DDOS Basics

Yue Duan
Illinois Institute of Technology

Denial of Service

- Denial of Service (DoS)
  - an action that **prevents or impairs** the authorized use of networks, systems, or applications by **exhausting** resources
- Attacks may be directed against
  - network bandwidth
  - system resources (CPU, memory, disk space …)
  - application resources
- DoS is an established and continuing threat on the Internet

Denial of Service

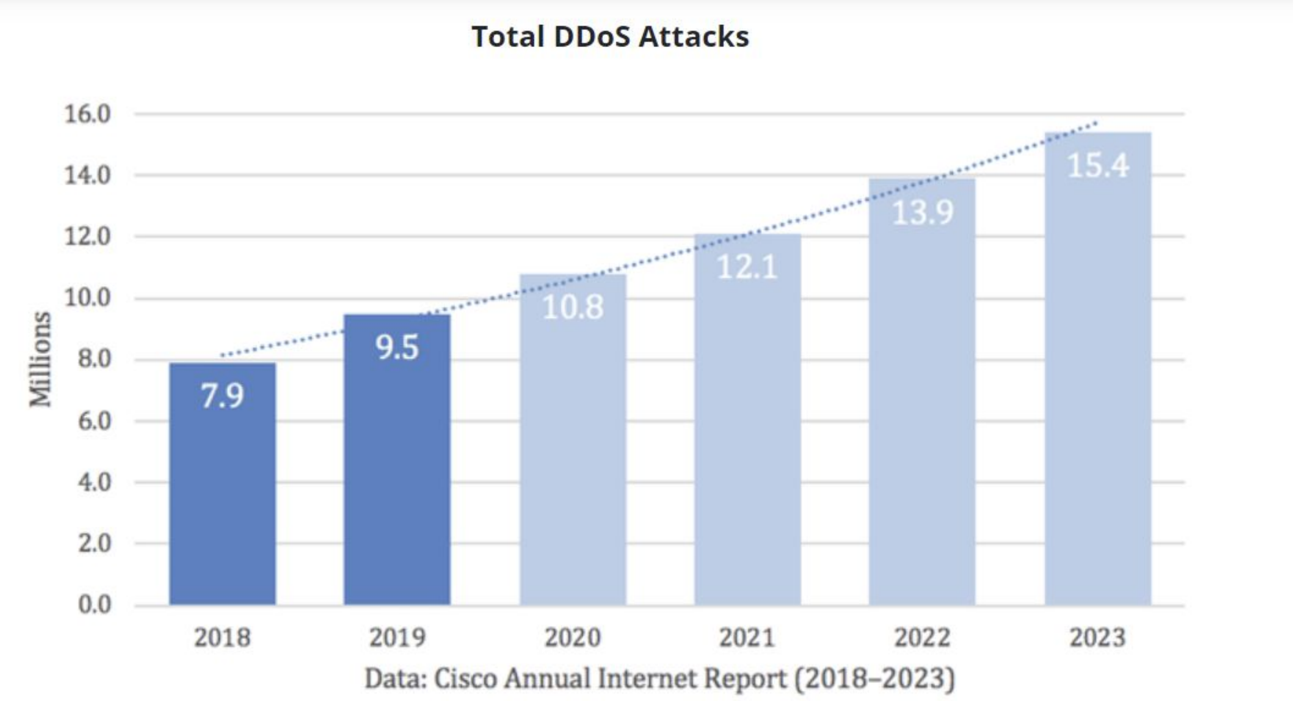
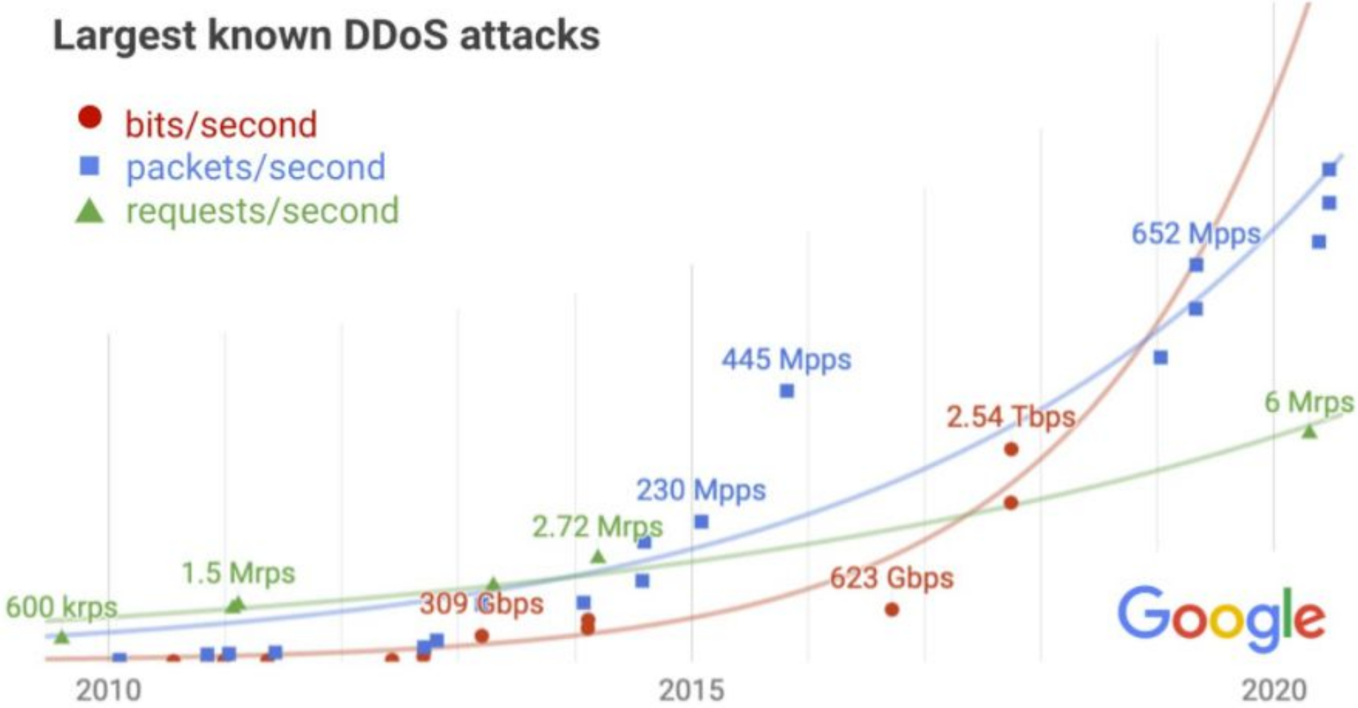
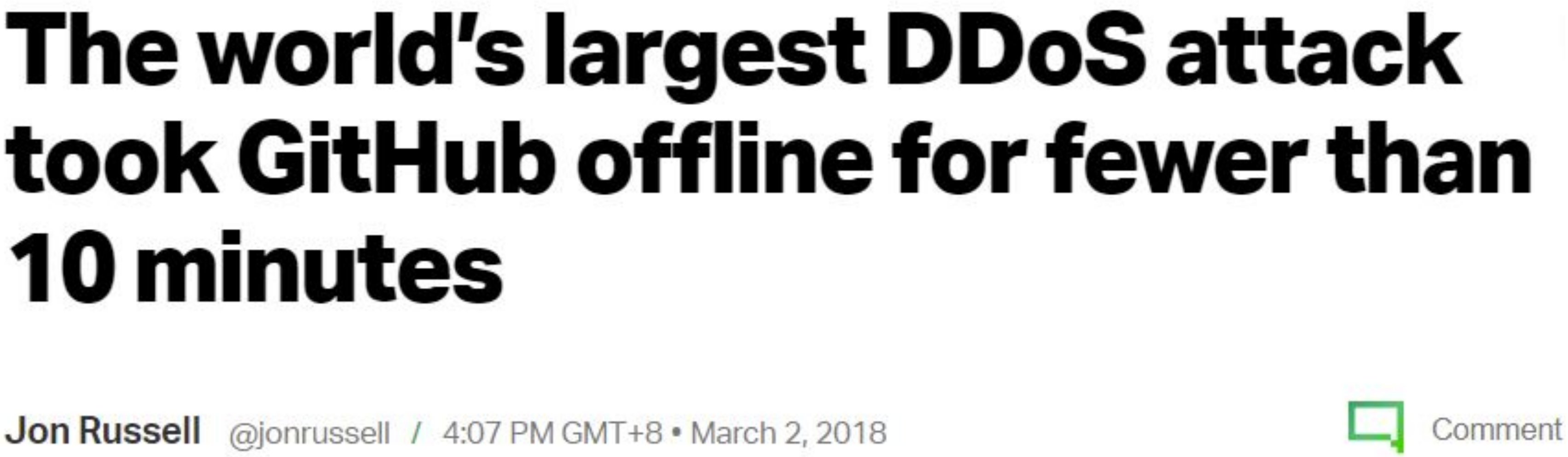


