DDoS attack and mitigation in web application

Rama Shah

Department of Computer Science

New York University Tandon School of Engineering

New York, USA

rls511@nyu.edu

***Abstract*—Distributed Denial of Service (DDoS) is a subset of Denial of Service (DoS) attack where compromised and connected online devices known as botnets are used to produce artificial traffic in mass to overwhelm a target website. This paper attempts to research DDoS mitigation currently available.**

Keywords—DDoS, Stateful multilayer inspection, SMLI, DoS attack, Network Security, Cybersecurity.

I. INTRODUCTION

A Distributed Denial of Service (DDoS) is a malicious attack in an attempt to make an online service or network unavailable by overwhelming them with internet traffic from multiple sources. In this day and age, having platform availability is a key and a default expectation from any customer or clients. DDoS is not only a nuisance in running a legitimate business but also a high security risk which falls under lack of Availability threat. I am exploring and attempting to use Stateful multilayer inspection (SMLI) firewall and its implementation to detect and mitigate DDoS attack.

II. METRICS

I attempt to use threshold detection rate metrics in DDoS mitigation to prevent DDoS attack by setting up a network firewall to scan the IP addresses to make sure that the entire data packets are safe and trusted. Identification of normal and attack patterns is crucial as this is a key metric to determine the utility and efficiency of the proposed techniques. Other commonly used metrics that have been considered in literature include detection rate, average response time, percentage bandwidth utilization and normal packet survival ratio [1].

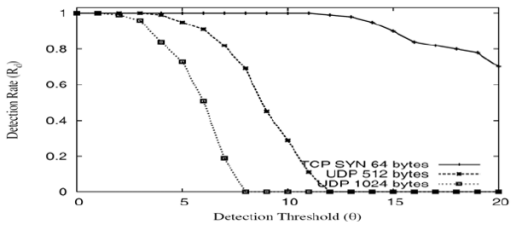

Fig. 1: Effects of server threshold on the detection rate of DDoS attack types of sample metrics [2]

III. THREAT MODEL

Based on the Threat modeling to understand the system and the assets involved, the threat modeling predicated for DDoS attack is represented in the diagram below.

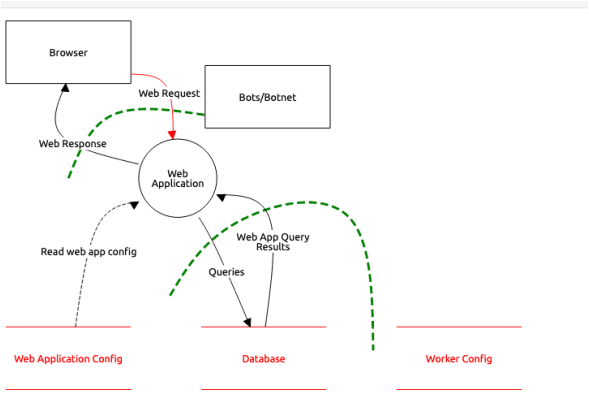

Fig. 2 Threat Model for DDoS attack

IV. RELATED RESEARCH

"To mitigate attacks, networks providers have two main tools available. One is to contract a DDOS mitigation services to scrub DDoS traffic and forward only legitimate traffic. Another option is to discard traffic for specific prefixes at the IXP before reaching their target network by using so- called blackholing" [3]. I am attempting to implement method(s) of DDoS attack mitigation via SMLI firewall. Many research articles have not discussed firewalls of any kind in depth. Since the author and others attempt to provide an "updated perspective on the state of DDoS amplification attacks and protocols in the wild" it differs from my approach is to implement SMLI, it does not work in my case. "The other prevention techniques include disabling unused services, applying security patches, changing IP address, disabling IP broadcasts, load balancing and honeypots" [4].Though

learning more about the DDoS especially in cloud computing attack in these days of virtualization is insightful, it differs from my SMLI firewall implementation approach. I am attempting to look at TCP/IP packets in a broader context ideally based on cumulative data i.e., request, response connection, application layers etc.

