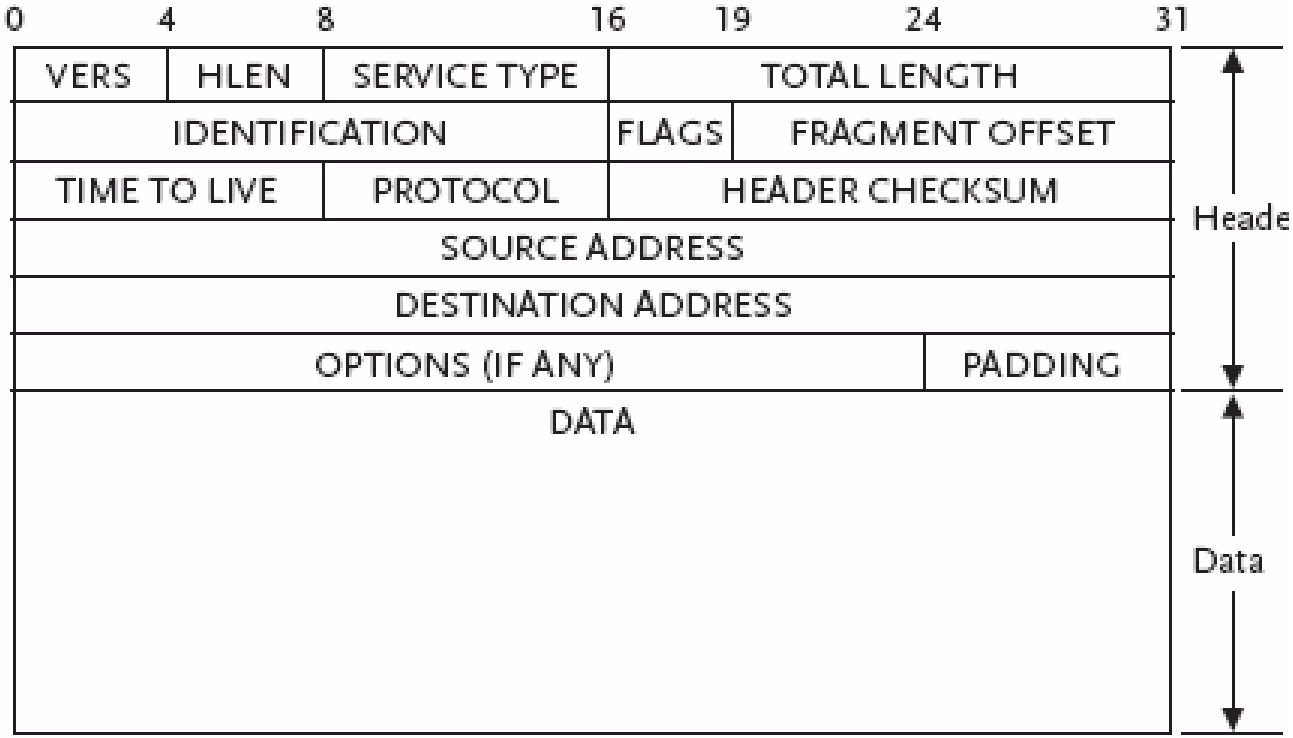
Overview

- Network communications exposes one to many different types of risks:
  - No protection of the privacy, integrity, or authenticity of messages
  - Traffic analysis - study communications patterns in order to guess the likely contents of the messages
    - Who is communicating with whom
    - How much
    - How often
  - Exploitation of the TCP/IP suite of network protocols

Overview of the Internet Protocol

- The **Internet Protocol** (IP) provides an unreliable packet delivery service
- IP packets, called **datagrams**, contain a header and data portion:



Overview of the Internet Protocol (cont)

- Important header fields:
  - VERS (4 bits) = version
  - HLEN (4 bits) = length of header in 32-bit words
  - TOTAL LENGTH (16 bits) = the length of the entire datagram (header and data) in 8-bit octets
    - Maximum possible length of a version 4 IP datagram is 65,536 bytes
  - IDENTIFICATION, FLAGS, and FRAGMENT OFFSET = used to control datagram fragmentation
    - A datagram may be too large to travel whole over a network
    - IP specifies a way to divide a datagram into smaller fragments
    - At the final destination, fragments are reassembled into the original datagram
  - SOURCE and DESTINATION IP ADDRESSES (32 bits)

