CS 419: Computer Security

Week 13: Network Attacks
DDoS: Amplification Attacks
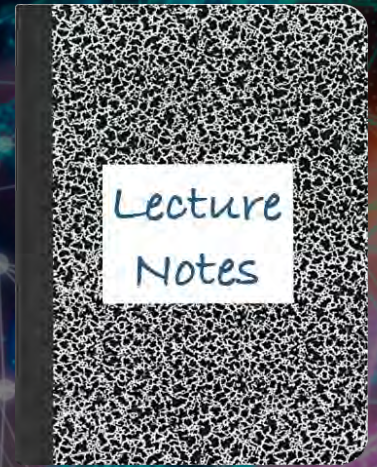
Paul Krzyzanowski

Lecture Notes

Denial of Service (DoS) Attacks

- **Find bugs**
  - Get the system to crash

- **Overwhelm a system so it will not be responsive**

  Challenge: overwhelm targets that may be far bigger than you

  - **Find asymmetries**
    - Cases where handling requests is more expensive than issuing them
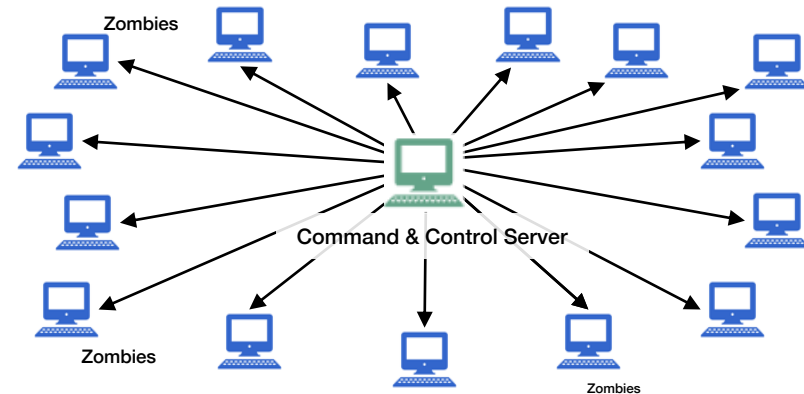 - **Avoid getting responses**
    - Fake return addresses
  - **Send responses to the target**
    - Set the return address to the target ⇒ amplification
  - **Join forces**
    - Get many systems to participate ⇒ create a **botnet** for a **Distributed DoS (DDoS)** attack
    - Systems contact a **command & control server** for directions

Zombies

Command & Control Server

Zombies

Zombies

Forms of overwhelming a system for DoS

- **Volumetric attack**
  - Generate more traffic than the target's network link(s) can handle

- **Packet-per-second focused attack**
  - Generate a higher packet rate than an application (or OS or routers) can process

Bugs & Asymmetric attacks

- **Challenge Collapser**
  - Attacker sends URLs that require time-consuming operations on the server

- **ICMP attacks**
  - Ping flood
    - Send ICMP Echo Request messages with responses that go to the target
  - Ping of Death
    - Send fragmented IP packets so that they will be >64KB when reassembled ⇒buffer overflow
  - Send spoofed source addresses to unreachable destinations
    - Routers will return *Destination Unreachable* to the target

Amplification Attacks

Goal: send a small request that produces a large response

Reflection amplification attack
- Attacker spoofs target's IP address
- Sends request to a service — server responds to the target
- Need UDP so there's no connection state

Amplification attacks generate a lot of traffic for targets
- Magnify the response size relative to the request
- Obscure the origin of the attack
- Exploit services that generate a lot of traffic to a small query

Some services vulnerable to amplification attacks

Memcached
– Attacker enters a large payload onto an exposed memcached server
– Spoofs an HTTP GET request with IP address of target (often requesting web cache data)
– Amplification factor: up to 51,200

Network Time Protocol (NTP)
– *Monlist* command causes NTP to respond with the last 600 source IP addresses of requests which have been made to the server
– Amplification factor: 556

Domain Name System (DNS) Server
– Send a DNS lookup request for as much info as possible with a spoofed source address
– Amplification factor: 50 - 179

Datagram TLS (D/TLS; TLS over UDP)
– Because it's UDP (connectionless), protocol is spoofable
– Affects misconfigured servers: attackers send small DTLS packets and get large responses sent to spoofed addresses
– Amplification factor: 37

CLDAP (Microsoft derivative of the Lightweight Directory Access Protocol over UDP)
– Affects Windows servers running domain controllers with CLDAP enabled and exposed on the public Internet [link]
– Amplification factor: 56 - 70