Figure 1. Cisco's analysis of DDoS total attack history and predictions.

Denial of Service



Real-world attack



The world's largest DDoS attack took GitHub offline for fewer than 10 minutes

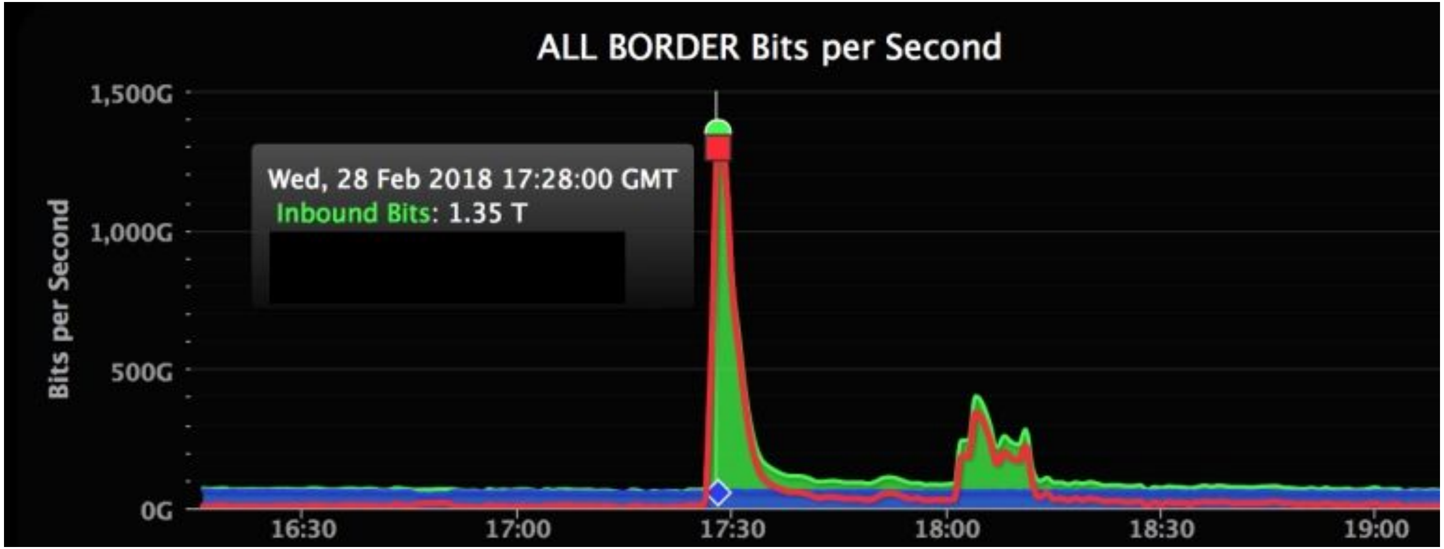
Jon Russell @jonrussell / 4:07 PM GMT+8 • March 2, 2018

