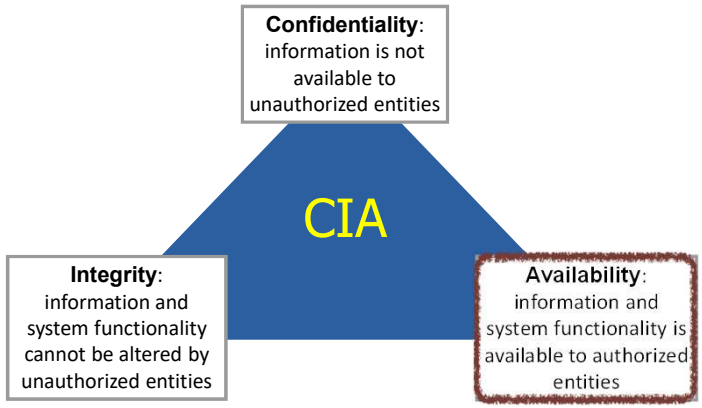
Lecture 26: Denial of Service

Stephen Huang

Content

1. Denial of Service
2. Mitigation of DoS Attacks

Security Objectives



1. Denial-of-Service Attacks

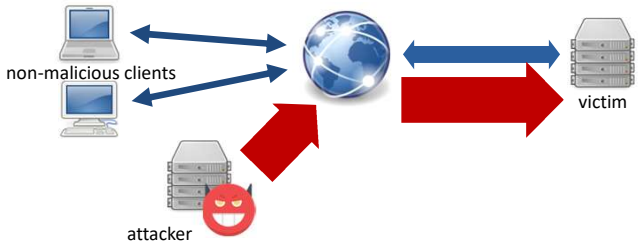
- Denial-of-service (DoS): attack against availability
  - Availability: information and system functionality is available to authorized entities.
- Vulnerability exploitation
  - The attacker may exploit software or configuration vulnerabilities to crash a system.
  - example: CVE-2011-1871
  - "Tcpip.sys in the TCP/IP stack in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (reboot) via a series of crafted ICMP messages."

Denial-of-Service Attacks

- Resource Exhaustion
  - The attacker uses up all of the victim's resources. No resources left for serving authorized entities (might even crash the system).
  - The attacker may exhaust
    - bandwidth,
    - computational power,
    - memory, etc.

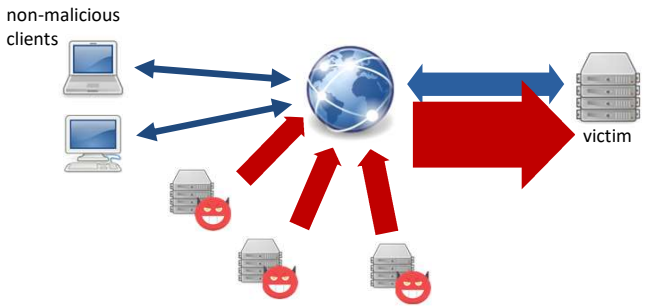
Network Bandwidth Exhaustion

- DoS Basic Principle: Denial of the Victim's Resources
- Challenges for the attacker
  - generating enough traffic to exhaust the target's bandwidth is hard/expensive
  - blacklisting/shutting down the attacker's host is relatively easy



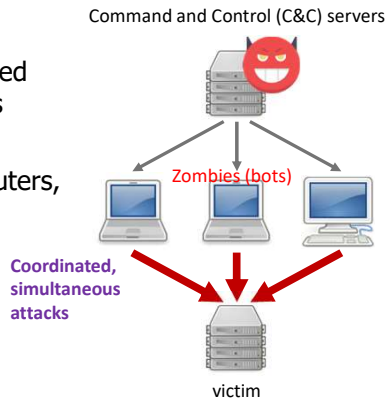
Network Bandwidth Exhaustion

- Distributed DoS (DDoS) Basic Principle



Botnets for DDoS

- Botnet
  - collection of remotely controlled compromised ("zombie") computers
  - zombies may be laptop/desktop computers, IoT devices, …