Amplification Vectors

The evolution of DDoS reflection amplification vectors: a chronology — ©Link11 — www.link11.com

https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/

Application-Layer Loop DoS

- **Spoof UDP packets to cause a pair of systems to communicate indefinitely**
  - Affects DNS, DTP, TFTP, and other protocols
  - First documented in March 2024

- **A trigger message with a spoofed source IP address is sent to one target**
  - It responds to the service in the spoofed source IP address, which creates and endless sequence of back-and-forth responses
  - E.g., send a spoofed error message to a TFTP server, that will respond back with an error to another TFTP server, which will respond back, …

- **Puts 300,000+ systems at risk**

See: https://cispa.de/en/loop-dos

DDoS: Distributed Denial of Service

- **A DDoS attack is one where many systems attack a target**
  - This provides a better opportunity for overwhelming the target with traffic
  - Many systems can generate more data than one and aren't limited by the network bandwidth of any one system

- **Huge numbers of compromised systems reduce need for amplification**
  - The network of attackers is a collection of millions of compromised machines
  - Each system waits for directions from a command & control server
  - Blocking a distributed attack is harder because the data doesn't come from one IP address or one set of addresses

- **Some targets are too huge to hurt with traffic**
  - Amazon, Google, sites using CDNs such as Akamai

AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever

2020

The previous record for the largest DDoS attack ever recorded was of 1.7 Tbps, recorded in March 2018.

Catalin Cimpanu • June 17, 2020

Amazon said its AWS Shield service mitigated the largest DDoS attack ever recorded, stopping a 2.3 Tbps attack in mid-February this year.

The incident was disclosed in the company's AWS Shield Threat Landscape, a report detailing web attacks mitigated by Amazon's AWS Shield protection service.

The report didn't identify the targeted AWS customer but said the attack was carried out using hijacked CLDAP web servers and caused three days of "elevated threat" for its AWS Shield staff.

CLDAP (Connection-less Lightweight Directory Access Protocol) is an alternative to the older LDAP protocol and is used to connect, search, and modify Internet-shared directories.

The protocol has been abused for DDoS attacks since late 2016, and CLDAP servers are known to amplify DDoS traffic by 56 to 70 times its initial size, making it a highly sought-after protocol and a common option provided by DDoS-for-hire services.

https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/

Two record DDoSes disclosed this week underscore their growing menace

More bots + better DDoS traps = ever-growing amounts of junk traffic.

Dan Goodin • June 25, 2020

The race upward is showing no signs of slowing. Last week, Amazon reported that its AWS Shield DDoS mitigation service went head-to-head with a 2.3 Tbps attack, a 35-percent increase over the 2018 record. Meanwhile, network provider Akamai said on Thursday that its Prolexic service repelled a DDoS that generated 809 million packets per second. That's a 35-percent increase over what's believed to be the previous high-water mark of the 600Mpps DDoS that Roland Dobbins, principal engineer at competing mitigation service Netscout Arbor, said his company handled.

"We anticipate continued innovation in the area of DDoS attack vectors due to the various financial, ideological, and social motivations of attackers," Dobbins told me. "DDoS attacks allow attackers to have a hugely disproportionate negative impact on both the intended targets of attacks, as well as uninvolved bystanders."

The attack, which Akamai said hit an unnamed European bank, was notable for how quickly it ramped up. As the image below illustrates, attackers needed less than three minutes to unleash its peak of 809 Mpps.

https://arstechnica.com/information-technology/2020/06/two-record-ddoses-disclosed-this-week-underscore-their-growing-menace/

Google Cloud Stops Monster DDoS Attack

Google successfully fended off an HTTPS Distributed Denial of Service (DDoS) attack, which peaked at 46 million requests per second (RPS) -- the largest Layer 7, the application layer, DDoS reported to date.

Steven Vaughan-Nichols • August 22, 2022

Distributed Denial of Service (DDoS) attacks don't need to be big to wreak havoc on a target, but it doesn't hurt. In the latest biggest of all times attacks, Google fended off an HTTPS DDoS attack, which peaked at 46 million requests per second (RPS). That made it the largest Layer 7, the application layer, DDoS reported to date. It was 76% larger than the previously reported record.

So how big is that? Imagine a day's worth of requests to Wikipedia hammering down in just 10 seconds.

Yeah, that's a lot.

Welcome to the 2022 internet. A few weeks earlier, Cloudflare had beat off a then record 26 million RPS DDoS attack. Before that, Cloudflare, in August 2021, handled a 17.2M RPS HTTP DDoS attack. Gigantic DDoS attacks are happening ever more often. These put the top DDoS attacks of the past to shame.

https://thenewstack.io/google-cloud-stops-monster-ddos-attack/

Microsoft fends off record-breaking 3.47 Tbps DDoS attack

While a crude brute-force attack, DDoSes are growing ever more potent.