V. MOTIVATING EXAMPLE

In Confidentiality, Integrity and Availability (CIA) principle, Network Security is a domin classified as the "A". In recent events, many companies had to suffer from a DDoS attack where many users were unable to access certain platforms. As a software engineer for a Crypto financial service, availability is very important. DDoS is intriguing to me because the attacks and its negative repercussions are highly visible in press and social media which can affect the "trust" people have in order to use financial services. Platform unavailability can be bad for business. DDoS is an unusual number of traffic coming to the network through a few specific IP addresses manually or by botnets. The motivation is addressing the origination and detection of Network Security and DDoS attacks.

VI. HYPOTHESIS

In order to prevent DDoS attack, we can set up a network firewall to scan the IP addresses to make sure that the entire data packets are safe and trusted. There are different types of firewalls, but I came across Stateful multilayer inspection (SMLI) firewalls that seem interesting and applicable. Generally, there are seven layers of OSI model which are Physical layer, data link layer, network layer, transport layer, session layer, presentation layer and finally application layer. Setting up the SMLI firewall will inspect the data packet in each layer.

I came across multiple companies that provide "next-gen" firewalls including SMLI firewall for DDoS attack prevention. What differentiated from my approach is that I am looking into DIY SMLI firewall but not completely sure if this is a good approach for a newbie in Network Security. The way my solution differs from the current solution to the DDoS problem is that the current service we are using does not mention SMLI in their services.

VII. EMPIRICAL EVIDENCE

As per my hypothesis, attempting to prevent DDoS attack is to set up a network firewall to scan the IP addresses to make sure that the entire data packets are safe and trusted, I came across few open-source software to simulate the firewall and programs to configure packet filtering such as iptables. I tried to simulate "fake" traffic using network traffic generator such as WAN Killer and second contender NetScanTools however I am having issues making both simulators i.e., firewall and fake network interact with each other. I also tried to use CAIDA's data set which I want to upload in the firewall simulator however I am waiting for permission.

For my research the closest empirical evidence I can demonstrate right now is from the articles "Fig. 2: Time Series: Packet size vs Relative time [1] which shows the time chart where the attack timeline was detected."

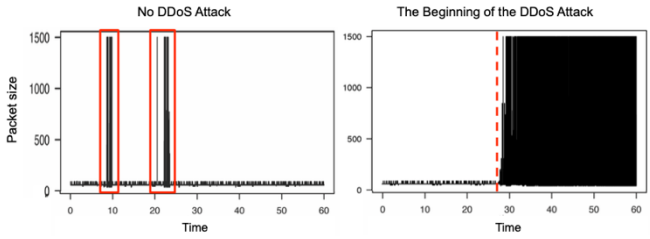

Fig. 3 Time Series: Packet size vs Relative time which shows the time chart where the attack timeline was detected. [5]

VIII. CONCLUSION

In conclusion SMLI is an advanced firewall security system. SMLI has a series of advanced firewall that work in tandem to work as a stateful and stateless packet filtering working on multi-layer such as network and transport layer which can be used to mitigate DDoS attack.

A. Limitation

There are larger corporations such as IBM which offers SMLI firewall, however DIY was not viable currently due to lack of knowledge and time

B. Future work

There are some Mini-ITX Firewall DIY instructions I found which are highly interesting. Hopefully in network security class I will attempt to build one.

REFERENCES

[1] Opeyemi Osanaiyeab, Kim-Kwang Raymond Choo, Mqhele Dlodloa, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework" in Journal of Network and Computer Applications, Volume 67, May 2016, Pages 147-165

[2] Yu Chen, Kai Hwang, "Distributed Change-Point Detection of DDoS Attacks over Multiple Network Domains* " in Research gate, December 2010, Pg 21-22

[3] Daniel Kopp, Christoph Dietzel, and Oliver Hohlfeld, "DDoS Never Dies? An IXP Perspective on DDoS Amplification Attacks" arXiv, 2103.04443v1 March 2021, Page 10.

[4] N. Weiler, "Honeypots for distributed denial-of-service attacks," Proceedings. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002, pp. 109-114, doi: 10.1109/ENABL.2002.1029997.

[5] Michele Nogueira, Augusto Almeida Santos andJose´ M. F. Moura, "Early Signals from Volumetric DDoS Attacks: An Empirical Study", 1609.09560v2, May 2017, Page 4