Comment

Real-world attack

- According to the report, attackers hijacked something called “memcaching”
  - a distributed memory system known for high-performance and demand
- **Amplification factor** is up to 51,000
  - for each byte sent by the attacker, up to 51KB is sent toward the target
- Results:
  - offline for five minutes between 17:21 to 17:26 UTC
  - intermittent connectivity between 17:26 to 17:30 UTC

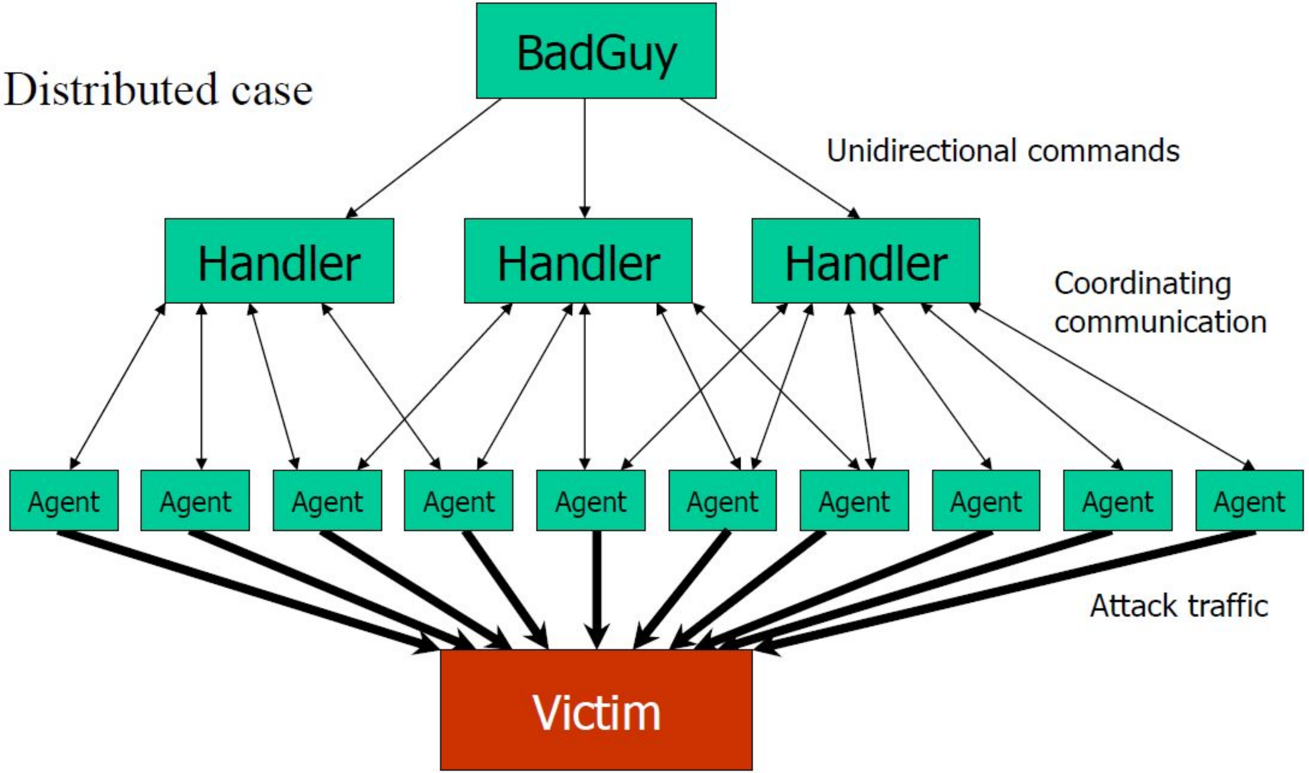
Real-world attack



DENIAL-OF-SERVICE

- Basic case
  - Use simple flooding ping
  - Higher capacity link floods lower capacity link
  - Problem: Easily **traceable and preventable**
- Advanced case: Distributed DOS (DDOS)
  - Attacker controls multiple agents
  - agents launch attacks to the victim server

