Cybersecurity (Security+) and P4 Programmable Switches

Overview Cybersecurity Labs

Ali AlSabeh, Jorge Crichigno
University of South Carolina
http://ce.sc.edu/cyberinfra

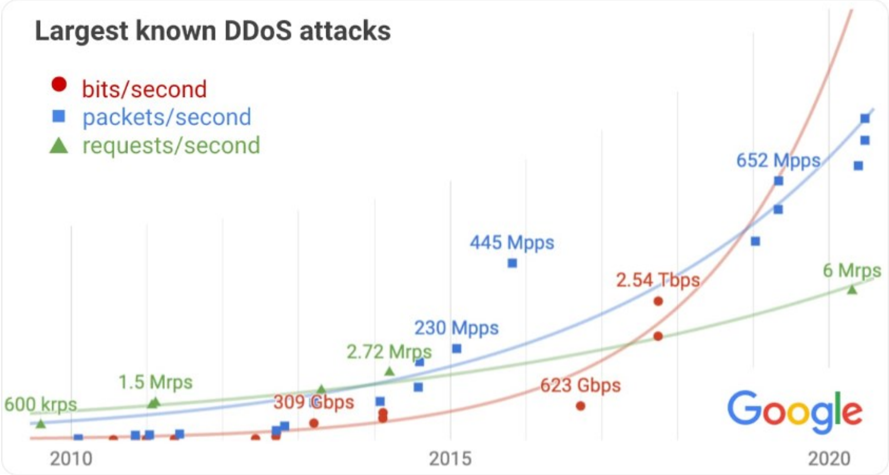
Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 20th, 2023

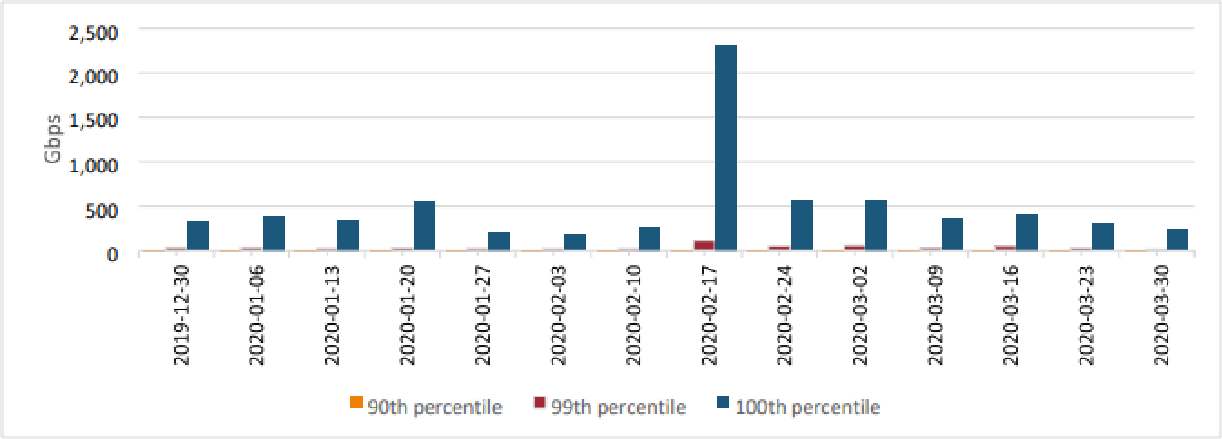
Denial of Service (DoS) and Distributed DoS (DDoS) Attacks

Denial of Service Attack (DoS)

- A Denial of Service (DoS) attack aims to render a server or a device unavailable to legitimate users by interrupting the device's normal services[1]
- A Distributed DoS (DDoS) is a type of DoS that originates from multiple distributed sources (e.g., botnet DDoS attack), thus, amplifying the effect of DoS



Largest known DDoS attacks in Google Cloud between 2010 and 202. [Figure taken from Google Cloud blogs. https://tinyurl.com/bdzuupb6]