Teardrop

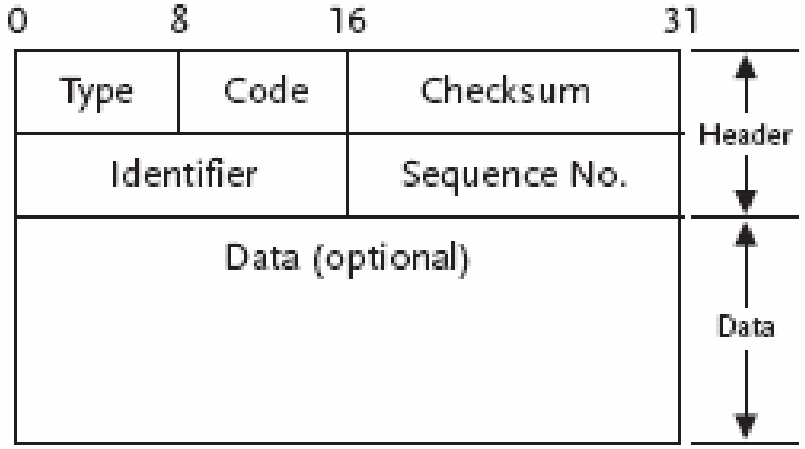
- Enabled attackers to crash vulnerable remote systems by sending a certain type of fragmented IP datagram
  - Normal datagram fragments do not overlap
  - Teardrop created fragments that did overlap
  - Some implementations of the TCP/IP IP fragmentation re-assembly code do not properly handle overlapping IP fragments
    - Windows and some Linux kernels
  - Caused system crash
  - Fixed by software patches

IP Spoofing

- DESTINATION ADDRESS field is used to route a datagram to its final destination
- SOURCE ADDRESS field identifies the sender so that the receiver knows where to send a reply
- **IP spoofing –** sender of a datagram inserts the address of another machine (or a nonexistent machine) in the source address field
  - Prevent the receiver from determining the host from which an attack datagram originated
  - Want reply sent to a another (victim) host

Overview of the Internet Control Message Protocol (ICMP)

- A sub protocol (part of IP) used to transmit error messages and report other unusual situations
- Composed of a header and data portion and are encapsulated in the data portion of an IP datagram:

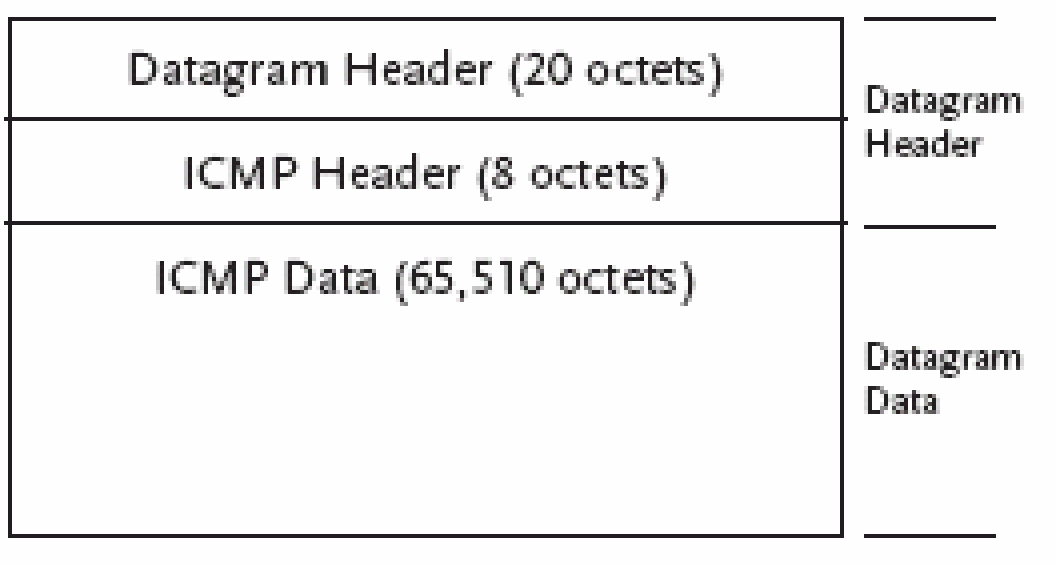


Overview of the ICMP (cont)