Dan Goodin • January 28, 2022

The company's Azure DDoS Protection team said that in November, it fended off what industry experts say is likely the biggest distributed denial-of-service attack ever: a torrent of junk data with a throughput of 3.47 terabits per second. The record DDoS came from more than 10,000 sources located in at least 10 countries around the world.

The DDoS targeted an unidentified Azure customer in Asia and lasted for about two minutes. The following month, Microsoft said, Azure warded off two other monster DDoSes. Weighing in at 3.25Tbps, the first one came in four bursts and lasted about 15 minutes.

… The 3.7Tbps attack delivered roughly 340 million packets per second.

…

Sadly, the Internet is awash with millions of misconfigured servers that make reflection amplification attacks possible. These Internet nuisances played a big role in the 3.47Tbps attack Microsoft reported.

…

Most of those attacks came from Internet-of-Things devices infected with the open source Mirai botnet malware and lower-volume UDP protocol attacks. The vast majority were UDP spoof floods. A much smaller portion used UDP reflection and amplification, mostly SSDP, memcached, and NTP.

https://arstechnica.com/information-technology/2022/01/microsoft-fends-off-record-breaking-3-47-tbps-ddos-attack/

Google Cloud, AWS, and Cloudflare report largest DDoS attacks ever

2023

The attack on Google Cloud was 7½ times larger than any previously recorded DDoS attack. Here's what else you need to know

Steven Vaughan-Nichols • October 10, 2023

The Google Cloud was hit by the largest DDoS attack in history this past August, with the digital onslaught peaking at an unprecedented **398 million requests per second (RPS).** How big is that? According to Google, in two minutes, the Google Cloud was slammed by more RPS than Wikipedia saw in all of September 2023.

That's big. The attack on Google Cloud, which employed a novel "Rapid Reset" technique, was 7½ times larger than any previously recorded DDoS attack. 2022's largest-recorded DDoS attack peaked at "only" 46 million RPS.

Google wasn't the only one to get hit. Cloudflare, a leading cloud delivery network (CDN), and Amazon Web Services (AWS), the world's biggest cloud provider, also reported getting blasted. Cloudflare fended off a 201 million RPS attack, while AWS held off a 155 million RPS assault.

https://www.zdnet.com/article/google-cloud-aws-and-cloudflare-report-largest-ddos-attacks-ever/

Cloudflare blocks largest recorded DDoS attack peaking at 3.8Tbps

Ionut Ilascu • October 3, 2024

During a distributed denial-of-service campaign targeting organizations in the financial services, internet, and telecommunications sectors, volumetric attacks peaked at 3.8 terabits per second, the largest publicly recorded to date. The assault consisted of a "month-long" barrage of more than 100 hyper-volumetric DDoS attacks flooding the network infrastructure with garbage data.

In a volumetric DDoS attack, the target is overwhelmed with large amounts of data to the point that they consume the bandwidth or exhaust the resources of applications and devices, leaving legitimate users with no access.

Asus routers, MikroTik devices, DVRs, and web servers
Many of the attacks aimed at the target's network infrastructure (network and transport layers L3/4) exceeded two billion packets per second (pps) and three terabits per second (Tbps).

According to researchers at internet infrastructure company Cloudflare, the infected devices were spread across the globe but many of them were located in Russia, Vietnam, the U.S., Brazil, and Spain.

https://www.bleepingcomputer.com/news/security/cloudflare-blocks-largest-recorded-ddos-attack-peaking-at-38tbps/

A new DDoS record in 2024

In 2024, Cloudflare mitigated the largest distributed denial-of-service (DDoS) attack ever reported, ==an attack that reached 5.6 terabits per second (Tbps) and 666 million packets per second at its peak==. The attack lasted about 80 seconds and was part of a larger ongoing campaign of hyper-volumetric DDoS attacks. The Cloudflare network automatically mitigated the 5.6 Tbps attack and all other attacks that were part of the campaign, protecting Cloudflare customers.

https://www.cloudflare.com/learning/ddos/famous-ddos-attacks

Dealing with DDoS

Really difficult in general

- **Disable unnecessary UDP services**
  - So you're not a participant in the attacks

- **Enable bandwidth management in routers**
  - Either in data center or ISP
  - Limit outbound or inbound traffic on a per-IP basis

- **Blackhole routing**
  - Set a **null route** route when DNS attack was detected
  - Traffic to attacked DNS goes nowhere

- **Egress filtering by ISPs**
  - Attempt to find malicious hosts participating in DDoS or sending spam

- **Identify incoming attackers & block traffic at firewall**
  - Difficult with a truly distributed DDoS attack

The End