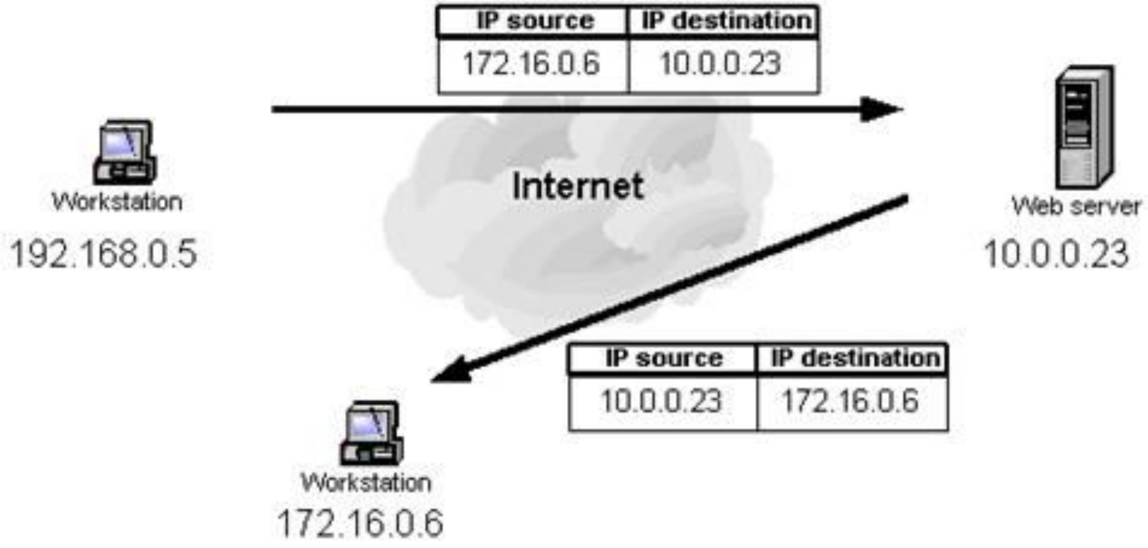
DENIAL-OF-SERVICE



Address spoofing

- Senders can put any source address in packets
  - Can **directly attack target** in a less traceable fashion
  - Can be used to **send unwelcome return traffic** to the spoofed address
- Routers can catch some spoofers
  - Reverse path verification
  - Egress filtering
    - control the traffic that is attempting to leave the network

Address spoofing



IP source	IP destination
172.16.0.6	10.0.0.23

IP source	IP destination
10.0.0.23	172.16.0.6

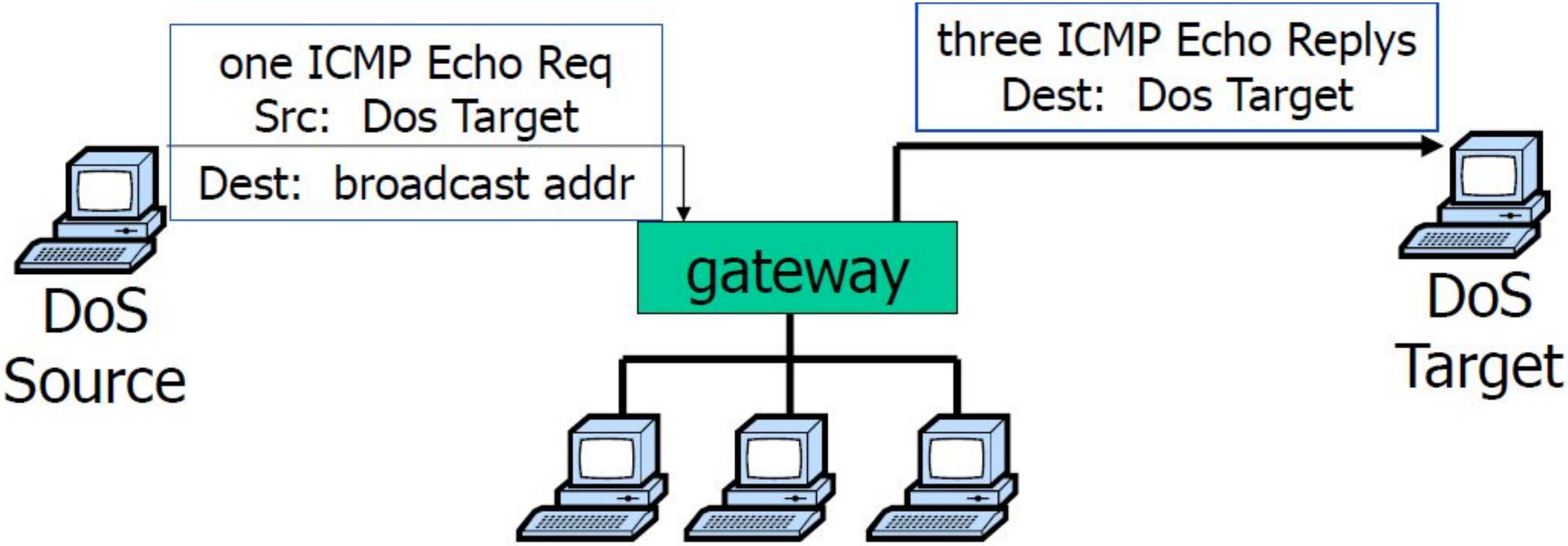
Smurf DoS Attack

- In a standard scenario
  - host A pings host B ===> **automatic response** from B to A
- In an IP broadcast network
  - an ping request is sent to **every host**, prompting a response from **each** of the recipients
- Smurf attacks
  - perpetrators take advantage of this function to **amplify** their attack traffic

Smurf DoS Attack

- Smurf malware is used to generate a **fake Echo request** containing a **spoofed source IP** (target server).
- The request is sent to an intermediate IP broadcast network.
- The request is transmitted to all of the network hosts on the network.
- **Each host** sends an ICMP response to the spoofed source address.
- With enough ICMP responses forwarded, the target server is brought down.

