INFS 5115 Security Principles

Denial of Service

University of South Australia

School of
Information Technology
and Mathematical Sciences

Denial of Service

- In this module, we will discuss the concept of Denial of Service attacks, including a classification of some of the more common practical attacks.
- We will also look at the effect of Distributed Denial of Service attacks through some recent case studies.
- Finally, a selection of mitigations will be outlined.

Denial of Service

Definition

- Denial of Service (DoS)
  - *The **prevention** of authorized access to resources or the **delaying** of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)*[1]

[1] CNSSI-4009 cited in Kissel, R., 2013. Glossary of Key Information Security Terms. NIST Interagency Reports, NISTIR 7298.

Number of DDoS per year

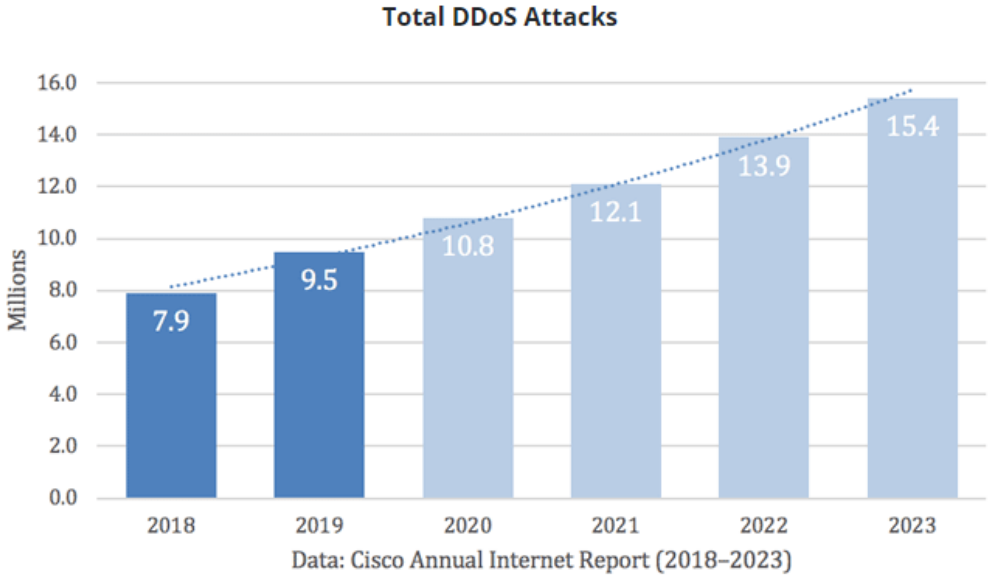
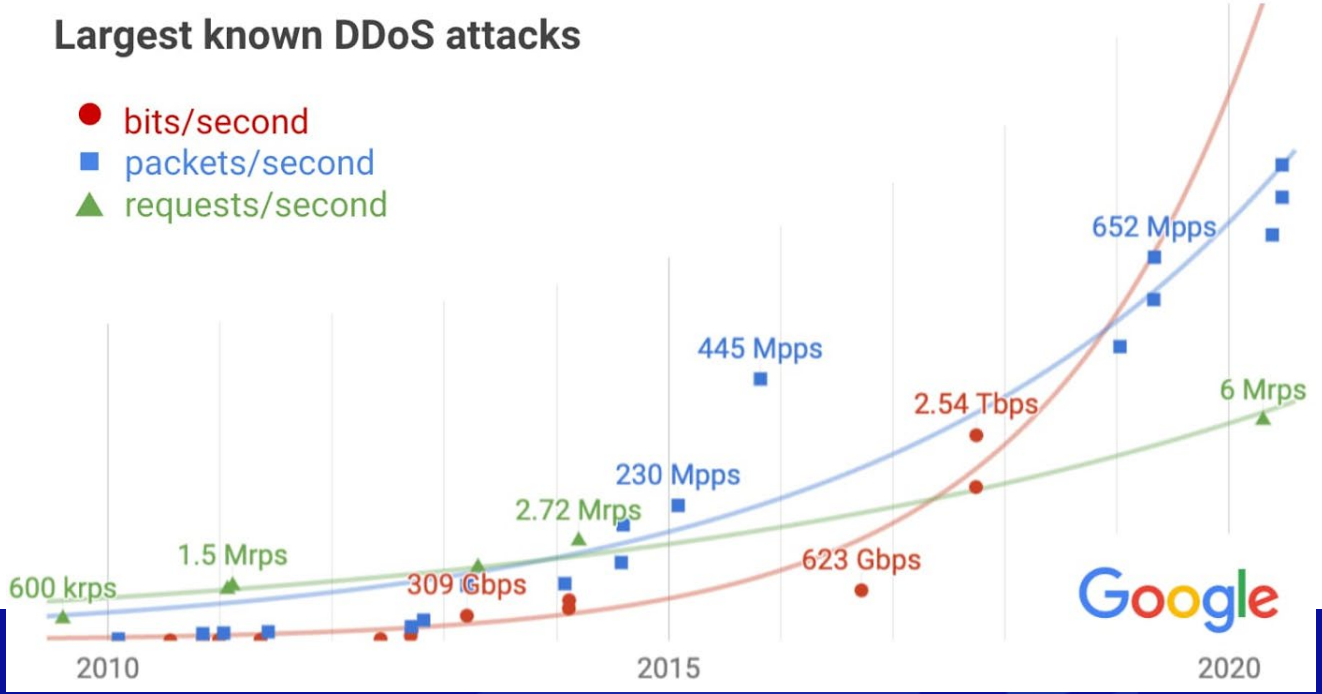