- Fields:
  - TYPE (8 bits) = identifies the type of the message
    - 8 = echo request
    - 0 = echo reply
  - CODE (8 bits) = identifies the subtype of the message
    - Must be 0 for echo requst/reply messages
  - CHECKSUM (16 bits) = integrity check on header and data portion of ICMP message
  - IDENTIFIER and SEQUENCE NUMBER = enable the sender to match each reply to the proper request
  - DATA = any data included in an echo request is copied into the data portion of the reply message

Ping of Death

- Attacker constructs an ICMP echo request message containing 65,510 data octets and sends it to a victim host:



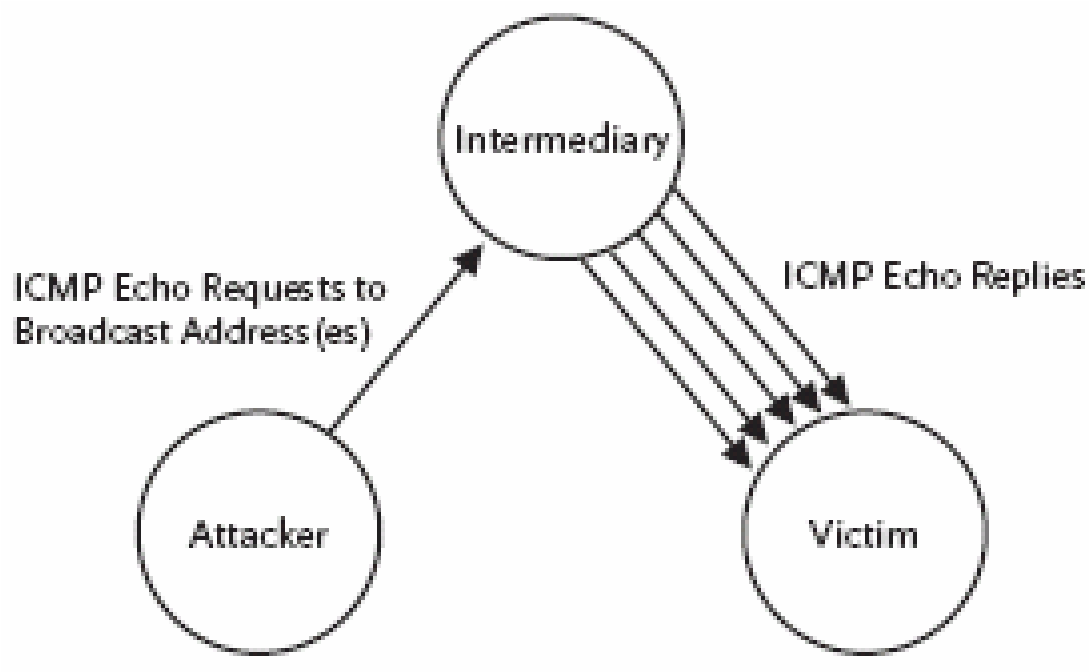
Ping of Death (cont)

- The total size of the resulting datagram (65538 octets) is larger than the 65,536 octet limit specified by IP
- Several systems did not handle this oversized IP datagram properly
  - Hang
  - Crash
  - Reboot
- Fixed by software patches

Smurf

- Attacker sends ICMP echo request messages to a broadcast address at an intermediate site
  - Broadcast address = a copy of the datagram is delivered to every host connected to a specified network
  - For some broadcast address, a single request could generate replies from dozens or hundreds of hosts
- The source address in each request packet is spoofed so that replies are sent to a victim machine
- Result: the victim's machine/network is flooded by ICMP echo replies
- Many sites have reconfigured their machines so that their machines do not respond to ICMP echo requests sent to a broadcast address