Smurf DoS Attack



DDoS Taxonomy

- victim type
- degree of automation
- agent Recruitment Strategies
- exploited Weakness
- Source Address Validity
- etc

DDoS Taxonomy: Victim type

- Application layer attacks (layer 7 of OSI model)
  - overload a server by sending a large number of requests requiring **resource-intensive handling and processing**
  - HTTP floods, slow attacks (e.g., Slowloris or RUDY) and DNS query flood attacks
- Network layer attacks (layer 3-4)
  - UDP flood, SYN flood, NTP amplification and DNS amplification attacks, and more
  - commonly measured in gigabits per second (Gbps) or packets per second (PPS)

DDoS Taxonomy: Degree of Automation

- Manual
  - attacker manually scans, breaks in, installs attack code, then directs the attack
  - Used by early DDoS attacks only
- Fully automated
  - exploit/recruitment phase and attack phase both automated
  - everything is preprogrammed in advance
  - no need for further communication between master & agent
  - **minimal exposure** for attacker
  - inflexible
    - attack specification is hard coded

DDoS Taxonomy: Degree of Automation

- Full automated
  - hybrid of auto/semi-auto
    - fully programmed in advance for auto, but leave a backdoor for future modification
- Semi-Automated
  - recruitment phase automated, attacks manually initiated
  - **requires** communication between master & agents
    - direct communication - need to know each other's IP address
    - indirect communication - use some pre-existing legitimate communication channel

DDoS Taxonomy: Agent Recruitment Strategies

- Host scanning strategy
  - The goal is to choose addresses of potentially vulnerable machines to scan.
  - Random Scanning
    - high traffic volume of internetwork traffic
    - may aid detection
    - increase likelihood of duplicate scans
  - Hit List
    - splits off pieces of the list to give to newly recruited machines
    - can be very **fast and efficient**
    - **no collisions**
    - a large list will cause more traffic

DDoS Taxonomy: Agent Recruitment Strategies

- Host scanning strategy (cont.)
  - Permutation Scanning
    - if an agent sees an already infected host, it chooses a new **random** starting point
    - if an agent sees a certain threshold number of infected hosts, it becomes dormant
  - Signpost Scanning
    - uses communication patterns or data found on **newly infected hosts** to select next targets
      - any email worm that spreads using address book of infected host
    - hard to detect based on traffic patterns

DDoS Taxonomy: Agent Recruitment Strategies

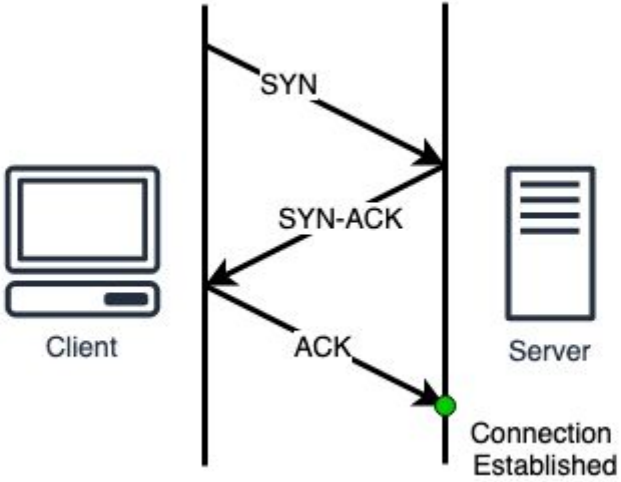
- Vulnerability Scanning strategy
  - go through chosen list of host addresses and probe for vulnerabilities
  - Horizontal
    - looks for **specific** port/vulnerability against a group of IPs
  - Vertical
    - look for multiple ports/vulnerabilities on the **same host**
  - Coordinated
    - scan **multiple** machines on the same subnet for a set of vulnerabilities
  - Stealthy
    - any of the above, but do it slowly to avoid detection

DDoS Taxonomy: Agent Recruitment Strategies

- Attack code propagation
  - Central Server (e.g., lion worm)
    - all newly recruited agents contact a central server to get attack code
    - single point of failure
      - can be discovered and shut down
      - high load at central server may limit efficiency or enable detection
  - Back-chaining (e.g., Ramen, Morris worms)
    - attack code downloaded from **machine that was used to exploit the new host**
  - Autonomous - (e.g., email worms)
    - attack code downloaded **concurrently** w/exploit

DDoS Taxonomy: Exploited Weakness

- Semantic (e.g., TCP SYN)
  - exploits a specific feature or bug of a protocol or application on the victim in order to **consume excessive amounts of its resources**
  - can potentially be mitigated by **deploying modified protocols/applications**