Figure 1. Cisco's analysis of DDoS total attacks history and predictions.

Source: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

Modified from: Cisco Annual Internet Report (2018 - 2023), p. 22
https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf

Trends in DDoS attack volumes



Exponential growth in DDoS attack volumes, Google Cloud https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks, viewed 08/05/2021

Denial of Service

- Many (although not all) DoS attacks are conducted remotely via a network service.

- Types of DoS attacks include
  - Flooding
  - Resource starvation/exhaustion
  - Improper configuration exploits
  - Distributed Denial of Service (DDoS)

Graham, J, Olson, R, & Howard, R (eds) 2010, Cyber Security Essentials, CRC Press, Boca Raton. (Chapter 3 - Exploitation)

Denial of Service

Classification

- One common example is consuming all of the network bandwidth available to a remote server with attacker controlled network traffic. This technique is known as ***flooding.***

See Activity 1 (under week 9) – Flooding Techniques.

Graham, J, Olson, R, & Howard, R (eds) 2010, Cyber Security Essentials, CRC Press, Boca Raton. (Chapter 3 - Exploitation)

Denial of Service

- ***Resource starvation*** is another similar form of DoS attack.
  - This involves the overutilization of system resources, including processing, memory and storage.
  - This type of attack can be accomplished in several different ways and can cause the targeted system to fail.

Graham, J, Olson, R, & Howard, R (eds) 2010, Cyber Security Essentials, CRC Press, Boca Raton. (Chapter 3 - Exploitation)

Denial of Service

- ***Improper configuration*** of services can facilitate DoS attacks, however it can also be the cause of a DoS condition. These services are often exploited as part of application layer attacks.
- For example, an authentication system that locks out users due to excessive authentication failures can be manipulated by an attacker to DoS legitimate users.
- A 2008 DoS affecting YouTube was caused by an ISP directing all internet traffic destined for YouTube to its routers due to an erroneous BGP (routing protocol) advertisement.