Smurf (cont)

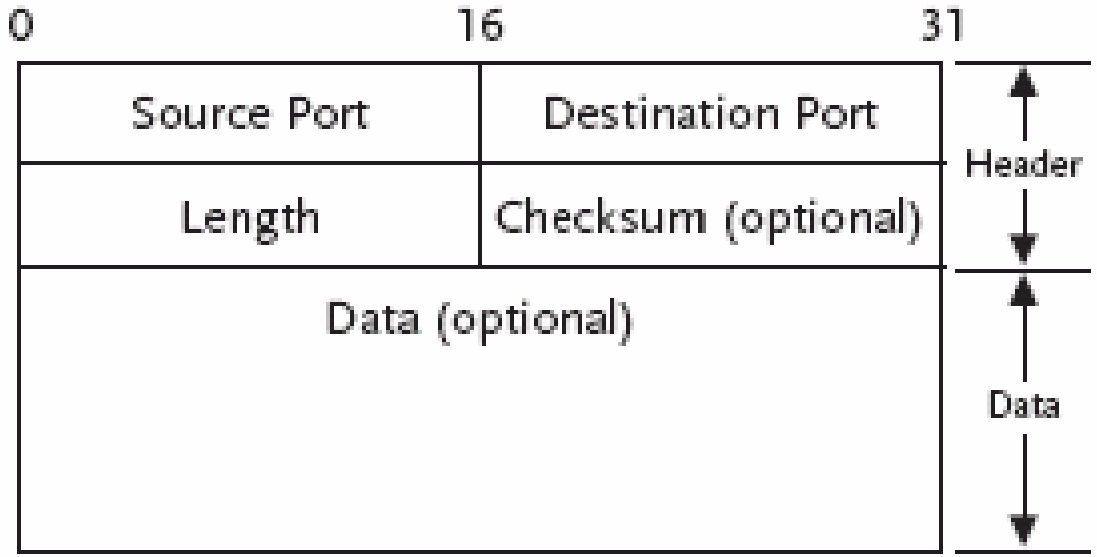

Intermediary
ICMP Echo Requests to
Broadcast Address (es)
ICMP Echo Replies
Attacker
Victim

Overview of the User Datagram Protocol (UDP)

- IP delivers data from one machine to another
- **UDP** runs on top of IP and delivers data from one application to another
  - A **port** (represented by a positive integer) is a unique destination on a single machine
  - Standard services run on reserved ports:
    - ECHO (port 7)
    - DISCARD (port 9)
    - TIME (port 37)
    - TFTP (port 69)
    - NTP (port 123)
    - Etc.
  - Programs can request an unused (dynamic) port and receive massages that arrive on that port

Overview of UDP (cont)

- The basic unit of communication in UDP is the **user datagram**
- User datagram = UDP header and UDP data



Overview of UDP (cont)

- Fields:
  - SOURCE and DESTINATION PORT (16 bits) = port identifiers
  - LENGTH (16 bits) = length of the user datagram (header and data) in octets
    - Header = 8 octets
    - Maximum length of data portion = 65,536-8 = 65,528 octets
  - CHECKSUM (16 bits) = optional integrity check of user datagram
- User datagrams are transported in the data portion of IP datagrams

Fraggle

- Similar to smurf attack:
  - UDP port seven is an echo service
  - Attacker sends user datagrams to port seven of a broadcast address at an intermediate site
    - Spoofed source addresses pointing to victim
    - Random source ports (or port 7)
  - Each request generates replies from many machines
  - Result: flood victim's machine/network with UDP replies
  - Fix: filtering out UDP echo requests (or anything else that might generate a response) sent to a broadcast addresses

