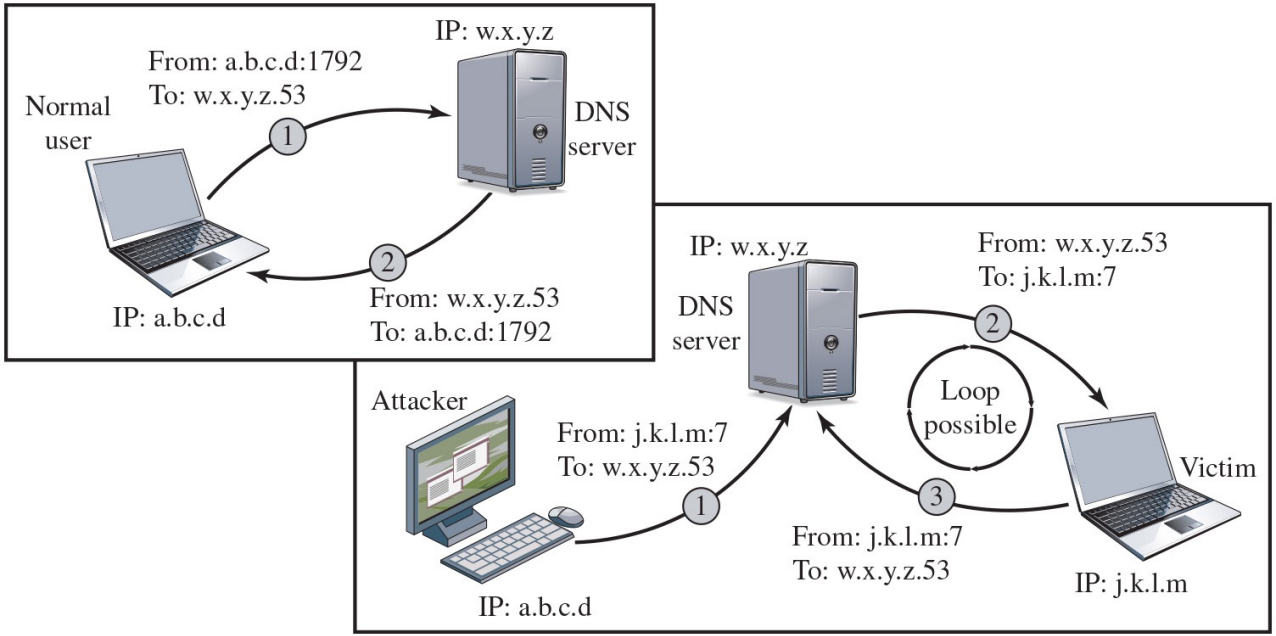
- TCP SYN flooding attack (cont.)
  - resources exhausted ⇒ legitimate requests rejected
  - the attack relies on the fact that many SYN-ACK packets will be unanswered
    - an existing host replies to a SYN-ACK packet
    - many IP addresses are not in use
  - the attacker needs to keep sending new SYN packets to keep the table full

Other DoS Attacks

- Other variants of DoS attacks that use additional machines
  - Reflection
    - Attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system
    - When intermediary responds, the response is sent to the target
    - "Reflects" the attack off the intermediary (reflector)
    - Goal is to generate enough volumes of packets to flood the link to the target system without alerting the intermediary
    - The basic defense against these attacks is blocking spoofed-source packets

Other DoS Attacks

- Other variants of DoS attacks that use additional machines
  - Reflection example