Graham, J, Olson, R, & Howard, R (eds) 2010, Cyber Security Essentials, CRC Press, Boca Raton. (Chapter 3 - Exploitation)

Distributed Denial of Service

- Many attacks rely upon the attacker having more resources (particularly bandwidth) than the target.
- This is often achieved by conducting a distributed and coordinated attack known as a ***Distributed Denial of Service (DDoS)*** attack.
- This style of attack can be more concerning than a traditional DoS attack, as it can be very difficult to defend against.

Graham, J, Olson, R, & Howard, R (eds) 2010, Cyber Security Essentials, CRC Press, Boca Raton. (Chapter 3 - Exploitation)

Distributed Denial of Service

- ***Botnets*** are commonly leveraged for the purpose of conducting DDoS attacks.
  - Botnets allow attackers to combine the resources of numerous relatively small resources into a single large scale attack.
  - For example 1000 machines with a 10 megabit uplink (not uncommon with modern broadband connections) can saturate a 10 gigabit server connection.

Graham, J, Olson, R, & Howard, R (eds) 2010, Cyber Security Essentials, CRC Press, Boca Raton. (Chapter 3 - Exploitation)

Amplification Attack

- ***Amplification*** attacks can be used to magnify attack capabilities.
  - This is commonly achieved via spoofed (faked) IP addresses and a technique known as *reflection*.
  - The attacker spoofs the IP address of the target in numerous requests to an intermediary known as a *reflector*.
  - The reflector then replies to the target, due to the spoofed IP address, rather than the attacker.
  - These responses can flood the target's available resources.

Graham, J, Olson, R, & Howard, R (eds) 2010, Cyber Security Essentials, CRC Press, Boca Raton. (Chapter 3 - Exploitation)

Amplification Attack Case Study 1 – The Google Attack.

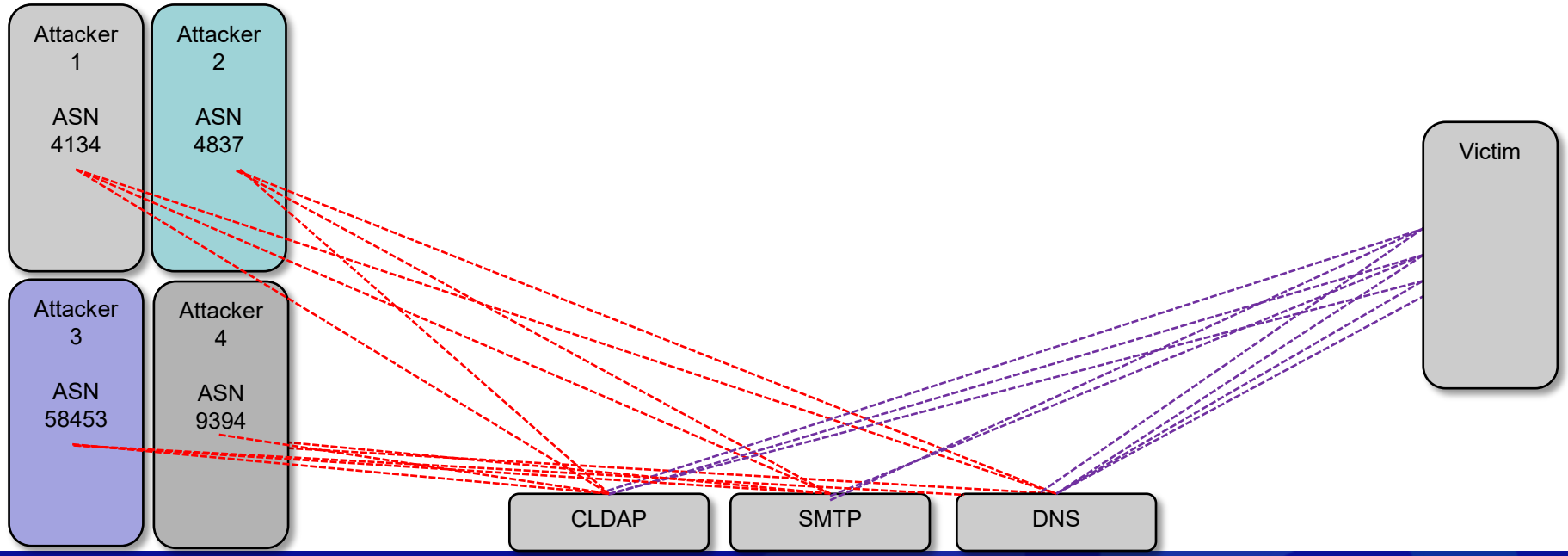
In 2017, Google's Security Reliability Engineering team measured a record-breaking UDP amplification attack sourced out of several Chinese ISPs (ASNs 4134, 4837, 58453, and 9394)