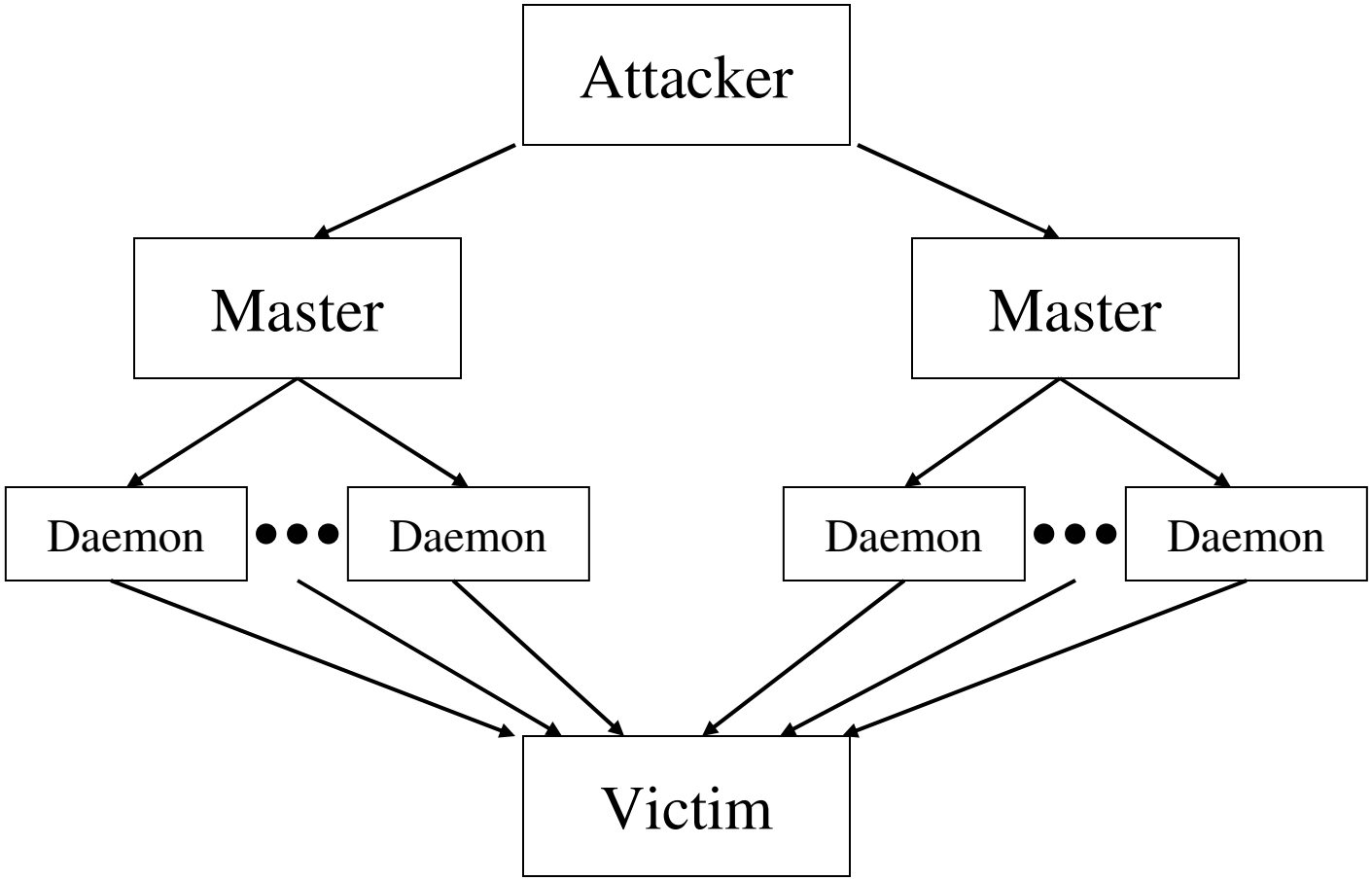
Trinoo

- **Distributed denial of service** attack tool that enables an attacker to inundate a victim with UDP traffic from many different hosts simultaneously
  - Daemon program
    - Setup:
      - Search for machines and attempt to break into them using a number of different exploits
      - Install the trinoo daemon
    - Attack:
      - When given a victim by a master server, sends a large number of UDP packets to random ports on the victim
  - Master server