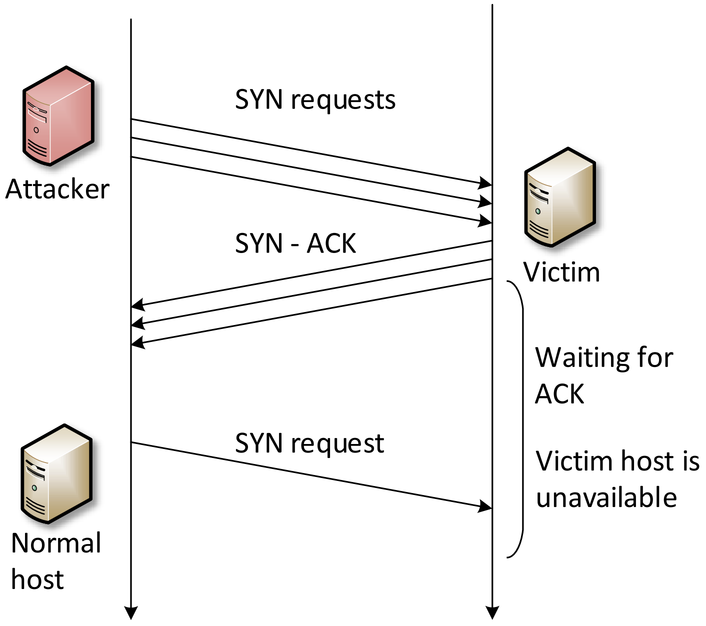


Packet volume of the largest network volumetric events observed by AWS in Q1 2020. [Figure taken from AWS Shield Report. https://tinyurl.com/yd3ehx47]

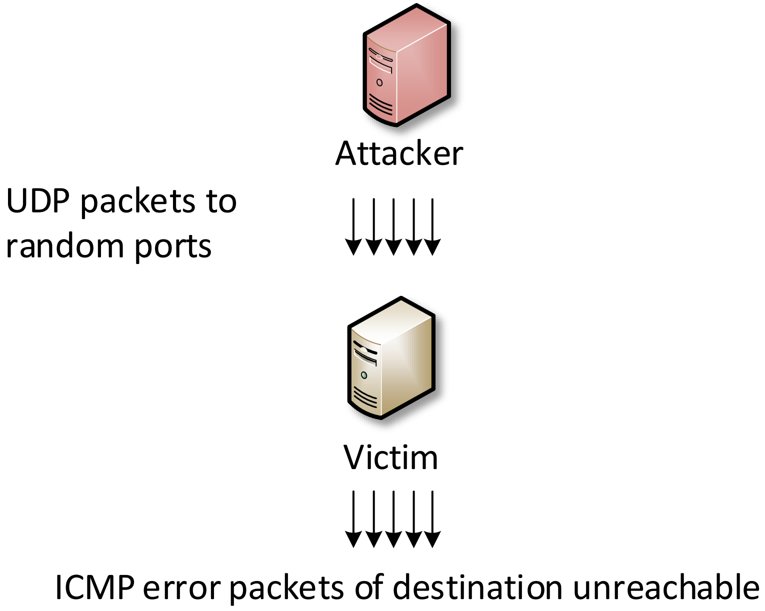
[1] Cloudflare, "What is a denial-of-service (DoS) attack?", [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

Types of DoS Attacks

- DoS attacks can be classified as volumetric, reflected, and stealthy DoS attacks
- Volumetric DoS attacks flood the target machine with traffic, depriving legitimate users from downloading the target's resources
- DoS attacks can be performed at various levels of the protocol stack (e.g., TCP, UDP)



TCP SYN flood attack

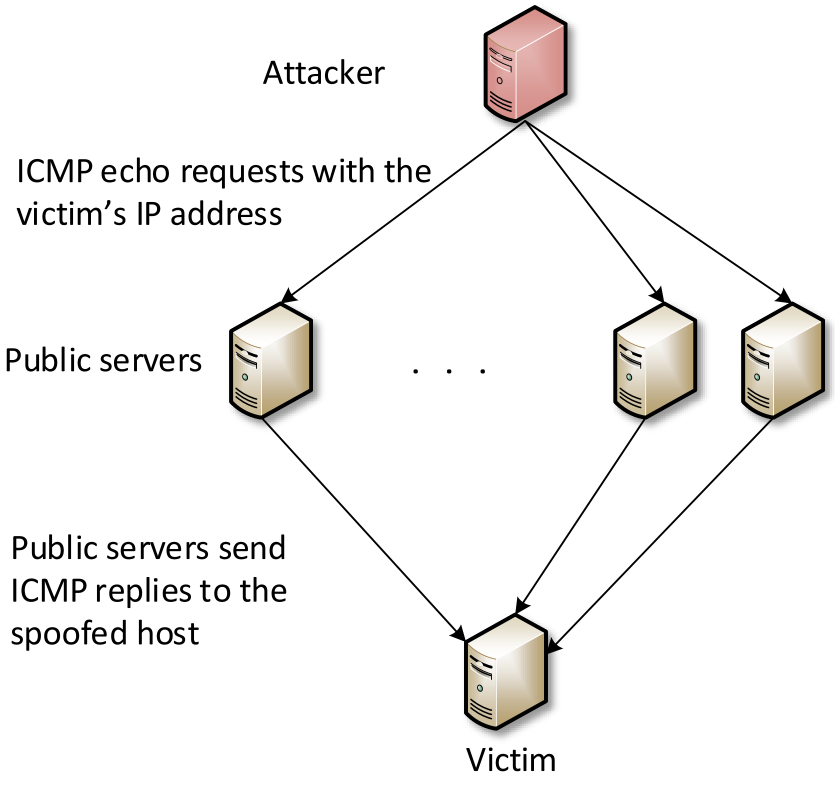


Attacker
UDP packets to random ports
Victim
ICMP error packets of destination unreachable