- The attack spoofed the IP address of the victim.
- The attack on thousands of Google's IP addresses lasted for six months
- The attacker used several networks to spoof 167 Mpps

Reflectors

https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

Amplification Attack Case Study 1 – The Google Attack.



https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

Botnet Attack Case Study 2 – The Mirai Krebs

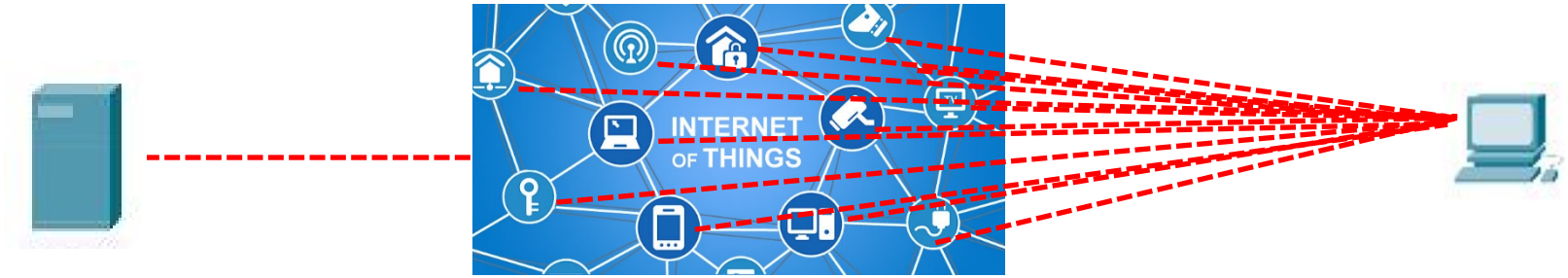
- A *botnet* is a collection of internet-connected computers — the "bots" — that are under remote control from some outside party.

- On September 20, 2016, the blog of cybersecurity expert Brian Krebs was assaulted by a DDoS attack in excess of 620 Gbps

- The source of the attack was the **Mirai** botnet, which, at its peak later that year, consisted of more than 600,000 compromised Internet of Things (IoT) devices such as IP cameras, home routers, and video players.

https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

Botnet Attack Case Study 2 – The Mirai Krebs



Distributed Denial of Service

- Utilising Malware to compromise high bandwidth servers is another attack method that must be considered.
  - Often vulnerabilities in server software will be revealed that could allow an attacker to install Malware that contains a DDoS attack tool as the payload.
  - Symantec found that the widespread ShellShock vulnerability was being exploited for the purpose of installing DDoS malware scripts within 24 hours of its publication.

Wueest, C 2014, 'The continued rise of DDoS attacks', Symantec Security Response, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/continued-rise-of-DDoS-attacks-14-en.pdf

Distributed Denial of Service

DDoS as a Service

- Similarly to Malware as a Service, ‘DDoS as a Service’ is a colloquial term used to describe the purchasing of DDoS attacks.
  - The Symantec report notes prices ranging from US$5 to more than $1,000. Pricing appears to be based on factors such as the duration of the attack and the level of DDoS defence mechanisms (if any) employed by the target.
  - Sellers were offering amplification attacks that generate more than 100 Gbps of traffic, however the report notes that in reality the traffic generally seen was in the range of 20-40 Gbps.