Trinoo (cont)

- Master servers
  - Each master server controls a number of daemons on different hosts (commands are password protected)
  - An attacker normally controls a number of master servers (on different hosts)
    - Commands are password protected:
      - Start/stop it running
      - Test that it is alive/listening
      - Ask for a list of all the daemons that it controls
      - Instruct it to order its daemons to attack a given victim

Trinoo (cont)


Attacker
Master
Master
Daemon
Daemon
Daemon
Daemon
Victim

Trinoo (cont)

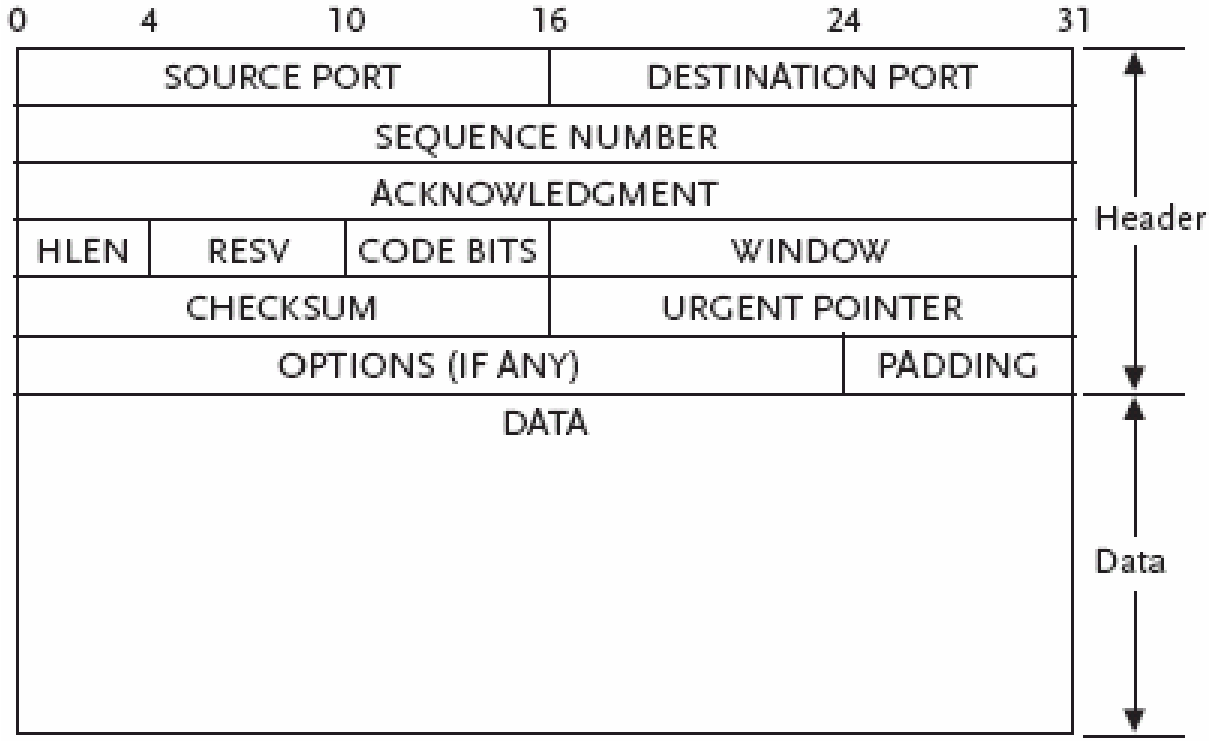
- August, 1999:
  - Trinoo daemons running on over 200 different machines flooded a University of Minnesota host for several days
- February, 2000:
  - Trinoo (and other distributed denial of service tools) used to attack several major e-commerce sites on the Web

Overview of the Transmission Control Protocol (TCP)

- TCP runs on top of IP and provides reliable delivery of a stream of data between two applications
  - TCP messages are sent inside IP datagrams
  - TCP:
    - Divides a stream of data into chunks that will fit in IP datagrams
    - Insure that each datagram arrives at its destination
      - Acknowledgements and retransmissions
    - Reassemble the stream at the destination