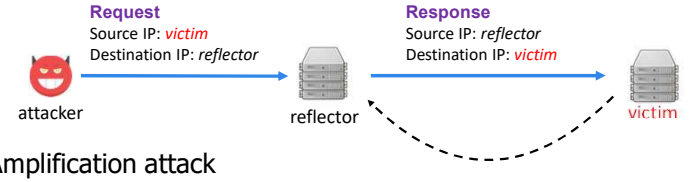


DDoS

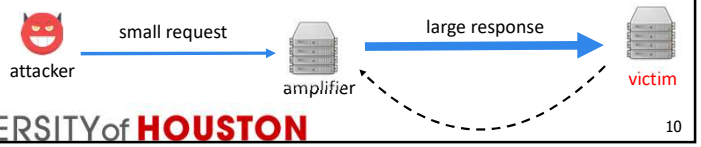
- Examples of DDoS attacks using IoT botnets
  - IoT devices include DVRs, cameras, …
  - OVH, a French ISP provider (September 2016)
    - Using the Mirai botnet
    - more than 1 terabit-per-second (Tbps) attack traffic
  - Dyn DNS provider (October 21st, 2016)
    - hundreds of thousands of IoT devices
    - attackers targeted authoritative DNS servers
    - Twitter, Spotify, Github, Reddit, CNN, PayPal were (partially) unavailable for hours
- Highest bandwidth DDoS: 3.47 Tbps, a packet rate of 340 million packets per second (pps)

Reflected Attacks

- IP address spoofing
  - The attacker can send packets with fake source addresses
  - The recipient will believe that the packets originate from the fake source
- Reflected attack



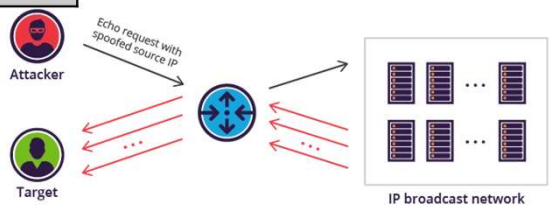
- Amplification attack



IP Packet

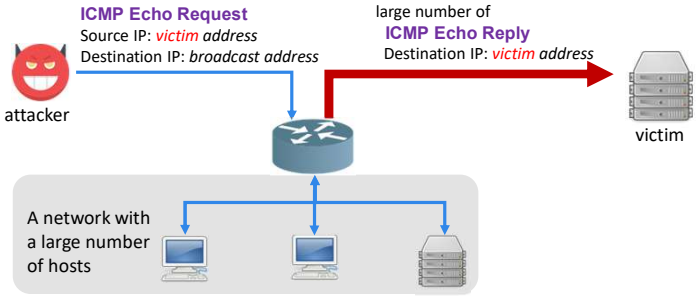
IP packet

Version& IHL	QoS	Length
ID		DF, MF, Fragment Offset
TTL	Protocol	Checksum
Source IP address		
Destination IP address		
Payload		



Smurf Amplification Attack

- Internet Control Message Protocol (ICMP)
  - supporting protocol in the IP suite for error messages and operational information
  - on receiving an Echo Request message (ping), a host should respond with an Echo Reply

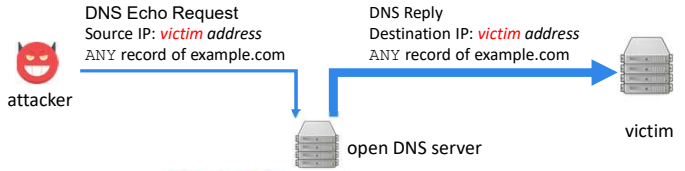


Fraggle Amplification Attack & Prevention

- Fraggle attack
  - Similar to the Smurf attack, but based on UDP protocols that are used for testing
  - Echo Protocol (UDP port 7): The receiver sends back an identical copy of the received data
  - Character Generator Protocol (UDP port 19): upon receiving a UDP packet, the receiver sends back a random number (0 … 512) of characters
- Prevention
  - Prevent routers from forwarding packets directed to broadcast addresses (default standard configuration)
  - Prevent hosts from responding to requests
    - Echo and Character Generator services are typically disabled

DNS Amplification Attack

- Open DNS resolver
  - DNS servers that are open to requests from any client on the Internet
  - at least 5 million such servers (2019 Nov., http://openresolverproject.org/)
- DNS Amplification
  - send a small (~64 byte) DNS query in UDP for `ANY` record of some domain name
  - server responds with a reply in UDP containing all records (e.g., addresses, authoritative name servers, DKIM keys) for the hostname → maximum UDP response size = 512 bytes → 8x amplification



DNS Amplification Attack (contd.)