UDP flood attack

Types of DoS Attacks

- Reflected DoS attacks (amplification attacks) make use of a third-party component to send the attack traffic to a victim, ultimately hiding the attacker's own identity
- In a reflected DoS attack
  - ➢ The attacker spoofs the source IP address of the target victim machine
  - ➢ The reflector sends response packets that overwhelm the victim
- *Smurf* reflected DoS attack uses ICMP echo requests and public servers to overwhelm a target victim

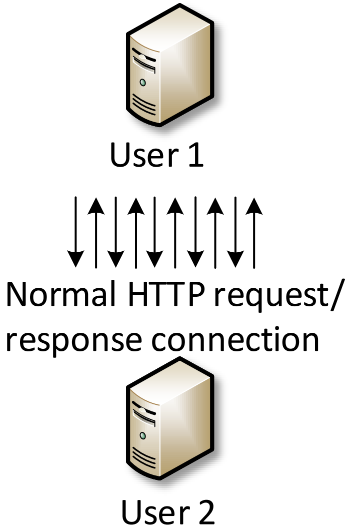


Attacker
ICMP echo requests with the victim's IP address
Public servers
. . .
Public servers send ICMP replies to the spoofed host
Victim

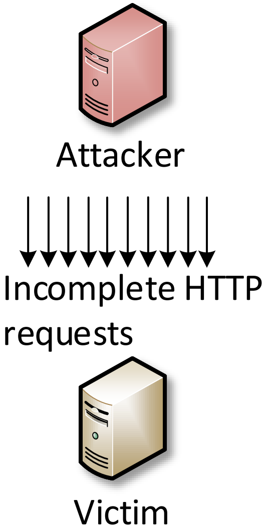
Smurf reflected DDoS attack

Types of DoS Attacks

- Stealthy DoS attack (slow DoS) use low bandwidth rates when targeting a victim
- *SlowLoris* attack establishes many connections to a target server and holds them as long as possible
- *SlowLoris* sporadically sends partial requests to keep the session active



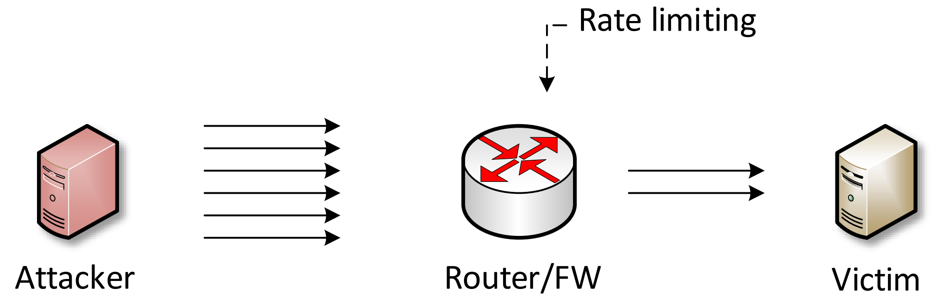
Normal connection: complete HTTP request/response connections



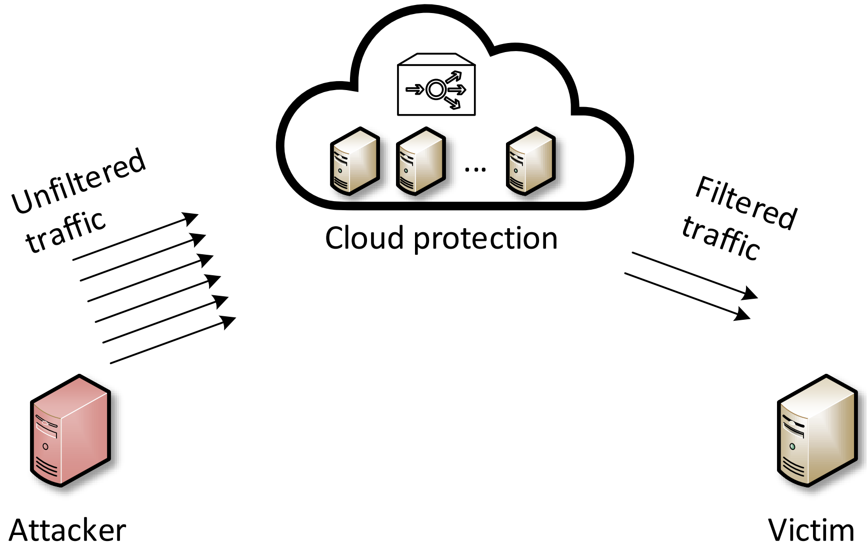
SlowLoris attack: incomplete HTTP requests

