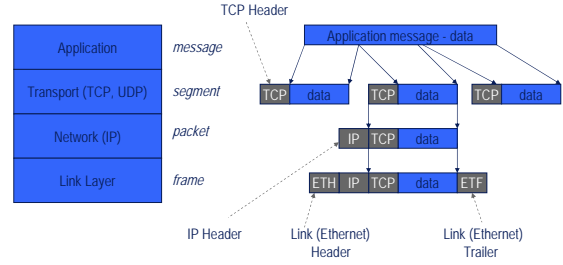


Network Security

Dawn Song
dawnsong@cs.berkeley.edu

Some slides from John Mitchell ¹

Data Formats



4

Internet Infrastructure



- **Local and interdomain routing**
 - TCP/IP for routing, connections
 - BGP for routing announcements
- **Domain Name System**
 - Find IP address from symbolic name (www.cs.stanford.edu)

2

IP

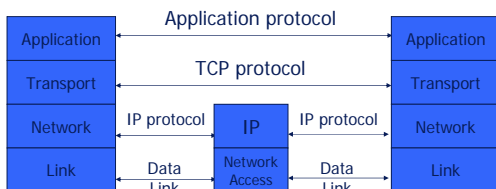
Internet Protocol

- **Connectionless**
 - Unreliable
 - Best effort
- **Transfer datagram**
 - Header
 - Data

Version	Header Length
Type of Service	
Total Length	
Identification	
Flags	Fragment Offset
Time to Live	
Protocol	
Header Checksum	
Source Address of Originating Host	
Destination Address of Target Host	
Options	
Padding	
IP Data	

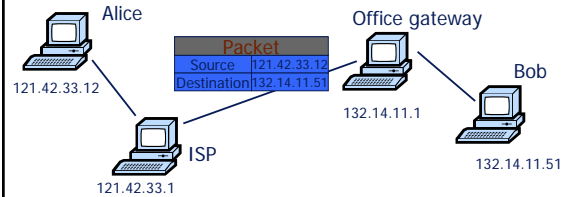
5

TCP Protocol Stack



3

IP Routing



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

6

IP Protocol Functions

- **Routing**
 - IP host knows location of router (gateway)
 - IP gateway must know route to other networks
- **Fragmentation and reassembly**
 - If max-packet-size less than the user-data-size
- **Error reporting**
 - ICMP packet to source if packet is dropped

7

ICMP

Internet Control Message Protocol

- **Provides feedback about network operation**
 - Error reporting
 - Reachability testing
 - Congestion Control
- **Example message types**
 - Destination unreachable
 - Time-to-live exceeded
 - Parameter problem
 - Redirect to better gateway
 - Echo/echo reply - reachability test
 - Timestamp request/reply - measure transit delay

10

UDP

User Datagram Protocol

- **IP provides routing**
 - IP address gets datagram to a specific machine
- **UDP separates traffic by port**
 - Destination port number gets UDP datagram to particular application process, e.g., 128.3.23.3, 53
 - Source port number provides return address
- **Minimal guarantees**
 - No acknowledgment
 - No flow control
 - No message continuation

8

Basic Security Problems

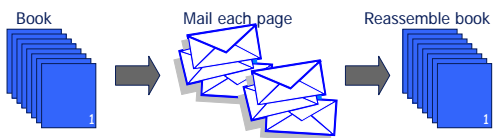
- **Internet was designed with a different trust model**
 - No security in mind
- **Network packets pass by untrusted hosts**
 - Eavesdropping, packet sniffing (e.g., "ngrep")
- **TCP state can be easy to guess**
 - TCP spoofing attack
- **TCP connection requires state**
 - SYN flooding attack
- **DDoS attacks**

11

TCP

Transmission Control Protocol

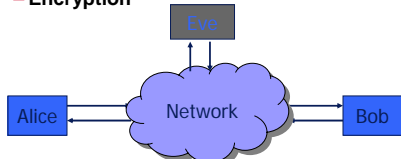
- **Connection-oriented, preserves order**
 - **Sender**
 - » Break data into packets
 - » Attach packet numbers
 - **Receiver**
 - » Acknowledge receipt; lost packets are resent
 - » Reassemble packets in correct order



9

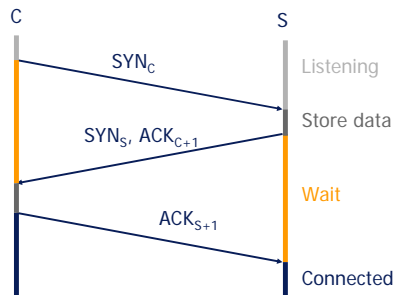
Packet Sniffing

- **Promiscuous NIC reads all packets**
 - Read all unencrypted data (e.g., "ngrep")
 - ftp, telnet send passwords in clear!
- **Solution**
 - Encryption



12

TCP Handshake



13

Force TCP Session Close

- **Suppose attacker can guess seq. number for an existing connection:**
 - Attacker can send Reset packet to close connection. Results in DoS.
 - Naively, success prob. is $1/2^{32}$ (32-bit seq. #'s).
 - Most systems allow for a large window of acceptable seq. #'s
 - » Much higher success probability.
- **Attack is most effective against long lived connections, e.g. BGP.**