- Extension Mechanisms for DNS (EDNS)
  - relaxes the 512-byte limitation on UDP replies
  - introduced to support DNSSEC, which requires sending large number of public keys

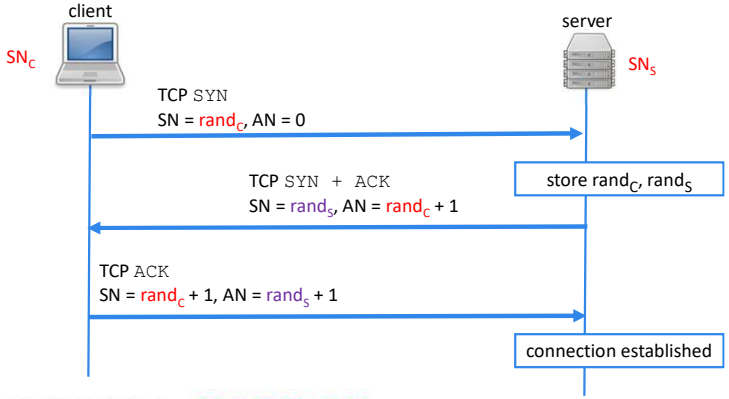
  → reply may be as big as 4000 bytes → more than 60x amplification
- Prevention and mitigation
  - disabling ANY requests on open DNS resolvers
    - attacker may register a domain and create a larger record under it (e.g., attacker registers attacker.com and sets a 4000-byte TXT record for it)
  - closing down open DNS resolvers
    - practically impossible, there are millions of them…
    - some companies provide this as a service intentionally (e.g., Google)
  - Rate-limiting: limit the number of queries that are answered for a client in a given time interval

Amplification Attacks

- *Example:* 2013 DNS amplification attack against *Spamhaus*
  - Spamhaus is an international anti-spam organization, that tracks spammers and spam-related activity, providing black and whitelists
  - over 30,000 open DNS servers, 100x amplification, 300 Gbps traffic
- Other amplification approaches
  - Network Time Protocol (NTP): 500x amplification, popular in recent years
  - Lightweight Directory Access Protocol (LDAP): 50x amplification
  - Simple Service Discovery Protocol (SSDP): 31x amplification
  - …
- *Example:* February 28, 2018 attack against *GitHub*
  - peaked at 1.35 Tbps via 126.9 million packets per second
  - using `memcached` servers with UDP, up to **51,000** amplification ratio

Background: TCP Handshake

- TCP header: sequence number (SN) and acknowledgment number (AN)

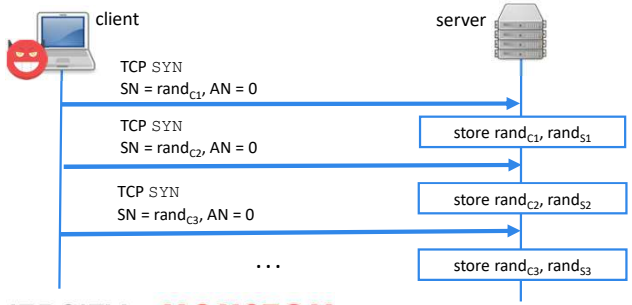


TCP Control Block

- Each TCP connection maintains a state, usually in a TCP Control Block (TCB) data structure.
- The TCB contains information about the connection state, its associated local process, and feedback parameters about its transmission properties.
- A TCP buffer is used to store TCBs.
- Once a server entered the SYN RCVD state, it would remain in that state for several seconds, waiting for an ACK and not accepting any new, possibly genuine connections, thus being rendered unavailable.