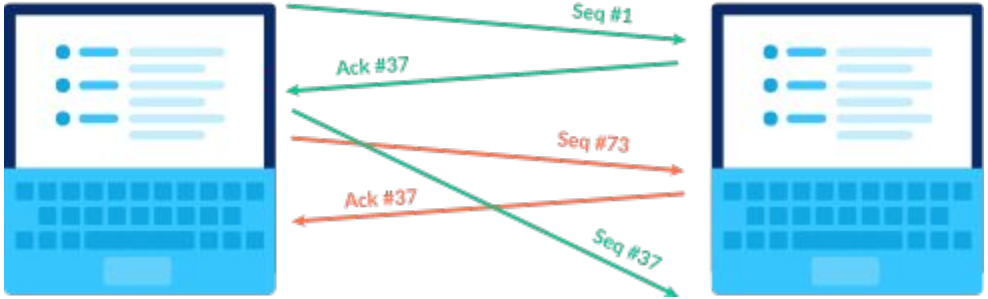


DDoS Taxonomy: Exploited Weakness

- Brute Force
  - intermediate network has more resources than victim
    - Example: control google server to attack IIT server
    - deliver **higher** volume of packets than victim can handle
  - overwhelm victim resources using seemingly legitimate packets
    - **hard to filter** without also harming legitimate traffic
  - requires higher volume of attack packets
    - modifying protocols to counter semantic attacks raises the bar for the attacker

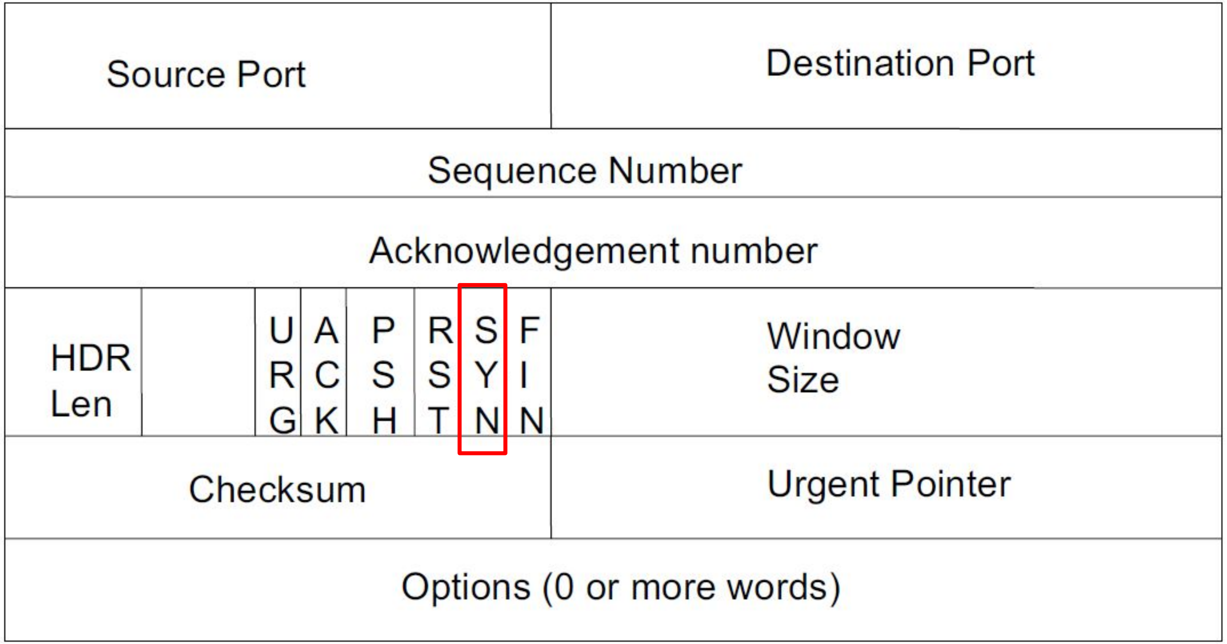
TCP

- Transmission Control Protocol (TCP)
  - Guarantees reliable, ordered stream of traffic -Such guarantees impose overhead
  - A fair amount of state is required on both ends
- **Most** Internet protocols use TCP
  - e.g., HTTP, FTP, SSH