Overview of TCP (cont)

- TCP messages that carry data and acknowledgements are called *segments*

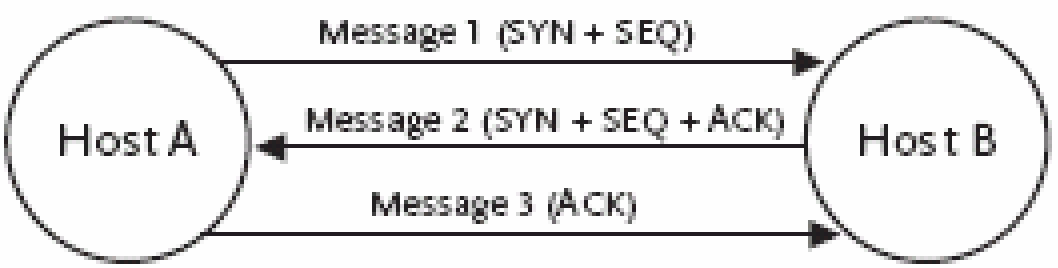


Overview of TCP (cont)

- Important fields:
  - SOURCE and DESTINATION PORT (16 bits) = port identifiers
  - SEQUENCE NUMBER (32 bits) = identifies the position of the data in the segment in the data stream
  - ACKNOWLEDGEMENT (32 bits) = acknowledge the receipt of all data up to given point
  - CODE BITS (6 bits) = URG, ACK, PSH, RST, SYN, and FIN

Overview of TCP (cont)

- Establishing a TCP connection using the three-way handshake:
  - Two parties exchange messages to ensure each is ready to communicate and to agree on initial sequence numbers for the conversation

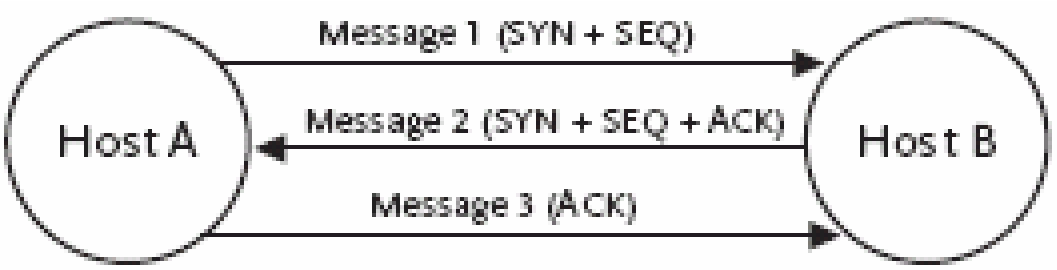


Overview of TCP (cont)

- Closing a TCP connection (one way):
  - Connection is closed from *A* to *B*
  - *B* may continue sending data to *A* before fully closing the connection

SYN Flood

- Recall the three-way handshake used to establish TCP connections:



- After the second message has been sent but before the third message has been received the connection is half opened
  - Most hosts store these half-opened connections in a fixed-size table while they await the third message
  - Half-opened connections are timed out after after half a minute or so

SYN Flood (cont)

- Attacker attempts to:
  - Fill up the half-opened connection table
    - Attacker sends the victim machine a large number of SYN segments with spoofed source addresses (to nonexistent or unreachable hosts)
    - Produces a large number of half-opened connections at the victim's machine that will never become fully open
    - The half-opened connection table fills and no new connections can be accepted until space is available
  - Keep it full
    - Continue sending SYN segments to replace half-open connections as they time out
- Result: the victim host cannot accept any other, legitimate attempts to open a connection

Land

- Attack tool exploits a vulnerability in certain TCP implementations
- Attacker creates an invalid TCP SYN segment:
  - Spoofed source address is identical to the destination address
  - Source port is identical to the destination port
- Causes some TCP implementations to freeze or crash
- Fixed with software patches

Tribe Flood Network (TFN)