Wueest, C 2014, ‘The continued rise of DDoS attacks’, Symantec Security Response, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/continued-rise-of-DDoS-attacks-14-en.pdf

Distributed Denial of Service

Evolution

- DDoS attackers continue to change their tactics with the aim of reducing the resources required on their part (e.g. with the use of amplification) and defeating DoS defence techniques[1].

- Some of the factors driving the evolution of DDoS attacks include
  - Increased use of mobile devices and services
  - Proliferation of IoT devices and IoT-based services [2].

Wueest, C 2014, 'The continued rise of DDoS attacks', Symantec Security Response, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/continued-rise-of-DDoS-attacks-14-en.pdf

Al-Hadhrami, 2021, 'DDoS attacks in IoT networks: a comprehensive systematic literature review'. *World Wide Web*

Distributed Denial of Service

- The Symantec report lists a range of common motivations for DDoS attacks:
  - Extortion and Profit
    - Extorting funds from the victim to avoid a DDoS attack. Can be accompanied by a small attack to demonstrate capability. Ransom demands can be small, however they can later grow if the victim pays the ransom.
  - Diversion
    - DDoS attacks can act as a distraction from a targeted cyber attack. There are several side effects such as preventing legitimate users from checking their data on the service and a loss of forensic data as services and devices are restarted.

Wueest, C 2014, 'The continued rise of DDoS attacks', Symantec Security Response, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/continued-rise-of-DDoS-attacks-14-en.pdf

Distributed Denial of Service

- Hacktivism
  - Various groups use DDoS attacks for ideological reasons and to attract media attention.
- Disputes
  - Any dispute between two individuals could result in a DDoS attack, particularly when the dispute arises on online services such as forums and games.
- Collateral Damage
  - Some DDoS attacks are unintentional, such as publication of a particular website on a popular forum or via traditional media, causing an increase in traffic that the service cannot natively handle.

Wueest, C 2014, 'The continued rise of DDoS attacks', Symantec Security Response, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/continued-rise-of-DDoS-attacks-14-en.pdf

Denial of Service

Mitigations

You can take a few simple steps to prevent DDoS attacks:

- Regularly apply security patches to your website.
- Use a CDN or DDoS mitigation provider to front your online services.
- Be careful not to allow details about the address of your 'origin servers' to leak onto the internet, so that attackers cannot attempt to access it directly, bypassing the CDN or DDoS mitigation provider.

ACSC, 2020 *Denial of Service,* https://www.cyber.gov.au/acsc/view-all-content/threats/denial-service

Denial of Service

Mitigations

- Protect your 'origin servers' from direct access by implementing network filtering that limits access to traffic coming through your CDN or DDoS mitigation provider.
- Harden DNS servers against DDoS attacks.
- Consider mirroring part or all of your DNS infrastructure with DDoS resilient DNS providers.
- Run online services on different infrastructure to your critical business systems where practical.
- Have an incident response plan in place that accounts for DDoS attacks, and conduct exercises to ensure that the plan is effective.

ACSC, 2020 *Denial of Service,* https://www.cyber.gov.au/acsc/view-all-content/threats/denial-service

Denial of Service

Mitigations

- NIST SP 800-53 Control SC-5 relates to Denial of Service Protection.
- It notes that various technologies can be used to limit or eliminate the effects of DoS attacks.
- This includes boundary protection devices filtering certain traffic, and employing increased capacity and bandwidth to reduce susceptibility to these attacks.
- Restricting internal users from being able to launch DoS attacks, and detecting DoS attacks and monitoring to ensure availability of systems, are also both noted enhancements.

NIST 2017, 'Security and Privacy Controls for Federal Information Systems and Organizations', National Institute of Standards and Technology, SP 800-53r4.