TCP SYN Flood

- Send a large number of TCP SYN packets from various spoofed source IP addresses.
- In most implementations, the number of pending connections is limited
  → non-malicious users will not be able to connect.

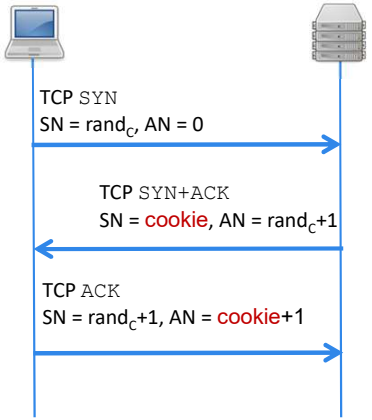


TCP Cookies

- Specially chosen sequence number instead of stored number
  - sequence number is a concatenation of
    - current time with low precision (e.g., 64 seconds).
    - secret-key-based MAC of source and destination IP addresses, port numbers, and the current time.
  - upon receiving ACK, the server can subtract one and verify the MAC.
  - spoofed clients cannot send a correct ACK
  - non-spoofed malicious clients can be blacklisted during an attack
- Modern operating systems (e.g., current versions of Linux and Windows) support some form of this protection

TCP Cookies

- SYN cookies is an IP Spoofing attack mitigation technique whereby server replies to TCP SYN requests with crafted SYN-ACKs, without creating a new TCB.
- A TCB is created for the respective TCP connection after the client replies to this crafted response.



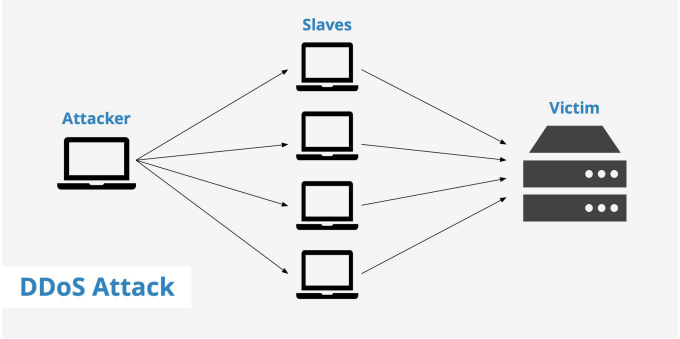
Massive Flooding Attacks

- The attacker can flood a server with TCP SYN packets
  - traffic saturates the network link of the victim
  - packets from spoofed IP addresses look the same as legitimate connections
  - could also use other "junk" packets (e.g., ICMP Echo Request)
- TCP connection flood
  - attacking computers can establish TCP connections and send HTTP requests
  - Slowloris attack
    - attacking computer sends a partial HTTP request
    - then periodically sends new HTTP header fields
    - server needs to keep track of HTTP connections
  - attacking computers can be blacklisted

Types of DDoS attacks

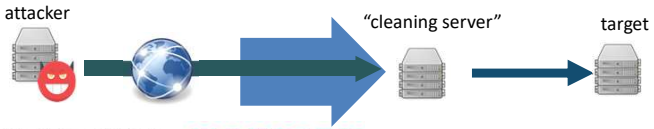
- Network layer
  - DNS amplification
  - SYN Flood
  - NTP attacks
- Application layer
  - HTTP floods
  - Slowloris attacks
  - Application layer protocol attacks
- Volumetric attacks
- Protocol attacks
- Reflective attacks
- IoT botnet attacks

2. Mitigation of DoS Attacks



Hardware and Service Based

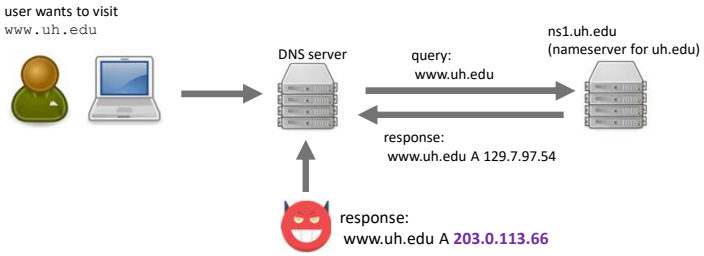
- Application front-end hardware
  - filter network traffic using high-performance dedicated hardware before it reaches the servers
  - does not protect against bandwidth exhaustion
- Upstream filtering and DDoS-resistant hosting
  - in case of an attack, traffic may be redirected to a "cleaning server," which filters malicious traffic and sends only non-malicious traffic to the actual server
    - cleaning server may be implemented as an application-level proxy
  - DDoS-resistant hosting may be provided using content delivery networks
  - many providers offer such services (e.g., CloudFare, Akamai, Incapsula)