- Distributed denial of service attack tool
  - Newer versions have been developed (TFN2K, TFN3K, Stacheldraht)
  - Used in February, 2000 to attack several major e-commerce sites on the Web
- Similar to trinoo:
  - Daemon programs: listen for and execute commands from a master
  - Master programs
    - Control a number of daemons
    - Communicate with an attacker and pass his/her commands on to daemons

TFN (cont)

- "Improvements" over trinoo:
  - Random protocol (TCP, UDP, or ICMP) for communication between master and daemons
  - Can send out "decoy" packets to random IP addresses to obscure the true target of the attack
  - Daemons spoof the source IP address in the attack packets they send
  - Daemons can attack multiple targets
  - Wider variety of attacks

TFN (cont)

- Daemon attack strategies:
  - UDP flood (like with trinoo)
  - TCP SYN flood
  - ICMP ping flood
  - ICMP directed broadcast flood (smurf)
  - All of the above

Scans and Probes

- Attackers typically engage in a variety of reconnaissance activities before attacking:
  - To identify important/interesting hosts
  - To identify potential vulnerabilities that could be exploited
- A **port scanner** is a program that tries to determine which ports have programs listening on them
- Example:
  - Attempts to open a TCP connection to each port in order
  - If a connection is made then immediately close it and record the fact that the port is open
  - If the connection fails then the port is closed

Port Scanning (cont)

- Using fully-open connections to scan is likely to draw a lot of attention to the scan
  - Most hosts log:
    - Each attempt to connect to a closed port
    - Each time a newly-opened connection is closed with little or no data having been sent
- Clandestine scanning methods:
  - SYN scan:
    - A SYN segment is sent to each port and any port that responds with a SYN+ACK segment is opened
    - Instead of completing the handshake, a RST (reset) segment is sent to close the connection before it is fully opened
    - Some hosts do not log half-opened connections

Port Scanning (cont)

- Clandestine scanning methods (cont):
  - FIN scanning:
    - A FIN segment is sent to each port which opened ports should ignore (since no connection has been established)
    - Closed ports are required to respond to a FIN with a RST segment so ports that do not answer are opened

Traceroute

- The **traceroute** program discovers the path that an IP datagram follows to reach a target host
  - Start by sending a probe message with a TTL value of 1 bound for the target host
  - If the target host cannot be reached in one hop then:
    - The datagram is dropped
    - The machine that drops it returns an ICMP TTL-exceeded message
    - Traceroute records the name and address of the machine and the round trip time
  - The TTL value is incremented by one, and the probe is sent again
  - This process continues until the target is reached, and traceroute generates a report of its findings
- Can be used to gain some idea about the topology of a network

Remote Operating System Fingerprinting

- Certain attacks only work on certain operating systems (and certain versions of those operating systems)
- Techniques enable attackers to try to determine what operating system is running on a host
- Typically, specially crafted (and usually invalid) IP, ICMP, UDP, or TCP packets are sent to a host
- Different operating systems (and sometimes different versions of the same operating system) are known to respond to these packets in certain ways
- Examples:
  - FIN segments for closed connections
  - TCP options

Vulnerability Scanners

- Tools that automate the hacker's job:
  - Probing, scanning, other reconnaissance activities
    - Identify target hosts and potential vulnerabilities
  - Attack
    - Execute exploits
  - Cover tracks
    - Sanitize logs, install root kit, install backdoor for future access

Security Assessment Tools

- Tools that allow system administrators to scrutinize their sites for vulnerabilities
- Examples:
  - SAINT (http://www.wwdsi.com/saint)
  - SARA (http://www-arc.com/sara)
  - SATAN (http://www.fish.com/satan)
  - Many others
- Some automate the fixing of vulnerabilities that are identified

Summary

- Network communications exposes one to many different types of risks:
  - Attacks on the privacy, integrity, or authenticity of messages
  - Traffic analysis
  - Exploitation of the TCP/IP suite of network protocols
    - Attacks on IP (Teardrop, IP Spoofing)
    - Attacks on ICMP (Ping of Death, Smurf)
    - Attacks on UDP (Fraggle, Trinoo)
    - Attacks on TCP (SYN Flood, Land, TFN)
    - Probes and scans