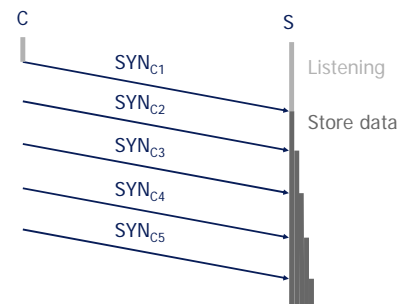
16

TCP Connection Spoofing

- **Each TCP connection has an associated state**
 - Client & Server's IP and port number
 - Sequence numbers
- **Problem**
 - Easy to guess state
 - » Port numbers are standard
 - » Sequence numbers often chosen in predictable way

14

SYN Flooding



17

TCP Session Hijacking

- **Need high degree of unpredictability**
 - If attacker knows initial seq # and amount of traffic sent, can estimate likely current values
 - Send a flood of packets with likely seq numbers
 - Attacker can inject packets into existing connection
- **Some implementations are vulnerable**

15

SYN Flooding

- **Attacker sends many connection requests**
 - Spoofed source addresses
- **Victim allocates resources for each request**
 - Connection requests exist until timeout
 - Fixed bound on half-open connections
- **Resources exhausted \Rightarrow requests rejected**
 - SYN flooding may require much less bandwidth than a bandwidth exhaustion attack
- **Defense: SYN Cookie**
 - Server computes MAC of TCP header info, including src/dst IP addresses, port #
 - Use this MAC value as SYN/ACK #

18

Denial-of-Service (DoS) Attack

- A Denial-of-Service (DoS) attack is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as CPU, memory, bandwidth, and disk space
 - A DoS attack can be local (within a single host) or network-based
- A Distributed Denial-of-Service (DDoS) attack is a networked-based DoS attack using a multiple attacking hosts

19

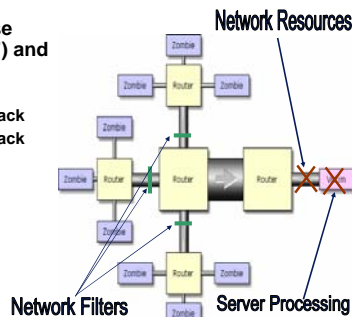
Reflector Attacks

- Put victim's IP as the source address in requests to reflectors
- Use reflectors to flood victim
- Advantages
 - Bandwidth amplification
 - Hiding origin of attack
- Many examples
 - DNS
 - » Register.com (Jan 2001)

22

Distributed Denial-of-Service

- Hacker(s) compromise machines ("zombies") and use them to flood a particular server.
 - Network Resource Attack
 - Server Processing Attack
- IP Spoofing
 - Complicates effective filtering



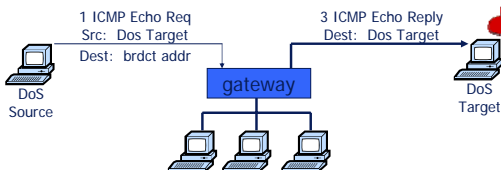
*modified from grc.com 20 20

Long History of DDoS Attacks

- Early attacks took down Yahoo!, eBay for fun & fame (2000)
 - Early DDoS tools & zombie network
- Recent attacks
 - Botnets
 - Extortion for profit
 - 10,000 online game servers in games such as Return to Castle Wolfenstein, Halo, Counter-Strike attacked by "RUS" hacker group (2007)
- Cyber warfare?
 - Attacks on Estonia government website (May 2007)
 - Attacks on Georgia government website before war (2008)

23

Smurf DoS Attack



- Send ping request to broadcast addr (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

Prevention: reject external packets to broadcast address

21

DDoS Activity Measurement: Backscatter

- Use Internet telescope
 - Monitor large blocks of IP addresses
- Receive TCP SYN ACKs in IP spoofing DDoS attacks
- Estimate global activity assuming spoofed IP addresses are generated uniformly at random
- Study finds >12000 attacks on over >5000 victims in three weeks
 - Mostly short attacks, some last for weeks

24

DDoS Attack Defenses

1. **Server resource exhaustion-based attacks**
 - TCP SYN cookies
 - CAPTCHA
 - Overprovisioning/replication, Akamai-style
2. **Flooding attack, link towards server congested**
 - Overprovisioning/replication, Akamai-style
 - In-network filtering, victim asks ISP to setup filter
- **IP spoofing (in conjunction with another attack class)**
 - Ingress filtering

25 25

Other Defenses

- **Traffic scrubbing**
 - Centralized service with big pipe
 - Forward cleaned traffic to victim site
- **Distributed infrastructure design**
 - E.g., Akamai service

28

CAPTCHAS

- CAPTCHA stands for “Completely Automated Public Turing Test to Tell Computers and Humans Apart”
- Puzzle that is easy to solve for humans but hard to solve for computers



26 26

Approaches Against IP Spoofing

- **Goal: prevent IP address spoofing**
 - Difficult challenge
- **Ingress Filtering: Routers drop packets with an “invalid” source IP address field**
 - Advantages: Eliminates source IP spoofing (if everyone does it)
 - Disadvantages: Source-based solution, no deployment incentives, everybody has to deploy

27 27