DDoS Midterm

Feng Wei

February 22, 2020

1 Introduction

DDoS introduction

2 What is DDoS

- What is a Denial of Service / Distributed Denial of Service attack?
- If you classified (D)DoS attacks which metrics would you use? Why?
- Explain the difference between symmetric and asymmetric (D)DoS attacks?
- How does a reflection and amplification (D)DoS attack work? What is the amplification factor?
- List 5 protocol/services, other than the ones given in the text, that can be used to amplify a (D)DoS attack.
- What is the difference between exploiting vulnera and misuse type (D)DoS attacks?
- Considering the recent trends in cyber space, what other (D)DoS attack approaches are expected in the next 5 years?
- Pick a protocol (you may use IETF RFC documents) and find 3 of its native features/functionalities that can be misused to perform (D)DoS attack.
- Compare and contrast the different botnet topologies. Which one do you think is better? Why?
- If you ran a botnet, which new technologies would you incorporate in your design to increase resilience?
- Design a botnet. Discuss and justify your architecture, topology and resilience technology choices.
- If you classified (D)DoS attack tools which metrics would you use? Why?
- Discuss the capabilities of (D)DoS tools through time. Which new approaches should be expected in the next 5 years?

3 History and Motivation

- List the classes of attacks handled by technologies described in this chapter.
- For each security technology discussed in this chapter, explain which attacks it mitigates and how the risk of a successful attack is di- minished.

- Explain the security issues that remain open, in spite of the available security measures.
- For each DDoS tool and technology, explain the vulnerability that it exploits. Give an explanation as to why those vulnerabilities have not been fixed.
- For each attack in Table 3.2 explain whether it was legal or not and why.
- For each attack in Table 3.2 explain whether it was justified or not and why.

4 Legal Considerations

- Some security professionals have been suggesting that victims of cyber-attacks "hack back" and attack the criminals that are at- tacking them. Provide the outline of a legal reasoning either for or against using DDoS to act against someone you perceive as attacking your system.
- Outline the importance of attack attribution in enforcing anti-DDoS laws.
- Is it reasonable to have laws that define liability for victims of DDoS events? Explain your answer.
- Look up instances of DDoS being used for protest. Attempt to draft a legal strategy defending the use of DDoS in the protest for at least one that you agree with and one you find offensive.
- Use the Tallinn Manual 2.0 to explain whether or not the Russian DDoS attacks on Estonia and Georgia were legal.
- Find laws that justify the use of Internet blackouts by a nation state within its own territory.
- Find laws that forbid the use of Internet blackouts by a nation state within its own territory.

5 DDoS Research: Traffic

- Classify and compare the datasets used for DDoS studies. Discuss the pros and cons of each class.
- What are the three most important dataset properties? Why?
- What are the well known assumptions used to generate synthetic network traffic? Under what conditions do these assumptions hold and fail?
- What are the commonly used network traffic characteristics inorder to generate synthetic network traffic? List two additional character- istics that will improve the quality of generated traffic.
- What is the difference between DDoS attack tools and stress testing toos?
- What are the known shortcommings of background traffic genera- tors? Which current trends in today's network traffic is not repre- sented properly by existing traffic generators? Why?
- Discuss the pros and cons of using operational background traffic and using synthetically generated network traffic.

6 DDoS Research: Testing

- Discuss the difference between network emulator and network sim- ulator.
- List couple of contemporary network simulation / emulation tools, that are not listed in the chapter, and point out the differences.

- List and briefly explain the technologies used in contemporary net- work testbeds.
- Discuss the importance of system and network virtualization.
- List couple of contemporary network testbeds, that are not listed in the chapter, and point out the differences.
- Network Mirroring approach does not consider some of the effects of a DDoS attack. Couple of them are listed in the chapter. List (if any) other effects that are not considered. Propose (if possible) ways to include them into testing environment.