IP Address Spoofing

- Reminder: IP address spoofing
  - sending IP packets with a fake source address
  - no verification defined in the basic Internet protocol
  - some upper-layer protocols protect address spoofing (e.g., TCP sequence numbers)
- Example applications of spoofing
  - legitimate use for testing (e.g., stress testing servers)
  - (D)DoS attack (see prior slides)
  - circumventing address-based access control (e.g., circumventing firewalls; see previous lecture)
  - DNS cache poisoning attack (see Lecture 15)

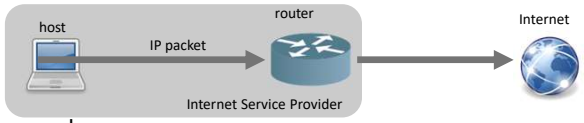
DNS Cache Poisoning Attack



- Attacker may send a fake response "from" the spoofed address of the authoritative nameserver
  - if the cache on the DNS server is successfully poisoned, every user relying on that DNS server will be directed to the attacker's malicious server

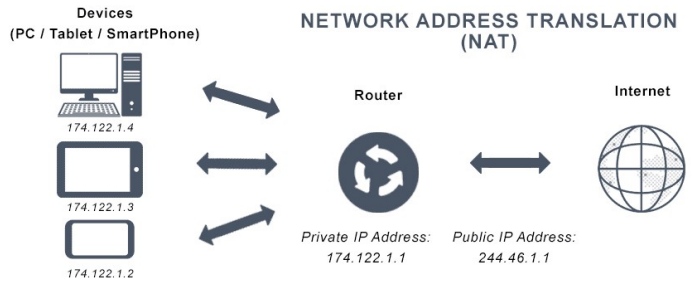
Ingress Filtering

- Network ingress filtering
  - service providers may forward only packets with legitimate source addresses
  - described in IETF BCP (Best Current Practices) 38 and 84
    - defined by IETF RFC 2827 and 3704



- Approaches
  - static packet filtering: manually configure filtering based on addresses allocated by the upstream network
  - Network Address Translation (NAT): address translation has an inherent "source validation side effect."
  - Forwarding-based validation (see next slides)