DoS Mitigation

- DoS mitigation refers to the process of successfully protecting a targeted server or network from a DoS attack
- Traditional DoS mitigation strategies include purchasing and maintaining expensive equipment
- Modern infrastructure rely on cloud providers to provide DoS mitigation services[1]



Rate limiting against DoS attacks

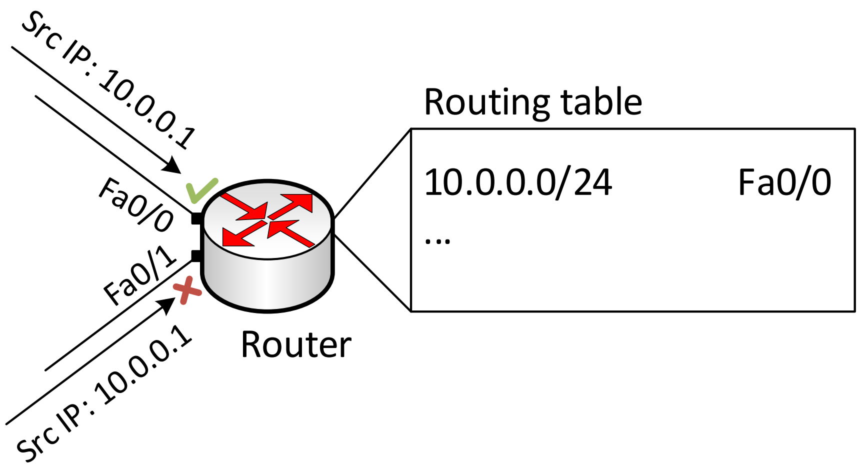


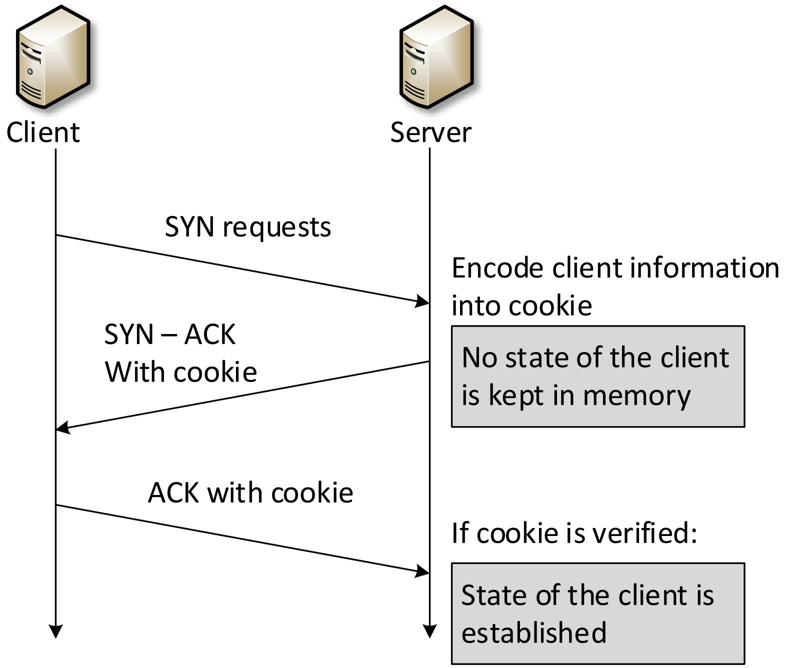
Cloud-based DoS protection

[1] Cloudflare, “What is DDoS mitigation?”, [Online]. Available: https://www.cloudflare.com/learning/ddos/ddos-mitigation/

DoS Mitigation

- Additionally, operating systems provide some level against DoS attacks
  - In Linux, the following techniques are implemented:
    - Reverse path filtering: prevents IP spoofing associated with DoS attacks
    - SYN cookie: prevents against SYN flood attacks
    - Session's caching: allows for rapid recent TCP sessions to




Client
Server
SYN requests
Encode client information into cookie
SYN – ACK
With cookie
No state of the client is kept in memory
ACK with cookie
If cookie is verified:
State of the client is established