TCP

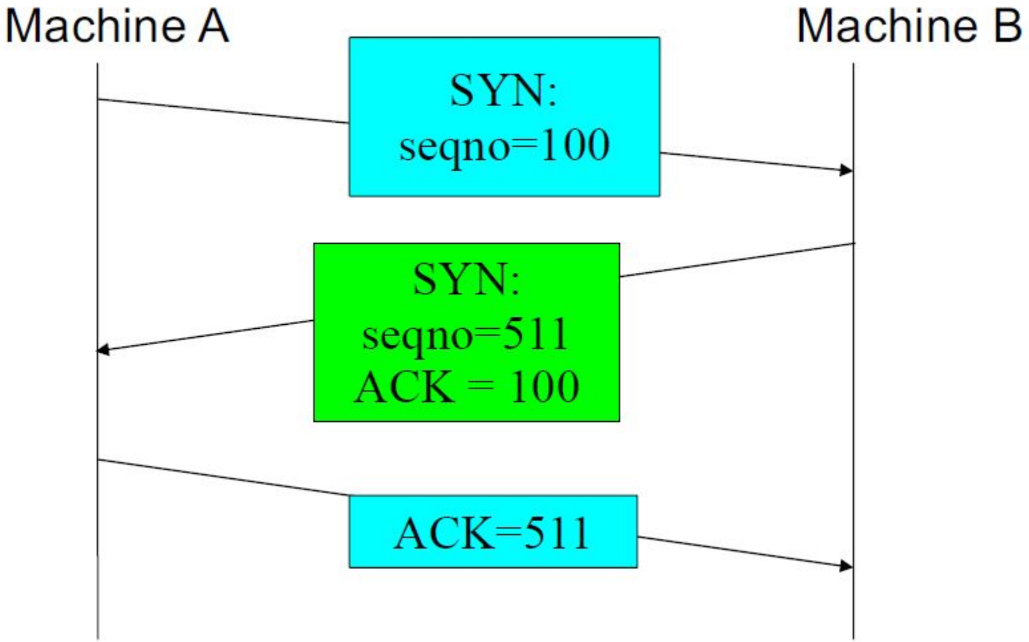
- TCP header



<table>
<tr><td colspan="8">Source Port</td><td>Destination Port</td></tr>
<tr><td colspan="9">Sequence Number</td></tr>
<tr><td colspan="9">Acknowledgement number</td></tr>
<tr><td>HDR Len</td><td></td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>Window Size</td></tr>
<tr><td colspan="8">Checksum</td><td>Urgent Pointer</td></tr>
<tr><td colspan="9">Options (0 or more words)</td></tr>
</table>

TCP

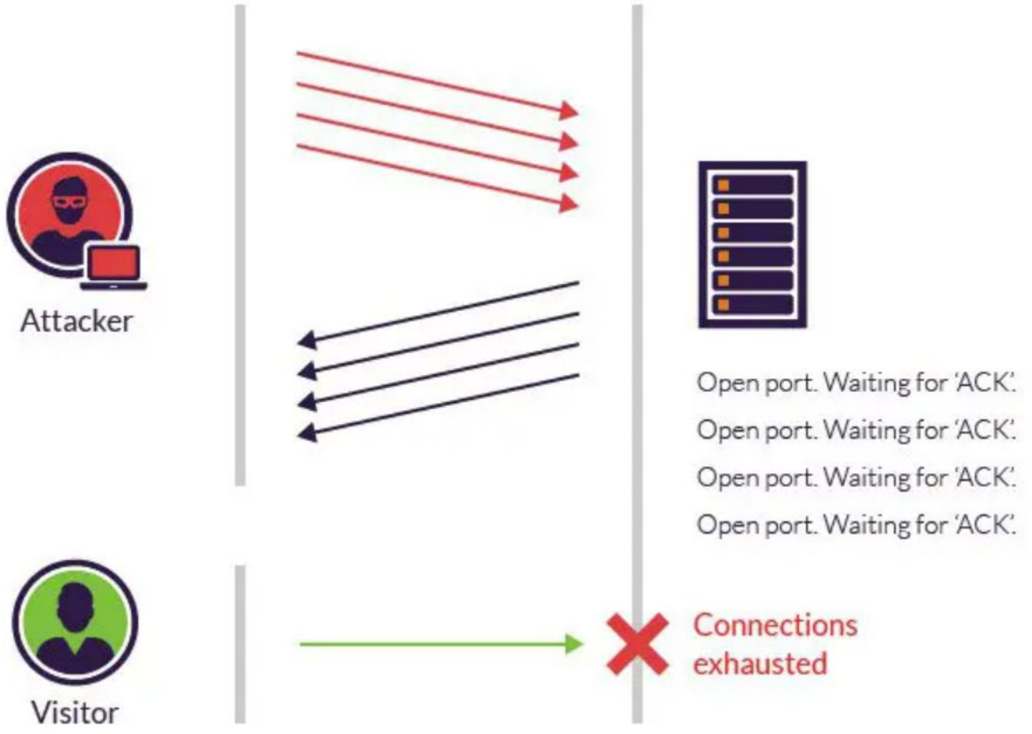
- Three way handshake



SYN Flood

- Attacker ===> **repeated** SYN packets to every port on the targeted server, often using a **fake IP address**
- The server ===> respond to **each attempt** with a SYN-ACK packet from **each open port**.
- Attacker
  - either does not send the expected ACK
  - or—if the IP address is spoofed—never receives the SYN-ACK in the first place
- The server
  - leaves an increasingly large number of connections half-open

SYN Flood


Attacker
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Visitor
Connections exhausted

DDoS Taxonomy: Source Address Validity

- Address Routability
  - routable source address attacks
    - **take over** the IP address of another machine
    - perform a reflector attack (e.g., smurf attack) on the machine whose address was hijacked
  - non-routable source address attacks
    - can belong to a reserved set of addresses (such as 192.168.0.0/16)
    - be part of an **assigned but not used** address space of some network

DDoS Taxonomy: Source Address Validity

- Spoofing Technique (cont.)
  - Random Spoofed Source Address
    - **easiest** method
    - can be prevented by ingress filtering and route-based filtering
  - Subnet Spoofed Source Address
    - spoof a random address from the address space assigned to the agent machine’s subnet
  - En Route Spoofed Source Address
    - spoof the address of a machine or subnet that lies along the path from the agent machine to the victim

DDoS Taxonomy

Reference: Mirkovic, Jelena, and Peter Reiher. "A taxonomy of DDoS attack and DDoS defense mechanisms." ACM SIGCOMM Computer Communication Review 34.2 (2004)

