Introduction to DoS and DDoS Attacks

Setting the Stage

Klaus Möller
WP8-T1 - EaPConnect

Webinar, November 2021

Public

www.geant.org

Game Plan

- Denial-of-Service concepts
- Distributed DoS specialties
- Considerations from the attackers and defenders points of view
- Questions/discussion/open mike session

Denial of Service Concepts

Public

www.geant.org

What is a Denial-of-Service Attack?

- A Denial-of-Service (DoS) attack **denies** the **normal usage** of a **service**
- The target might want to **use** the service or want to **provide** the service:
  - An attacker might overload the mail server so the employees cannot access their mail
  - An attacker might overload the web server of a company so (potential) customers cannot access important information
- So for this talk, we will call the affected service the “victim”

“Real-World” Analogy

By way of analogy, consider a vaccination center as the service that is attacked:

- An attacker might want to deny people the benefits of vaccination. In this case, the intended targets of the attack are the patients.
- The intention might also be to make the government look bad because it cannot even make sure the people get vaccinated on time. In this case, the intended target is the government.

In either case, identical attack methods can be used, and collateral damage is identical as well.

How Service Can Be Denied

"Denial of Service" is a **very** generic concept and does not specify any technical details at all. (At least) the following layers can be attacked:

- Metadata/prerequisite data
- Network information
- Network components and resources
- Systems and system resources
- Applications and application resources

Metadata/Prerequisite Data

- Any information that is required to use a particular service
- Examples:
  - DNS resolution
  - NTP synchronisation
  - OCSP lookups
  - Kerberos tickets
- Vaccination center: Published location

Network Information

- Necessary information for network traffic to reach the victim service
- Examples:
  - Routing information
  - Peering relationships
- Vaccination center: Road signs

Network Components and Resources

- Components and resources that are necessary for network traffic to reach the victim system
- Components can be crashed, resources can be exhausted
- Examples:
  - Link bandwidth
  - Router Forwarding Information Base capacity
  - Firewall connection state table capacity
- Vaccination center: Road capacity

Systems and System Resources

- Victim systems and resources on them that are necessary to provide the service
- Systems can be crashed, resources can be exhausted.
- Examples
  - Memory
  - CPU capacity
  - Disk drive availability
- Vaccination center: Parking lot capacity

Applications and Application Resources

- Victim applications and resources in them that are necessary to provide the victim service
- Applications can be crashed, resources can be exhausted
- Examples:
  - Application threads
  - Connection handles
  - Buffer capacity
- Vaccination center: Vaccination booth capacity

Enhancing the game: Efficiency improvements

Public

www.geant.org

Mirrors

Observation: To avoid attribution and make defense harder, an attack should (appear to) come from many sources simultaneously

Idea: Use third-party services to **reflect** network traffic to the victim (**reflectors**)

Examples:

- DNS
- NTP
- ICMP

Magnifying Glasses

To exhaust resources, large amounts of traffic must be generated - this is hard

Idea: Use third-party services that not only reflect, but also **amplify** traffic (**amplifiers**)

Examples:

- memcached (amp factor: up to ~50000)
- NTP (amp factor: up to ~500)
- DNS (amp factor: up to ~50)

(Source: https://us-cert.cisa.gov/ncas/alerts/TA14-017A)

Crowdsourcing

Observation: Amplification attacks are also fairly hard to pull off nowadays

Idea: Use hacked third-party resources for more direct DoS attacks instead. These computers are called **bots** or **zombies**; a "network" of bots under central control is called a **botnet**.

Examples:

- Dark Nexus
- Smominru
- Mirai

Bots as a Service

Observation: Creating a botnet is very hard and requires skill, tools and time, which most attackers do not have.

Idea: Have skilled hackers specialize in creating botnets (**botherders**) and rent botnets to attackers for money. Additional toolsets (**booters**) to make launching attacks easier are also helpful to help the attackers.

Putting things into perspective: Attackers' and victims' point of view

Public

www.geant.org

Offensive Thinking

- DoS attacks are suitable to hurt a target with relatively generic methods from afar
- Using amplifiers allows for much more powerful attacks
- Using reflectors allows the attacker to stay in the shadows
- DDoS attacks combine all of the above advantages: Very powerful, yet very hard to track and defend against

Attacker Motivation

Common attacker types and their objectives:

- Criminals: Extorting ransom from the target for financial gain
- Hacktivists: Punishing a target for ideological or even personal reasons
- Nation-states or equivalent: Disrupting a target for political benefit

Defensive Thinking

- Depending on the particular attack and skill level, DoS attacks are a very serious threat
- It is very hard or even impossible for the victim to defend itself against DDoS attacks without external help
- Attribution is rather difficult

Possible Consequences

(D)DoS attacks can have rather nasty consequences for the victim:

- Immediate: Critical services with real-life impact
- Financial: Dealing with the attack, restoring services, ransom, loss of revenue
- Reputation: Being perceived as incompetent or helpless

Things Left to Do

Topics that will be covered in the talks ahead:

- What are the juicy technical details of the most common DDoS attacks?
- How can you detect DDoS attacks?
- What can you do against DDoS attacks?

Thank you

Any questions?

Next session: November, 2021:

“Details of Selected DDoS Attacks”

www.geant.org

The research leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).