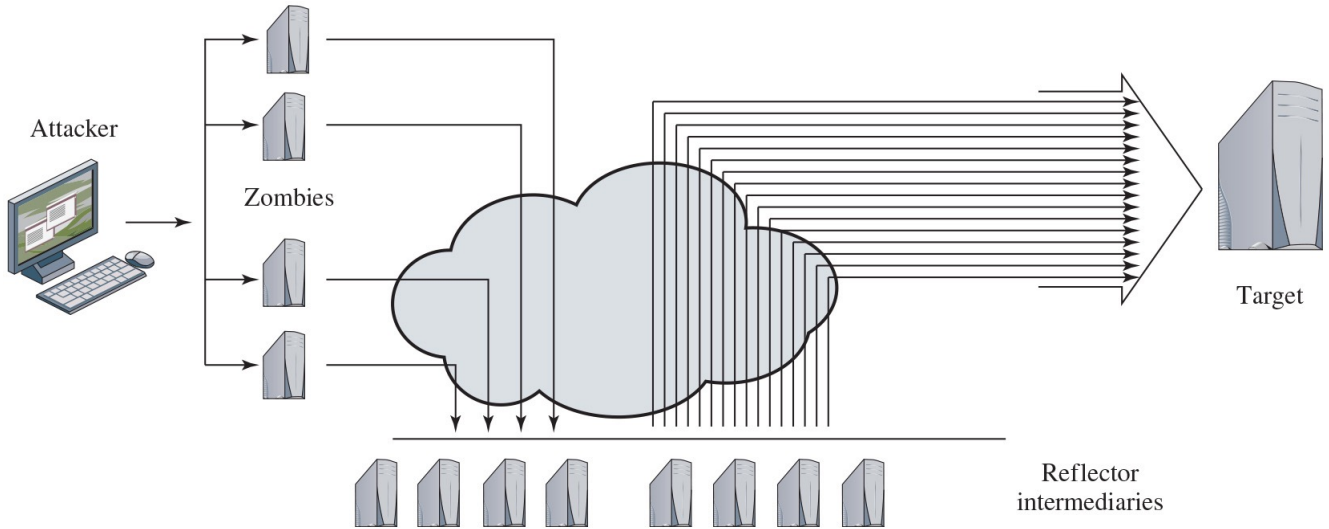


Other DoS Attacks

- Other variants of DoS attacks that use additional machines
  - Amplification
    - Also sends packets with spoofed addresses to intermediaries
    - Now one original packet generates many response packets
    - Target is flooded with responses
    - Basic defense against this attack is to prevent the use of spoofed source addresses

Other DoS Attacks

- Other variants of DoS attacks that use additional machines
  - Amplification example



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

Other DoS Attacks

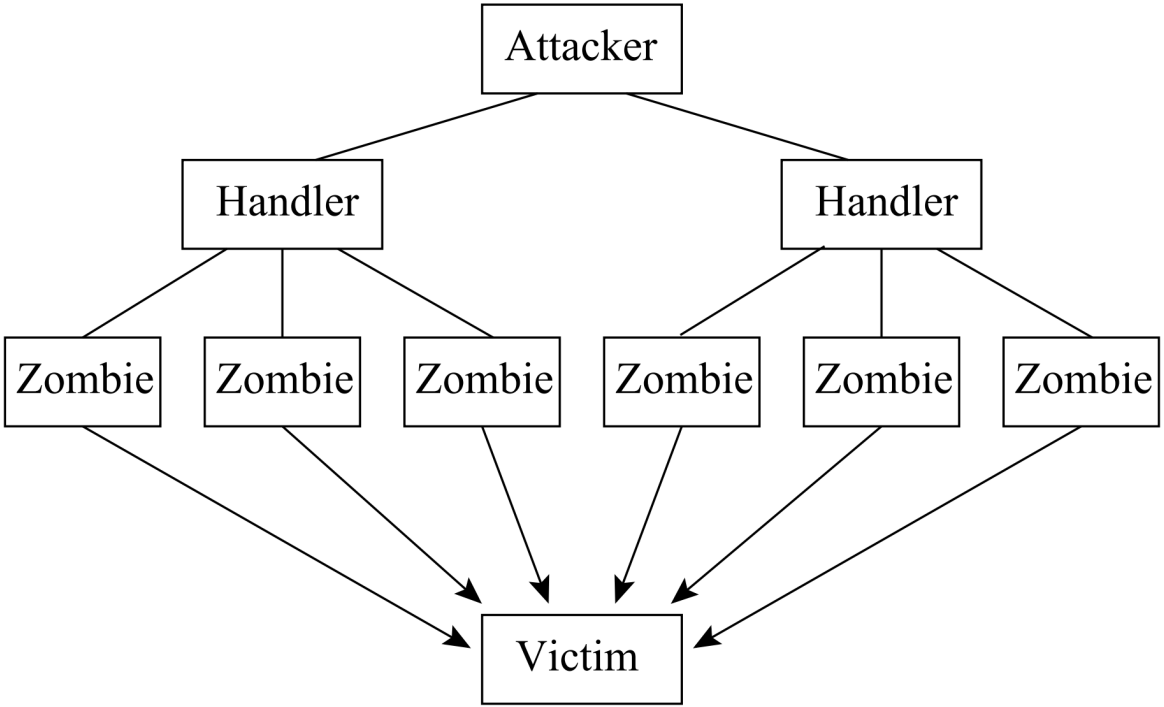
- Other variants of DoS attacks (cont.)
  - Pulsing zombie floods
    - each zombie is active briefly and then goes dormant
    - zombies take turns in attacking
    - this makes tracing difficult

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 (Internet service providers) 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

Next

Network Attacks

- MAC Spoofing, ARP Spoofing
- IP Spoofing
- Denial of Service
- DNS Cache Poisoning

Network Security