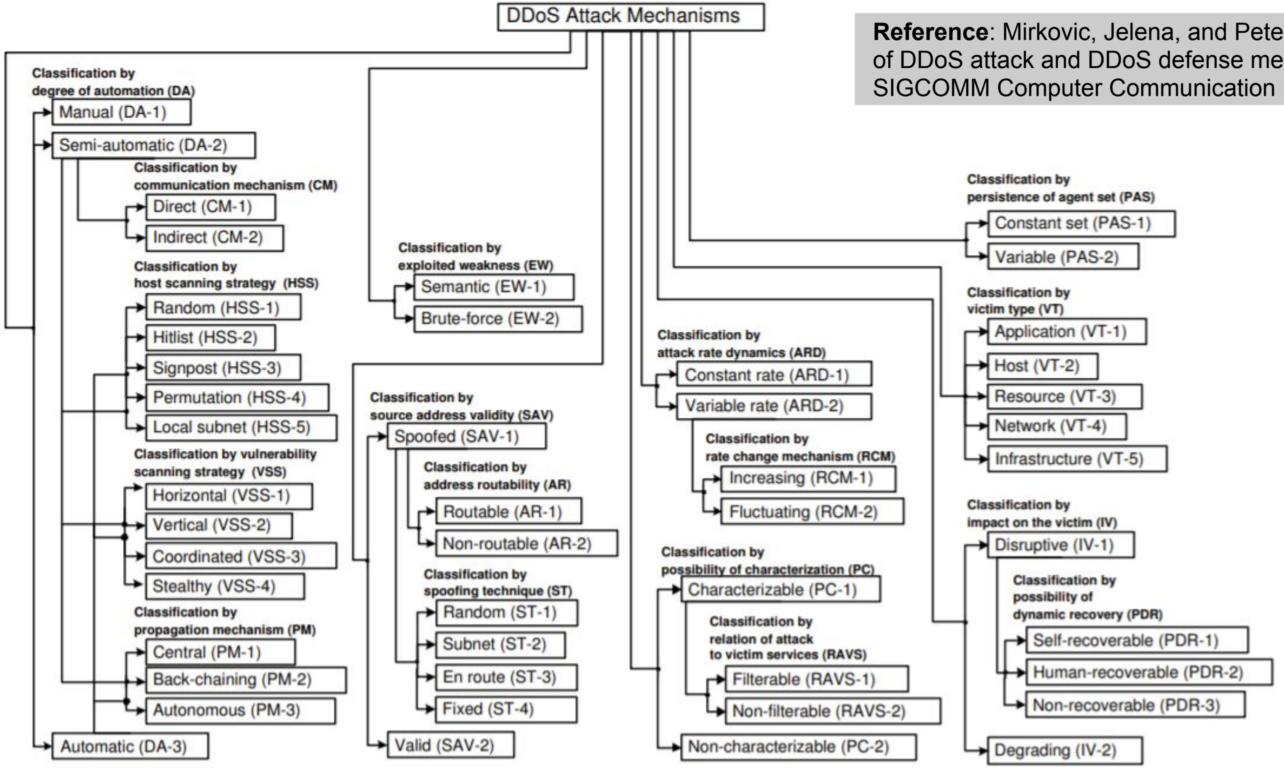

DDoS Attack Mechanisms
Classification by degree of automation (DA)
Manual (DA-1)
Semi-automatic (DA-2)
Classification by communication mechanism (CM)
Direct (CM-1)
Indirect (CM-2)
Classification by host scanning strategy (HSS)
Random (HSS-1)
Hitlist (HSS-2)
Signpost (HSS-3)
Permutation (HSS-4)
Local subnet (HSS-5)
Classification by vulnerability scanning strategy (VSS)
Horizontal (VSS-1)
Vertical (VSS-2)
Coordinated (VSS-3)
Stealthy (VSS-4)
Classification by propagation mechanism (PM)
Central (PM-1)
Back-chaining (PM-2)
Autonomous (PM-3)
Automatic (DA-3)
Classification by exploited weakness (EW)
Semantic (EW-1)
Brute-force (EW-2)
Classification by source address validity (SAV)
Spoofed (SAV-1)
Classification by address routability (AR)
Routable (AR-1)
Non-routable (AR-2)
Classification by spoofing technique (ST)
Random (ST-1)
Subnet (ST-2)
En route (ST-3)
Fixed (ST-4)
Valid (SAV-2)
Classification by attack rate dynamics (ARD)
Constant rate (ARD-1)
Variable rate (ARD-2)
Classification by rate change mechanism (RCM)
Increasing (RCM-1)
Fluctuating (RCM-2)
Classification by possibility of characterization (PC)
Characterizable (PC-1)
Classification by relation of attack to victim services (RAVS)
Filterable (RAVS-1)
Non-filterable (RAVS-2)
Non-characterizable (PC-2)
Classification by persistence of agent set (PAS)
Constant set (PAS-1)
Variable (PAS-2)
Classification by victim type (VT)
Application (VT-1)
Host (VT-2)
Resource (VT-3)
Network (VT-4)
Infrastructure (VT-5)
Classification by impact on the victim (IV)
Disruptive (IV-1)
Classification by possibility of dynamic recovery (PDR)
Self-recoverable (PDR-1)
Human-recoverable (PDR-2)
Non-recoverable (PDR-3)
Degrading (IV-2)

Figure 1: Taxonomy of DDoS Attack Mechanisms

THANK YOU!
QUESTIONS?