Network Address Translation

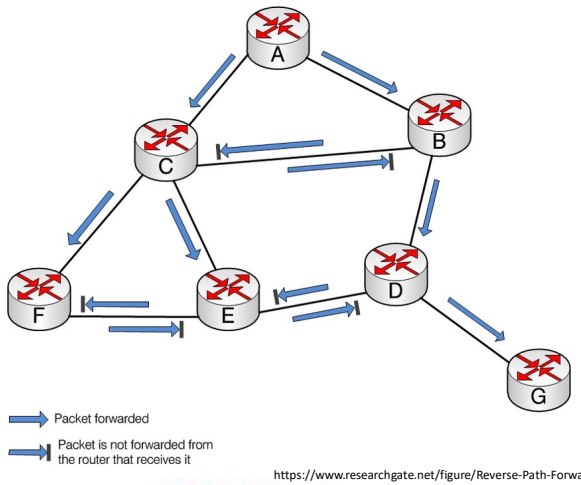


https://avinetworks.com/glossary/network-address-translation/

Reverse Path Forwarding

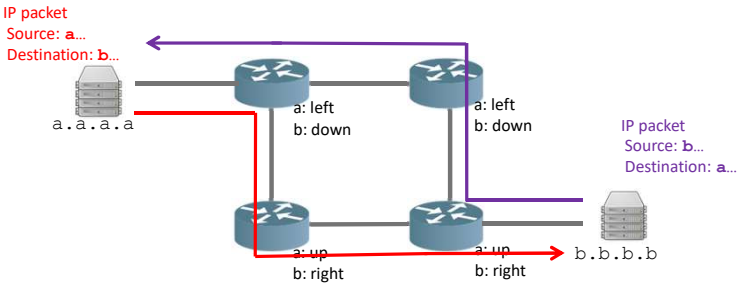
- IP packet forwarding is based on forwarding tables
  - specifies an output interface for any destination address
- Reverse path forwarding
  - forwarding decision for a packet is affected by its source address
  - used for loop-free forwarding of multicast packets and for ingress filtering
- Unicast Reverse Path Forwarding (uRPF)
  - ingress packet filtering defined in RFC 3704
  - strict mode: test if the incoming interface is the best path to the source according to forwarding information base (FIB), a.k.a, forwarding table → drop failed packets

RPF



https://www.researchgate.net/figure/Reverse-Path-Forwarding_fig1_221565465

uPRF: Feasible and Loose Modes

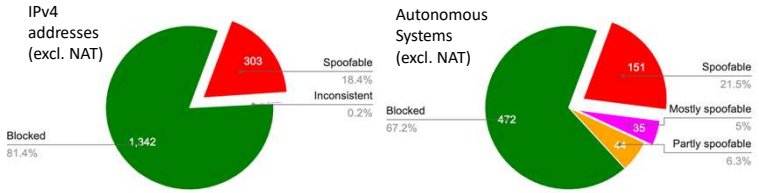


Problem: routing is often asymmetric on the Internet backbone
Unicast Reverse Path Forwarding (uRPF)

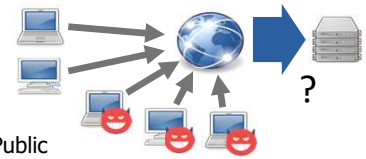
- strict mode (previous slide) would filter out packets on asymmetric routes
- feasible mode: maintain multiple feasible paths in the FIB
- loose mode: verify the existence of a route (regardless of interface of direction)

State of IP Spoofing

- Challenges
  - (almost) all ISPs must implement filtering in order to prevent attacks
  - similar to reflectors/amplifiers used for DoS, there is little incentive for implementation
- Statistics (https://spoofer.caida.org/summary.php, April 2022)
  - 20% of global IP address space and 24% of Autonomous System are spoofable



CAPTCHA



- Problem: differentiating malicious clients from honest ones
- Solution: differentiate by verifying that connections are from humans
- CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)
  - challenge-response test used to determine if a client is human
    ~ "reverse Turing test" (the judge is a computer)
  - typically based on hard AI problems, such as image recognition (e.g., character recognition)

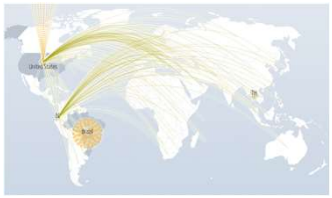
- Present one CAPTCHA per source IP address
  - if a client passes the test, whitelist the source IP address

CAPTCHA Limitations

- Cannot protect against low-level attacks (massive flooding attacks)
- An attacker may circumvent CAPTCHA
  - attacker may use cheap labor or machine learning algorithms to solve CAPTCHAs
  - in 2010, a study found that the price of solving 1000 CAPTCHAs is as low as $1
  - An attacker may also set up its site, which reposts the target site's CAPTCHAs
- May present accessibility problems for users with disabilities (e.g., visual CAPTCHAs for visually impaired or color-blind users)
  - audio CAPTCHAs are often provided as an alternative
  - if multiple CAPTCHA techniques are available, an attacker will opt for the one that is easiest to defeat
  - some users may have both visual and hearing impairment
- Usability cost for honest users

DoS Attacks Conclusion

- (D)DoS mitigation is a very challenging problem
- Example incident: DDoS attack against Dyn DNS provider
  - on October 21, 2016, attackers impaired authoritative DNS servers using DDoS
  - Twitter, Spotify, Github, Reddit, PayPal were (partially) unavailable for hours
- DoS attacks worldwide:



www.digitalattackmap.com, September 18, 2023